المركز الديمقراطي العربي
برلين - المانيا

الجرائم الالكترونية
في الفقه الإسلامي والقانون الوضعي

جمع وتنسيق:
د. عباس حفصي

وقائع اعمال المؤتمر
الدولي الافتراضي
أيام 14 - 15 /ايار- مايو 2022

Democratic Arabic Center
Berlin - Germany

الجرائم الالكترونية في الفقه الإسلامي والقانون الوضعي

VR . 3383 – 6628 B

DEMOCRATIC ARABIC CENTER
Germany: Berlin 10315 Gensinger- Str: 112
http://democraticac.de
TEL: 0049-CODE
030-89005468/030-898999419/030-57348845
MOBILTELEFON: 0049174274278717

المركز الديمقراطي العربي ألمانيا - برلين
&
جامعة الجفرة - ليبيا

2022

جامعة الجفرة
UNIVERSITY OF ALJUFRA

المركز الديمقراطي العربي
للدراسات الاستراتيجية، الاقتصادية والسياسية
Democratic Arabic Center
for Strategic, Political & Economic Studies

كتاب وقائع المؤتمر العلمي الافتراضي:

الجرائم الإلكترونية في الفقه الإسلامي والقانون الوضعي

Cybercrime in Islamic jurisprudence and positive law

الجـــــــــزء الثـــــاني: Second Part

إشراف وتنسيق:

د.عباس حفصي، جامعة الأغواط، الجزائر

د.حنان طرشان، جامعة باتنة1، الجزائر

الناشر:

المركز الديمقراطي العربي

للدراسات الإستراتيجية والسياسية والاقتصادية

ألمانيا/برلين

Democratic Arabic Center

Berlin / Germany

المركز الديمقراطي العربي

للدراسات الإستراتيجية والسياسية والاقتصادية ألمانيا/برلين

Tel: 0049-code Germany

030-54884375

030-91499898

030-86450098

البريد الإلكتروني

book@democraticac.de

المركز الديمقراطي العربي، برلين، ألمانيا

جامعة الجفرة، ليبيا

ينظمون المؤتمر الدولي الافتراضي السابع الموسوم بـ:

الجرائم الإلكترونية في الفقه الإسلامي والقانون الوضعي

Cybercrime in Islamic jurisprudence and positive law

أيام 14-15 مايو2022

إقامة المؤتمر بواسطة تقنية التّحاضر المرئي عبر تطبيق Zoom

ملاحظة: المشاركة مجانا بدون رسوم

الرئاسة الشرفية للمؤتمر:

أ. عمار شرعان، رئيس المركز العربي الديمقراطي، برلين، ألمانيا

د.يوسف أبوبكر جلالة، رئيس جامعة الجفرة، ليبيا

رئيس المؤتمر:

د.عباس حفصي، ليبيا

رئيس اللجنة العلمية للمؤتمر:

د. محمد عبد الحفيظ الشيخ، عميد كلية القانون، جامعة الجفرة، ليبيا

المنسق العام للمؤتمر:

د.أحمد بوهكو، رئيس تحرير المجلة الدولية للدراسات الإقتصادية

رئيس اللجنة التحضيرية للمؤتمر:

د.ناجية سليمان عبد الله، رئيسة تحرير مجلة العلوم السياسية والقانون

رئيس اللجنة التنظيمية للمؤتمر:

أ.كريم عايش، المركز الديمقراطي العربي، برلين، ألمانيا

مدير المؤتمر:

أ.كريم عايش، المركز الديمقراطي العربي، برلين، ألمانيا

التنسيق والنشر:

د.حنان طرشان، جامعة باتنة1، الجزائر

مدير إدارة النشر:

د.أحمد بوهكو، المركز الديمقراطي العربي، برلين، ألمانيا

أعضاء اللجنة العلمية:

د. زعادي محمد جلول، جامعة البويرة، الجزائر	د.برني كريمة، جامعة قسنطينة1، الجزائر
د.عالي حسن، جامعة سعيدة، الجزائر	د.نورس أحمد كاظم الموسوي، كلية المستقبل الجامعة
د.بوديبة رابح، جامعة سكيكدة، الجزائر	د.عدراء بن يسعد، جامعة قسنطينة!، الجزائر
د.دعاس آسيا، جامعة باتنة1، الجزائر	لوني تصيرة، جامعة البويرة، الجزائر
د.أحمد بوعون، كلية الحقوق، تونس	د.أمل فوزي أحمد عوض، جامعة حلوان، مصر
د.ميثم منفي كاظم العميدي، جامعة الكاظم، العراق	د.عبد القادر الشايط، جامعة محمد الأول، وجدة، المغرب
د.نبيل عبد الرحمن ناصر الدين إسماعيل، عضو هيئة التدريس، أكاديمية الشرطة، اليمن	د. هشام خلوق، جامعة عين الشق، المغرب

كلمـــــة رئيـــــس المؤتمـر:

بسم الله الرحمن الرحيم:

معالي الدكتور/ يوسف أبوبكر جلالة رئيس جامعة الجفرة بليبيا الشقيقة

سعادة الدكتور عمار شرعان، رئيس المركز الديمقراطي العربي، برلين، بألمانيا

رئيس اللجنة العلمية، د.محمد عبدالحفيظ الشيخ عميد كلية الحقوق بجامعة الجفرة

رئيس اللجنة التحضيرية، الدكتورة ناجية سليمان عبد الله، رئيس تحرير مجلة العلوم الساسية والقانونية

المنسق العام، د. أحمد بوهمو

رئيس اللجنة التظيمية، أ. كريم عايش

أصحاب السعادة والسيدات والسادة رؤساء المشاركين في المؤتمر الدولي للجريمة الالكترونية

إن الجرائم بطبيعتها توجد بوجود الإنسان وتتطور بتطوره ، وما أن الإنسان دائما في تطور مستمر بفضل ثورة المعلومات والتكنولوجيا المتطورة فإننا نجد العلماء يحاولون الاستفادة منها، وبالمقابل نجد أن المجرمين يحاولون الاستفادة أيضا من التقدم التقني فأصبحت التكنولوجيا شيئا مباحا للجميع للصالح والطالح ، بل إن المجرمين كثر، واستطاعوا اكتساب خبرات ومهارات أكثر في تعاملهم مع الانترنت وارتكابهم للجرائم الإلكترونية عبر الأقمار الصناعية، ولم تعد جرائمهم تقتصر على إقليم دوله واحدة بعينها بل تجاوزت حدود الدولة، وهى جرائم متكررة ومستحدثة تمثل ضربا من ضروب الذكاء الإجرامي، استعصى إدراجها ضمن الأوصاف الجنائية التقليدية في القوانين الجنائية الوطنية والأجنبية، مما أوجب تطوير الأنظمة التشريعية الجنائية الوطنية بذكاء تشريعى مماثل للذكاء الإجرامى تعكس فيه الدقة الواجبة على المستوى القانوني وسائر جوائب تلك التقنيات وأبعادها الجديدة

ما يضمن في كافة الأحوال احترام مبدأ شرعية الجرائم والعقوبات من ناحية، ومبدأ الشرعية الإجرائية من ناحية أخرى، وتكامل في الدور والهدف مع المعاهدات والأنظمة الدولية، وهذا كله يمكن الوصول إلى سبل مواجهة هذه الجرائم الإلكترونية من حلال تعاون الأنظمة الدولية وفهمها للسبل الشرعية والعملل بها في مكاافحة هذا النوع من الجرائم المتكررة والمستحدثة، فتكثر الاستفادة من هذه الوسائل والأجهزة الالكترونية، ويقل خطرها.

بدأت الثورة المعلوماتية نتيجة اقتران تقنيتي الاتصالات من جهة، والمعلومات وما وصلت إليه من جهة أخرى، فالثورة المعلوماتية هي الطفرة العلمية والتكنولوجية التي نشهدها اليوم، حتى بات يطلق على هذا العصر عصر المعلومات. وتعد المعلومة من أهم ممتلكات الإنسان التي اهتم بها على مر العصور، فجمعها ودونها وسجلها على وسائط متدرجة التطور، بدأت بجدران المعابد والمقابر، ثم انتهت باختراع الورق الذي تعددت أشكاله، حتى وصل بها المطاف إلى الحاسب الآلي والأقراص الإلكترونية الممغنطة.

وقد تغني الأرقام عن الكثير من الأقوال، وأحيانا عن إيجاد مدخل مناسب عندما تزاحم العقل أفكارا عديدة ،ومنذ عقد مضى لم نكن نتصور إن الحياة سوف تعتمد بصفة أساسية ومطلقة على جهاز الحاسب الآلي وملحقاته، إلا أن ذلك أصبح واقعا وحقيقة، فمؤسسات الدولة تعتمد على الحاسب الآلي، والشركات العامة والخاصة كذلك، بل إن الأفراد في معاملاتهم الخاصة باتوا حريصين على التعامل معه و اعتماده في معاملاتهم بصورة تكاد تكون أساسية يمكن معها القول إن جهاز الحاسب الآلي أصبح يقاسم الإنسان حياته في نهاره وليله ونومه ويقظته، كيف لا وجهاز الحاسب الآلي في الطائرة وفي المعمل وفي القوات المسلحة وفي المواصلات والاتصالات على نحو يمكن معه القول إننا نعيش ثورة الحاسب الآلي. وقد تعززت منظومة الحاسب الآلي بالكمال بظهور شبكة المعلومات الدولية (الانترنت) والتي جعلت من العالم قرية صغيرة من حيث الأحداث والوقائع التي يمكن متابعتها في أي زمان ومكان، بل لحظة حصول الحدث ذاته.

ثم استتبع اتساع ونماء كل من تكنولوجيا الاتصالات والحاسبات من جهة، والبرمجية بما تضمنته من هندسة البرمجيات وصناعتها من جهة أخرى، والاندماج المذهل الذي حدث بينهما إلى الوصول إلى استحداث تقنية نظم المعالجة الآلية للمعطيات. لكن وعلى الرغم من المزايا الهائلة التي تحققت وتتحقق كل يوم بفضل الحاسب الآلي على جميع الأصعدة وفي شتى ميادين الحياة المعاصرة، فإن هذه الثورة التكنولوجية المتنامية صاحبتها في المقابل جملة من الانعكاسات السلبية والخطيرة جراء سوء استخدام هذه التقنية، ذلك أن الآثار الإيجابية المشرقة لعصر تقنية المعلومات لا تنف الانعكاسات السلبية التي أفرز تها هذه التقنية.

نتيجة إساءة استخدام الأنظمة المعلوماتية واستغلالها على نحو غير مشروع وبطرق من شأنها أن تلحق الضرر بمصالح الأفراد والجماعات، الشيء الذي استتبعه ظهور أنماط جديدة من الاعتداءات على تلك المعلومات المخزنة في بيئة افتراضية، ليس هذا فحسب بل سهلت هذه التقنية ارتكاب بعض الجرائم التقليدية، فازدادت هذه المخاطر تفاقما في ظل البيئة الافتراضية التي تمثلها شبكة المعلومات، مما أفرز نوعا جديدا من الجرائم، لم يكن معهودا من قبل عرفت بجرائم الحاسوب، أو الجرائم المعلوماتية.

والخطورة التي تتميز بها هذه الجرائم عن باقي الجرائم التقليدية تكمن في أنها سهلة الارتكاب نتيجة للاستخدام السلبي للتقنية المعلوماتية بما توفره من تسهيلات، وأن مرتكبي مثل هاته الجرائم لا ينتموا إلى زمرة المجرمين العاديين ذلك لأنهم يتسمون بالذكاء والدراية في التعامل مع مجال المعالجة الإلية للمعطيات والإلمام بالمهارات والمعارف التقنية، فضلا على أن آثارها ليست محصورة في النطاق الإقليمي لدولة بعينها بل تشمل جميع دول العالم على اعتبارها متصلة ببعضها البعض بواسطة الشبكة العالمية للمعلومات.

وكما تكمن الخطورة كذلك من عدة نواحي، وعلى سبيل الذكر لا الحصر نذكر من الناحية الأخلاقية أن مثل هاته الجرائم تستهدف فضح الأسرار الشخصيّة أو القذف أو التشهير بشركات أو أشخاص بقصد الإضرار بالسمعة الشخصية أو المالية ،ولعل أبرز الجرائم المتواجدة حاليا على مستوى الأنظمة المعلوماتية ومن خلال الانترنت نجد تجارة الدعارة و والصور الخليعة والاستغلال الجنسي بكل صوره التي أصبحت أكبر التجارات المتواجدة حاليا على الشبكة العنكبوتية، وأصبحت تؤرق جل دول المعمورة من أجل محاربتها ،ولقد أجريت دراسات حول علاقة مثل هاته الجرائم

عن باقي الجرائم الأخرى ،حيث وجد أن الجرائم تزداد اطرادا مع الجرائم الأخرى، وكثير من الدول سواء المتقدمة او غير المتطورة باتت تشتكوا من مثل هذه المواقع التي تبث هاته الافكار.

ومع الخطورة الأخلاقية نجد كذلك هناك خطورة مجتمعية حيث قد لا يدُرك كثيرون أنّ الجماعات المتطرّفة كانت من أولى الجماعات الفكريّة التي استخدمت الحاسوب ودخلت العالم الإلكتروني حتى قبل أنْ تظهر شبكة الإنترنت بسنوات، مما أصبح يهدد مجتمعات بأسرها. ومع الغموض الذي يكتنف جرائم الحاسوب حيث أصبحت تثير بعض التحديات القانونية والعملية أمام الأجهزة المعنية بمكافحة الجريمة (أجهزة العدالة الجنائية بجميع مستوياتها وعلى اختلاف أدوارها)، وبالذات فيما يخص إثبات هذه الجرائم وآلية مباشرة إجراءات الاستدلال والتحقيق عبر البيئة الافتراضية لتعقب المجرمين وتقديمهم للعدالة.

إن هذا الغموض الذي يصاحب هاته الجرائم جعل مجال البحث فيها يضيق بل جعل الكثير من الفقهاء سواء من الناحية الشرعية أو القانونية يترددون في إعطاء حكم شرعي أو تجريم بصورة واضحة، ومع ذلك حاول المشرع القانوني وكذا فقهاء الشريعة الإسلامية مسايرة هذا التطور لهذا النوع من الجرائم.

أيها السادة والسيدات: المشاركون الكرام

إننا وبكل فخر واعتزاز، نرحب بكم مجددا وآمل أن نستفيد من هذا المؤتمر على كافة الأصعدة والمستويات

في الأخير، وإذ أتشرف برئاسة هذا المؤتمر أجدد شكري وعرفاني لكل من ساهم في إنجاح هذا المؤتمر من قريب أو بعيد...

شكرا على حسن الإصغاء

والسلام عليكم ورحمة الله،

رئيس المؤتمر:

د.عباس حفصي، جامعة الأغواط، الجزائر

:

ديباجة المؤتمر:

إن الجريمة الالكترونية فعل يتسبب في ضرر جسيم للأفراد والجماعات والمؤسسات بهدف ابتزاز الضحية وتشويه سمعتها لتحقيق مكاسب مادية أو لخدمة أهداف سياسية باستخدام وسائل وأنظمة اتصال حديثة مثل الإنترنت. ويمكن وبحسب البيئات والوسائل المختلفة المستخدمة، تحدث الجريمة الإلكترونية دون تواجد الجاني في مكان الحدث، وتستند الطريقة المستخدمة إلى تكنولوجيا الاتصالات والمعلومات الحديثة. إن عدد الجرائم الالكترونية في انتشار واسع نظرا للتطور الحاصل في التكنولوجيا سواء في وسائل التواصل الاجتماعي آو عبر الدول مما أضر باقتصادها ومختلف تعاملاتها، كما أن الأساليب الإجرامية اختلفت وتنوعت من قبل متمرسين في هذا الجانب.

وبما أن الشريعة رادعة في جانب العقوبات فاشتملت على عقوبات توقف كل مجرم يتجاوز حدود الله تعالى ويسعى في الأرض فسادا والله لا يحب المفسدين. وجاء القانون أيضا معاقبا كل من تسول له نفسه الاعتداء على حقوق الناس بالسلب أو النهب أو الظلم.

كما أن هناك عدة انواع للجرائم الالكترونية وتتمثل في سرقة الهوية حيث يقوم فيها المجرم بإغراء الضحية واستخراج المعلومات منه بشكل غير مباش، واستهداف المعلومات الخاصة من أجل الربح واستغلالها لتحقيق مكاسب مادية وأيضا تهديد الأفراد حيث يقوم المجرم، من خلال القرصنة وسرقة المعلومات، بالوصول إلى المعلومات الشخصية الخاصة بالضحية، ثم ابتزازهم لكسب المال وتحريضهم على ارتكاب أعمال غير قانونية قد يتعرضون فيها للظلم.

وكذلك من الأنواع التشهير حيث يستخدم المجرم المعلومات المسروقة ويضيف اليها معلومات كاذبة ثم يرسلها عبر وسائل التواصل الاجتماعي أو البريد الإلكتروني لكثير من الناس بهدف تشويه سمعة الضحية وتدميرها نفسياً.وغيرها من الأنواع المتعددة في هذا المجال.

إن خطر الجريمة الالكترونية خطر عظيم تجاوز كل الحدود والأعراف وأصبح يهدد الأشخاص والدول، لذا وجب الحد من هذا التفاقم المتزايد بمعاقبة المجرمين عقابا صارما دون تردد أو تأخير. الجريمة الالكترونية يصعب اثباتها جراء التعقيدات التي في ثناياها لان من السهولة اخفاء دليل اثباتها لذلك يجد المحققون صعوبة جمة في اثبات أدلة الجريمة.

إشكالية المؤتمر الدولي:

- ✓ ما هو موقف الشريعة الاسلامية والقانون الوضعي من الجريمة المعلوماتية؟
- ✓ ماهي الطرق المنوطة بإثبات هاته الجرائم؟
- ✓ كيفية تعامل الجهات المختصة مع هذا النوع من الجرائم؟
- ✓ ماهي الحلول الممكنة للحد من هاته الجرائم وسبل مكافحتها؟
- ✓ ما مدى مواكبة المشرع العربي للقوانين المعاصرة في مجال المعلوماتية

أهداف المؤتمر الدولي:

- ✓ الجريمة الالكترونية ماهيتها ومعرفة أسبابها وأركانها
- ✓ الجريمة الالكترونية وسبل مكافحتها
- ✓ موقف الشريعة الإسلامية من الجريمة المعلوماتية.
- ✓ إثبات الجريمة من الناحية الشرعية والقانونية.
- ✓ مواكبة النصوص العقابية في القانون للنصوص في الشريعة الاسلامية.
- ✓ التعرف على تجارب الدول الأخرى في ردع أصحاب هاته الجرائم.
- ✓ مدى مواكبة نصوص القوانين العقابية في الدول العربية للدول المتقدمة في هذا الجانب.

محاور المؤتمر:

المحور الأول: الإطار العام للجريمة الالكترونية

- ✓ تعريف الجريمة الالكترونية وأركانها.
- ✓ أسباب ارتكابها
- ✓ طبيعتها وخصائصها

المحور الثاني: مواجهة الجرائم الالكترونية وطرق إثباتها

- ✓ الإثبات الشرعي والقانوني للجريمة الالكترونية
- ✓ طرق مواجهة الجرائم الالكترونية
- ✓ شروط وطرق الإثبات الالكتروني

المحور الثالث: الجرائم المتصلة بالجرائم الالكترونية

- ✓ جريمة القذف والتشهير الالكتروني
- ✓ جريمة السرقة الالكترونية
- ✓ جريمة النصب والاحتيال الالكتروني
- ✓ جريمة التزوير الالكتروني
- ✓ الإرهاب الالكتروني

المحور الرابع: دور مختلف المؤسسات في مكافحة الجريمة الالكترونية

- ✓ المحاكم والقضاء
- ✓ النيابة العامة
- ✓ المخابر الجنائية

فهرس المحتويات

الجريمة الإلكترونية وسبل المواجهة التشريعية

Cybercrime and legislative responses

د،نصيرة لوني/ جامعة أكلي محند أولحاج، البويرة/ الجزائر
Dr.Nacira Louni/ Akli Mohand Oulhadj، Bouira /Algeria

ملخص الدراسة:

تسعى الدراسة لتبيان ان الجريمة الإلكترونية هي جريمة تمس في صميمها قيما جوهرية تخص الأفراد والمؤسسات وحتى الدول، فسارعت العديد من الدول لإيجاد الحلول لها من خلال ايجاد اليات وسبل التي يمكن استغلالها التي تؤدي إلى الحد منها اذ قام المشرع الجزائري بسن نصوص قانونية لقمع الجريمة الإلكترونية وذلك بسبب التزايد الكبير اللامتناهي للاعتداءات الحاصلة على الانظمة المعلوماتيّة في الجزائر، ومن اهم الامور الني أولاها المشرع اهمية قصوى أمن الدولة والحفاظ على النظام العام.

الكلمات المفتاحية: الجريمة الإلكترونية، سبل المواجهة، المعلوماتيّة، الآليات، التشريع الجزائري.

Abstract:

This study aims to demonstrate that cybercrime is a crime that touches upon its core values for individuals، institutions and even states. Many States have sought solutions by adopting mechanisms and ways to reduce them. The Algerian legislator have enacted legal texts to deter cybercrime. This is due to a growing number of attacks on information systems in Algeria. One of the most important questions to which the legislature attaches the greatest importance is the security of the state and the maintenance of public order.

Keywords: Cybercrime, responses, information system, The Algerian legislation.

مقدمة:

لقد أدى التطور التكنولوجي السريع الذي نعيشه هذه الأيام الذي يطلق عليه عصر ثورة المعلومات أو تدفق المعلومات إلى ظهور وسائل وأساليب جديدة لاستخدامات الأنترنت والكمبيوتر، وهذه الوسائل في تطور مستمر بمرور الوقت، وبالتالي فإن الجرائم التي ترتكب بمناسباتها في تطور موازي، مما يصعب أن يحيط القانون بجميع الإلكترونية أو يضع حلا جذريا لها، لذلك فإن الأفراد ملزمين من أجل الحفاظ على خصوصياتهم وأموالهم باتخاذ الحيطة والحذر، وبالاستخدام العقلاني لوسائل الاتصال الحديثة

تعتبر الجريمة الإلكترونية من الجرائم الحديثة التي تطورت وانتشرت بوتيرة سريعة لتنقل عالم الجريمة إلى بعد جديد، تطور من خلاله كل من مرتكب الجريمة ووسائل ارتكابها لنصبح اليوم أمام مجرمين ذوي درجة عالية من الذكاء، متمرسين و ذوي كفاءة كبرى في استعمال التكنولوجيا الحديثة والتحكم فيها، لينتقل الفعل الإجرامي من الأفراد والمجتمعات إلى الدول ومؤسساتها، وهو الأمر الذي أصبح على التشريعات الوطنية والدولية التجند من أجل مكافحة الجريمة الإلكترونية بنصوص قانونية صارمة من شأنها الحفاظ على سلامة الأفراد والمؤسسات والدول من خطر الجريمة الإلكترونية بمختلف صورها (دمان ذبيح: 2020، ص. 137)

من هذا المنطلق تطلب الأمر منا وضع إشكالية مفادها:

مدى اهتمام المشرع الجزائري وكذا الأنظمة الدولية في التصدي للجريمة الإلكترونية باعتبارها من الجرائم المستحدثة الناتجة عن الممارسة السيئة للتكنولوجيا المعلوماتية؟

للإجابة على الإشكالية تم تقسيم بحثنا إلى مبحثين كالآتي:

المبحث الأول: مفهوم الجريمة الإلكترونية (تعريفها، خصائصها، مظاهر تحديها)

المبحث الثاني: سبل مواجهة الجريمة الإلكترونية (في التشريع الجزائري، الأنظمة الدولية)

خاتمة: تتضمن أهم النتائج والتوصيات التي توصلنا إليها

المبحث الأول: مفهوم الجريمة الإلكترونية

ظهرت الجريمة الإلكترونية لأول مرة في الدول التي عرفت تطورا لا مثيل له في المجالين التكنولوجي والمعلوماتي، ثم انتقلت إلى الدول الأخرى المستهلة للتكنولوجيا أصبحت محل الاهتمام المشرعين نظرا لخطورتها، لهذا نتطرق إلى تعريف الجريمة الإلكترونية مع تبيان خصائصها (المطلب الأول) ثم محاولة تبيان مظاهر تحديات الجريمة الإلكترونية' المطلب الثاني).

إن البحث في تعريف الجريمة محل الدراسة، يؤدي الي الاصطدام بالكثير من التعاريف

الفقهية المختلفة، وهو ما دفع بعض الفقهاء إلى القول أن هذه الجريمة تقاوم التعريف (رستم: 2000، ص.6). ورغم الجهود التي بذلتها عدة هيئات دولية على غرار الأمم المتحدة، ومنظمة التعاون الاقتصادي والتنمية، المجلس الأوربي وغيرها، والتي سعت الى وضع قواعد للمساعدة على محاولة فهم هذه الظاهرة، غير أن تلك الهيئات وغيرها من الفقهاء عجزوا عن وضع تعريف واحد متفق عليه (الحيسناوي: 2009، ص. 33).

يصعب الاتفاق على تعريف موحد للجريمة المعلوماتية، حيث اختلفت الاجتهادات في ذلك اختلافاً كبيرا ، يرجع إلى سرعة وتيرة تطور التقنية المعلوماتية من جهة، و تباين الدور الذي تلعبه هذه التقنية في الجريمة من جهة أخرى ، فالنظام المعلوماتي لهذه التقنية يكون محلاً للجريمة تارة، ويكون وسيلة لارتكابها تارة أخرى، فكلما كان البحث منصباً على الجرائم التي ترتكب ضد النظام المعلوماتي انطلق التعريف من زاوية محل الجريمة بأنها الجريمة المرتكبة بالاعتداء على النظام المعلوماتي، أما إذا كان البحث منصباً على دراسة الجرائم التي ترتكب باستخدام التقنية المعلوماتية ارتكز التعريف على الوسيلة وكان :" كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب الآلي(رستم :2000 ، ص.29)

فمنهم من يعرف الجريمة المعلوماتية على أنها فعل ضار يستخدم الفاعل، الذي يفترض أن لديه معرفة بتقنية الحاسوب، نظاماً حاسوبياً أو شبكةً حاسوبيةً للوصول إلى البيانات والبرامج بغية نسخها أو تغييرها أو حذفها أو تزويرها أو تخريبها أو جعلها غير صالحة أو حيازتها أو توزيعها بصورة غير مشروعة (السالك: 2000، ص.25)، ويعرفها **أحمد صياني** بأنها تصرف غير مشروع يؤثر في الأجهزة و المعلومات الموجودة عليها وهذا التعريف يعتبر جامع مانع من الناحية الفنية للجريمة الالكترونية حيث انه لارتكاب الجريمة يتطلب وجود أجهزة كمبيوتر زيادة على ربطها بشبكة معلوماتية ضخمة (مرعي: الجرائم الالكترونية- الأهداف-الأسباب-طرق الجرائم ومعالجتها).

ويعرفها آخرون على أنها جريمة ذات طابع مادي، تتمثل في كل فعل أو سلوك غير مشروع، من خلال استعمال الوسائط الإلكترونية، حيث تتسبب في تحميل أو إمكانية تحميل المجني عليه خسارة، وحصول أو إمكانية حصول مرتكبه على أي مكسب، وتهدف هذه الجرائم إلى الوصول غير المشروع لبيانات سرية غير مسموح بالاطلاع عليها ونقلها ونسخها أو حذفها، أو تهديد وابتزاز الأشخاص والجهات المعنية بتلك المعلومات، أو تدمير بيانات وحواسيب الغير بواسطة فيروسات (مرعي: الجرائم الالكترونية-الأهداف-الأسباب-طرق الجرائم ومعالجتها).

الفرع الثاني: خصائص الجريمة الإلكترونية

تميزت الجريمة الإلكترونية بخصائص ميزتها عن غيرها من الجرائم، سواء تعلقت هذه الخصائص بالشخص الذي يقدم على هذه الجرائم فميزته عن المجرم التقليدي أو تعلقت بالجريمة ذاتها وصعوبة اكتشافها وإثباتها أو ما يلعبه الضحية من دور فيها، أو تعلق الأمر بالنطاق المكاني لهذه الجريمة أو الخسائر التي تخلفها (خليفة: 2009، ص. 371)

أولا: الجرائم الإلكترونية من الجرائم العابرة للحدود

وسعت شبكات المعلومات عملية الاتصال وتبادل معلومات بين الدول والأنظمة التي يفصل بينها آلاف الأميال، ومع القدرة التي يتمتع بها الحاسب أدى ذلك إلى إمكانية ارتكاب الجريمة الإلكترونية في أماكن متعددة من العالم وفي وقت واحد، كما يمكن أن يكون المجني عليه في غير الدولة التي يقيم فيها الجاني (بولحية :2019 ، ص.1987) إن الجريمة المعلوماتية هي شكل من أشكال الجرائم العابرة للحدود، فمسرح الجريمة لم يعد محليا بل أصبح عالميا إذ أن الفاعل لا يتواجد ماديا على مسرح الجريمة وهذا التباعد في المسافات بين الفعل المرتكب من خلال الحاسوب والفاعل وبين المعلومات التي كانت محل الاعتداء، فالجاني يستطيع القيام بجريمته بالدخول إلى ذاكرة الحاسوب الآلي الموجود في بلد آخر وهذا الفعل قد يضر شخصا ثالثا في بلد آخر .ومن خلال هذه الخاصية الدولية يثار إشكال حول الاختصاص القضائي في محاكمة المجني عليه بمعنى آخر ما هي الدولة المختصة بمحاكمة الجاني؟ هل هي الدولة التي ارتكب على إقليمها النشاط إجرامي أم التي يوجد فيها المجني عليه؟ وبمعنى آخر أن هذه الجريمة لا تقع في دولة واحدة ولا تعترف هذه الجريمة بالحدود الجغرافية للدول إذ غالبا ما يكون الجاني في بلد والمجني عليه في بلد آخر وقد يكون الضرر المحتمل في بلد ثالث.

ثانيا: صعوبة اكتشاف وإثبات الجرائم الإلكترونية

تمتاز الجرائم المعلوماتية بصعوبة الاكتشاف والإثبات وذلك نظرا لعدم ترك الجاني آثار تدل على إجرامه، فالجرائم التي تتم بواسطة إدخال الرموز والأرقام، هي رموز دقيقة ويصعب اكتشافها وإثباتها لهذا عادة ما يتم اكتشافها بالصدفة وغالبا ما يتم معاقبة مجرمين وذلك لعدم وجود أدلة قائمة في حقه فالجريمة المعلوماتية لا تترك آثارا ملموسة وبذلك لا تترك شهودا يمكن الاستدلال بأقوالهم ولا أدلة مادية يمكن فحصها لأنها تقع في بيئة افتراضية يتم فيها نقل المعلومات وتناولها بواسطة نبضات الكترونية غير مرئية (بولحية : 2019، ص.1988).

وصعوبة اكتشاف وإثبات الجرائم المعلوماتية راجع لعدة أسباب منها وسيلة التنفيذ التي تتسم في أغلب الحالات بالطابع التقني الذي يضفي عليها الكثير من التعقيد ومن ثم فإنها تحتاج إلى خبرة فنية يصعب على المحقق التقليدي

التعامل معها، لأنها تتطلب إلماما خاصا بتقنيات الكمبيوتر ونظم المعلومات .ويصعب في جرائم المعلوماتية العثور على دليل مادي للجريمة وذلك راجع إلى استخدام الجاني وسائل فنية وتقنية معقدة في كثير من الأحيان، وهذا السلوك المادي في ارتكابها لا يستغرق إلا ثواني معدودة يتم فيها محو الدليل والتلاعب به.

ثالثا: تتطلب وسائل خاصة في الحاسب الآلي وشبكة الأنترنت

إن الجريمة المعلوماتية تستلزم لقيامها توفر الحاسب الآلي وكذلك شبكة الانترنت وسيلة ارتكاب الجريمة وأدواتها الرئيسية أماكن المعرفة التقنية فتكون ضرورية بحسب درجة خطورة الجريمة المعلوماتية

رابعا: تتطلب خبرة وتحكما في تكنولوجيا المعلوماتية عند متابعتها

إن جريمة المعلوماتية لها طبيعة تقنية وبذلك لا يستطيع رجال الضبطية القضائية التعامل باحترافية ومهارة أثناء البحث والتحري، لذلك لابد أن يكون المحقق متخصص في جريمة المعلوماتية حتى لا يتسبب في إتلاف الدليل الالكتروني.

خامسا: تعدد الجرائم المعلوماتية أقل عنفا من الجرائم التقليدية

إن هذه الجريمة تعتمد على الدراية الذهنية والتفكير العلمي المدروس القائم على معرفة بتقنيات الحاسب الآلي، وفي الواقع ليس هناك شعور بعدم أمان تجاه المجرمين في مجال المعرفة المعلوماتية لأن مرتكبيها ليسوا محترفي الإجرام

سادسا: دافع ارتكاب الجريمة المعلوماتية

إن باعث الدافع الجريمة المعلوماتية قد يختلف عن دافع الجريمة التقليدية فقد يكون الدافع مخالفة النظام العام والخروج على القوانين وقد يكون ماديا يراد به اكتساب مبالغ طائلة أو الإهانة والتشهير... إلخ يكن دون الاحتكاك المباشر بالمجني عليه (بولحية: 2019، ص.1988).

المطلب الثاني: مظاهر تحديات الجريمة الإلكترونية

ترتب على ظاهرة الجريمة الإلكترونية تحديات عدة: منها ظهور وتنامي الأنشطة الإجرامية الالكترونية وتَوَسُّل مرتكبيها بتقنيات جديدة غير مسبوقة في مجال تكنولوجيا المعلومات والاتصالات يسرت لهم ارتكاب هذه الأنشطة داخل حدود الدولة وخارجها، الأمر الذي أدى إلى انشغال المنظمات والمؤتمرات الدولية بهذا النوع من الجرائم ودعوتها الدول إلى التصدي لها ومكافحتها، من حيث تستعصي بعض الأنشطة على إدراجها ضمن الأوصاف الجنائية التقليدية في القوانين الجنائية الوطنية والأجنبية؛ ومن حيث ما يرتبط بهشاشة نظام الملاحقة الإجرائية التي تبدو قاصرة على استيعاب هذه الظاهرة الإجرامية الجديدة ، سواء على صعيد الملاحقة الجنائية في إطار القوانين الوطنية أم على صعيد الملاحقة الجنائية الدولية.

وعلى خلفية ما ذهب إليه البعض من أن القوانين القائمة تكفي في حد ذاتها لمواجهة الجرائم الإلكترونية، فإننا نعتقد إن كان لهذا الرأي شيئا من الواقعية، وهي أن بعض النصوص القائمة تواجه بعض الأنشطة المجرمة التي ترتكب بطريق الإنترنت، فإنه ينبغي ألا ننكر أن هناك نصوصا أخر صادف تطبيقها بعض الصعوبات، منها ما يتعلق بطبيعة الجريمة الإلكترونية غير المادية، ومنها ما يتعلق بهاجس التعارض مع مبادئ هامة ومستقرة في القانون الجنائي

، كمبدأ شرعية الجرائم والعقوبات والتفسير الضيق، دعا مشرعو بعض الدول إلى التدخل بتعديل بعض النصوص القائمة أو وضع نصوص جديدة تتلاءم وتلك الجرائم، ودعا أيضا القضاء إلى التوسع في تفسير النصوص الجنائية السارية.

إذن لا مناص من الاعتراف بأن ظاهرة الجرائم الإلكترونية التي باتت تتخذ أنماطا جديدة وضربا من ضروب الذكاء الإجرامي، تمثل بلا شك تحديا جديا وجديدا في الوقت الحاضر، تجاوزه يتطلب التعرف على هذه التحديات وإبراز جوانبها، بما يعني التشخيص الأمثل للظاهرة ومكافحتها على صعيد التجريم والعقاب من ناحية، وعلى صعيد الملاحقة الإجرائية من ناحية أخرى، وهذا أمر يستلزم: أولا - الانطلاق من الاقتناع بخطورة هذه الظاهرة، ومحاولة التوفيق بين احترام مبدأ السيادة الوطنية لكل دولة في صورته التقليدية، والنزول ولو بقدر أمام ضرورات ومقتضيات التعاون القضائي الدولي الذي بقدر نجاحه تتحقق فعالية كل الجهود والإمكانيات المسخرة للتصدي لظاهرة الجرائم الإلكترونية ومكافحتها، وثانيا – تطوير البنية التشريعية الجنائية بذكاء تشريعي متواصل ودؤوب يسد ثغرات الأنظمة الجنائية على نحو يجعلها قادرة على إخضاع هذه الجرائم لأوصافها ونصوصها، ومواكبة التطورات التي يتوسل بها مرتكبو هذه الجرائم، على أن يتم هذا التطور في إطار القانون وكفالة احترام مبدأ شرعية الجرائم والعقوبات من ناحية، ومبدأ الشرعية الإجرائية من ناحية أخرى، وأن يتكامل هذا التطور في الدور والهدف مع المعاهدات الدولية(فتح الله:2018)

المبحث الثاني: سبل مواجهة الجرائم الإلكترونية

الجزائر كغيرها من الدول استقطبت التكنولوجيا وإستهلكت منتجاتها فقد حملت إليها الجانبين الإيجابي المتمثل في تسهيل وتبسيط الحياة الاجتماعية والسلبي المتمثل في الضرر الناتج عن سوء استعمالها، عندها لبد من إيجاد إيطار قانوني مناسب، بوضع مجموعة مكن الإجراءات ووضع وسائل خاصة تتماشى مع طبيعة الجرائم المتسحدثة أو ما يسمى بالجرائم الإلكترونية (المطلب الأول)، مع تطور تقنيات المعلومات وإهتمام الأنظمة الدولية بموضوع الجرائم المعلوماتية وقعت العديد من الصكوك الدولية من طرف دول أدركت فعلا مدى الخطورة التي تشكلها هذه الجريمة بوصفها من الجرائم العابرة للحدود(شرابشة: 2009،ص. 244) (المطلب الثاني)

المطلب الأول: سبل مواجهة الجريمة الإلكترونية في التشريع الجزائري

حاول المشرع الجزائري خلال السنوات الأخيرة تدارك الفراغ القانوني الذي عرفه مجال الإجرام الالكتروني فقام بتعديل قانون العقوبات بموجب قانون رقم 04-15(قانون رقم 04-15 ،2004).

لقد أدرك المشرع الجزائري جيدا بأن المواجهة الفعالة للإجرام الالكتروني لا تكون فقط بإرساء قواعد قانونية موضوعية ذات طبيعة ردعية، إنما لا بد من مصاحبة هذه القواعد بقواعد أخرى إجرائية وقائية وتحفظية، والتي من شانها ان تتفادى وقوع الجريمة الإلكترونية أو على الأقل الكشف عنها في وقت مبكر يسمح بتدارك مخاطرها. وهو ما استدركه المشرع بتضمين القانون رقم 06-22 المعدل لقانون الإجراءات الجزائية تدابير إجرائية مستحدثة تتعلق بالتحقيق في الجرائم الإلكترونية تتمثل في مراقبة الاتصالات الإلكترونية تسجيلها (برا هيمي: 2016، ص.139)

الفرع الأول: اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

يقصد باعتراض المراسلات اعتراض أو تسجيل أو نسخ المراسلات التي تكون في شكل بيانات قابلة للإنتاج والتوزيع، التخزين، الاستقبال والعرض، التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية في إطار البحث والتحري عن الجريمة وجمع الأدلة عنها (برا هيمي: 2016، ص.139).

الفرع الثاني: جريمتا الدخول والبقاء غير المصرح بهما

نصت المادة ن 394 مكرر من قانون العقوبات على ما يلي: "يعاقب بالحبس من ثالثة أشهر إلى سنة وبغ ارمة من 50000دج إلى 100000دج كل من يدخل أو يبقى عن طريق الغش في كل جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.

تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة ."يستفاد من هذه المادة أن عنه المشرع يقصد بجريمة الدخول غير المصرح به الدخول غير المشروع ـ وهو ما عب بالغش إلى منظومة المعالجة الآلية للمعطيات، أي أن يكون الدخول إلى نظام المعلومات بدون وجه حق، فمناط عدم المشروعية هو انعدام سلطة الفاعل في الدخول إلى هذا النظام مع علمه بذلك .ومن الحالات التي يكون الدخول غير مصرح به في النظام المعلوماتي، دخول الفاعل إلى النظام دون تصريح من المسؤول عن النظام أو مالكه، وقد يكون الفاعل مصرحا له بالدخول إلى جزء من النظام إلا أنه يتجاوز التصريح الممنوح له (شيخ، شيخ: د.ت.، ص.04).

الفرع الثالث: جريمة الاعتداء على المعطيات

نصت على هذا الشكل من الاعتداء المادتين الخامسة والثامنة من الاتفاقية الدولية للإجرام المعلوماتي، في حين أن المشرع الجزائري لم يورد نصا خاصا بالاعتداء العمدي على سير النظام واكتفى بالنص على الاعتداء على المعطيات الموجودة بداخل النظام، ويمكن رد ذلك لكون أن المشرع الجزائري قد اعتبر من خلال الفقرة ج من المادة الثانية وتشمل صورة الاعتداء العمدي على سير النظام فعلين يتمثلان في الآتي :يتمثل الأول منها في فعل التعطيل (العرقلة) والذي يفترض وجود عمل إيجابي، مع العلم أن المشرع لم يشترط أن يتم التعطيل بوسيلة معينة فيستوي أن يتم التعطيل بوسيلة مادية ككسر الأجهزة المادية للنظام أو تحطيم أسطوانة أو عن طريق وسيلة معنوية تتم بموجب الاعتداء على الكيانات المنطقية للنظام كالبرامج والمعطيات وذلك بإتباع إحدى التقنيات المستعملة في هذا المجال مثل إدخال برنامج فيروسي، استخدام قنابل منطقية مؤقتة، جعل النظام يتباطأ في أدائه لوظائفه كما يستوي أن يقترن التعطيل بالعنف أم لا، أما الفعل الثاني يتمثل في الإفساد الذي يتم بكل فعل إلى تعطيل نظام المعالجة الآلية للمعطيات يؤدي إلى جعله غير صالح للاستعمال السليم وذلك من شأنه أن يعطي نتائج غير تلك التي كان من الواجب الحصول عليها(القهوجي: 1999، ص.143).

كخطوة أولى للحكومة الجزائرية لمواجهة ما يعرف بالجريمة الالكترونية، صدر سنة 2009 القانون رقم 09-04 المؤرخ في 05 غشت 2009، والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، إلا أن تجسيد بنوده على أرض الواقع ضعيف إلى حد الساعة، بعدما أهملت الجوانب التقنية الكفيلة بتصنيف هذه الجرائم وتحديد العقوبة المناسبة في حق مرتكبيها، واقتصرت العقوبات في أغلب الأحيان على الغرامة

المالي. ويتضمن القانون 19 مادة موزعة على 6 فصول، أعده نخبة من رجال القانون بمشاركة خبراء ومهنيين مختصين في مجال الإعلام الإلكتروني من كافة القطاعات المعنية، يتضمن القانون أحكاما خاصة بمجال التطبيق وأخرى خاصة بمراقبة الاتصالات الإلكترونية وعددت الحالات التي تسمح باللجوء إلى المراقبة الالكترونية، بالإضافة إلى القواعد الإجرائية المتضمنة تفتيش المنظومات المعلوماتية وكذا حجز المعطيات المعلوماتية التي تكون مفيدة للكشف عن الجرائم الالكترونية، ونص القانون في فصله الخامس على إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، تتولى تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ومساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن هذه الجرائم، وتتكفل أيضا بتبادل المعلومات مع نظيراتها في الخارج، قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم الالكترونية وتحديد مكان تواجدهم، كما أن هذا القانون أكد في فصله الأخير على مبدأ التعاون والمساعدة القضائية الدولية من إطار مبدأ المعاملة بالمثل(حفوظة، غرداين: 2017، ص. 83)

وفي نفس السياق، قال رئيس الكتلة البرلمانية لجبهة العدالة والتنمية لخضر بن خلاف، في تصريح خص به «يومية السلام اليوم » أن «مشكلتنا في قوانين سنّتها الحكومة فيما يخص الجريمة الإلكترونية ولم تطبّقها»، مضيفا أن هناك مراسيم متعلقة بهذا القانون المصادق عليه سنة 2009، لم تصدر لحد الساعة ولأسباب مجهولة، ما جعل حسبه، معالجة القضايا من هذا الشأن تصطدم بشبه فراغ قانوني، ما أدى في عديد الحالات إلى استصدار أحكام وعقوبات تقريبية لا سند لها، كما دعا نفس المتحدث، الحكومة إلى ضرورة مراجعة موقفها تجاه هذا القانون، وقال: لا بد من إيلائه أهمية أكبر في ظل دخول الشارع الجزائري نفق الإدمان، والاعتماد الرهيب على شبكة الإنترنت وما يصاحبها من آليات وخدمات إلكترونية، فضلا عن فتح مجال السمعي البصري، الذي يمكن أن يصطدم بمثل هذه الجرائم مستقبلا، مشددا في السياق ذاته على ضرورة تشريع قوانين جديدة تكرّس العقاب الصارم لكبح مثل هذه الجرائم التي وصفها بالخطيرة والمدمّرة(قاسمي،160 مليار دولار سنويا مكاسب عصابات الجريمة المنظمة عبر الإنترنت).

المطلب الثاني: سبل مواجهة الجريمة الإلكترونية في الأنظمة الدولية

إن مواجهة الجرائم الإلكترونية قد لاقت اهتماماً عالمياً فقد عقدت المؤتمرات والندوات المختلفة، وصدرت من خلالها قوانين وتشريعات تجرم من يقدم على ارتكاب هذه الجرائم، وتعد السويد أول دولة تسن تشريعات خاصة بجرائم الحاسب الآلي ولإنترنت حيث صدر قانون البيانات السويدي عام 1973الذي عالج قضايا الاحتيال عن طريق الحاسب الآلي إضافة إلى شموله فقرات عامة تشمل جرائم الدخول غير المشروع على البيانات الحاسوبية أو تزويرها أو تحويلها أو الحصول غير المشروع عليها، وجاءت الولايات المتحدة الأمريكية بعد السويد حيث شرعت قانونا خاصاً بحماية أنظمة الحاسب الآلي في الفترة من 1986 - 1985م، وفي عام 1985م حدد معهد العدالة القومي خمسة أنواع رئيسة للجرائم المعلوماتية وهي جرائم الحاسب الآلي الداخلية، وجرائم الاستخدام غير المشروع عن بعد، وجرائم التلاعب بالحاسب الآلي، ودعم التعاملات الإجرامية، وسرقة البرامج الجاهزة والمكونات المادية للحاسب، وفي عام 1986م صدر قانوناً تشريعياً عرف فيه جميع المصطلحات الضرورية لتطبيق القانون على الجرائم المعلوماتية كما وضعت المتطلبات الدستورية اللازمة التطبيقية، وعلى أثر ذلك قامت الولايات الداخلية بإصدار تشريعا الخاصة

وللتعامل مع هذه الجرائم، ومن ذلك قانون ولاية تكساس لجرائم الحاسب الآلي، وقد خولت وزارة العدل الأمريكية في عام 2000م خمسة جهات منها مكتب التحقيقات الفيدرالية fb1 للتعامل مع جرائم الحاسب الآلي والأنترنت (عطايا: 2015، ص.390)

ويلي الولايات المتحدة في الاهتمام بمواجهة الجرائم الإلكترونية مباشرة بريطانيا التي تأتي في المرتبة الثالثة بعد السويد وأمريكا فقد أقرت قانون مكافحة التزوير والتزيف عام 1981م الذي شمل في تعاريفه الخاصة بتعريف أداة التزوير وسائط التخزين الحاسوبية المتنوعة أو أي أداة أخرى يتم التسجيل عليها سواء بالطرق التقليدية أو الإلكترونية أو بأي طريقة أخرى

وتحظى كندا بالتصنيف بين هذه الدولة التي أولت مواجهة الجرائم الإلكترونية عناية فائقة حيث عدلت في عام 1985م قانونها الجنائي بحيث شمل قوانين خاصة بجرائم الحاسب الآلي والإنترنت، كما شمل القانون الجديد تجديد عقوبات المخالفات الحاسوبية وجرائم التدمير، أو الدخول غير المشروع لأنظمة الحاسب الآلي، كما وضح فيه صلاحيات جهات التحقيق كما جاء في قانون المنافسة الذي يخول المأمور الضبط القضائي متى ما حصل على أمر قضائي حق تفتيش أنظمة الحاسب الآلي والتعامل معها وضبطها (تمام: دت. ص.200)

وعلى مستوى الدول العربية لم تقم أي دولة عربية بسن قوانين خاصة بجرائم الحاسب الآلي والانترنت، ففي مصر مثلا لا يوجد نظام قانوني خاص بجرائم المعلومات، إلا أن القانون المصري يجتهد بتطبيق قواعد القانون الجنائي التقليدي على الجرائم المعلوماتية والتي تفرض نوعا من الحماية الجنائية ضد الأفعال الشبيهة بالأفعال المكونة لأركان الجريمة المعلوماتية واتخاذ إجراءات فورية تجاه المخالفين في المواقع الالكترونية ويتم تدميرها إذا ثبت إضرارها بمصلحة الأمن القومي أو الآداب العامة. شهدت فعاليات المؤتمر الإقليمي الأول حول الجريمة الإلكترونية، «تحديات تكنولوجيا المعلومات والتنمية الاقتصادية»، العديد من المطالب. دعا عدد من رجال القانون والقضاة وأعضاء النيابة العامة والمتخصصين في مجال مكافحة الجريمة الإلكترونية إلى ضرورة وضع تشريعات وقوانين تعاقب مرتكبي جرائم الإنترنت والمعلومات والبيانات، على شبكة المعلومات الدولية، وتطوير التشريعات الموجودة حاليا بما يواكب التطور العلمي والتكنولوجي، بما يكفل حقوق المواطنين المستخدمين شبكة المعلومات الدولية، وتحدد واجباتهم .أن التأثير المجتمعي الذي يحدثه التقدم التكنولوجي يحتاج إلي تنظيم قانوني، يضع إطارا للعلاقات التي تترتب علي استخدامه بما يكفل حماية الحقوق المترتبة علي هذا الاستعمال، ويحدد الواجبات تجاهها، فلابد للتقدم العلمي والتكنولوجي أن يواكبه تكيف في القواعد القانونية، إذ لا يجوز للقانون أن يقف صامتا مكتوف الأيدي حيال أساليب انتشار هذا التقدم، وحيال القيم التي يروجها ولا يقف دور القانون علي مجرد تنظيم العلاقات المترتبة علي التقدم التكنولوجي بل إنه يجب أن يحمي القيم التي تحيط باستخدام التكنولوجيا، ويحدد المسار الصحيح الذي يجب أن يسلكه التقدم التكنولوجي حتي لا يتخذه المجرمون أداة لتطوير وسائل إجرامهم، بل يكون علي العكس من ذلك وسيلة لمحاربة هذا الإجرام، وهو ما يوجب على القانون أن تمتد نصوصه إلي الأنشطة الجديدة التي تفرزها التكنولوجيا حتى تحدد الجريمة في نصوص منضبطة واضحة، ولا يترك بحثها إلى نصوص قانون العقوبات التقليدي، التي قد تتسم بعدم اليقين القانوني أو لا تتسع لملاحقة الأنماط الجديدة من الإجرام . وقد تتجاوز نتائج هذه الجرائم إلى وقوع جرائم أخرى تهدد

الحق في الحياة والسلامة البدنية، إذا ما أدي العبث في المعلومات إلى تغيير طريق العلاج أو تركيبة الدواء، وقد تؤثر على نطاق الخدمات الإلكترونية وقطاعات التنمية الاقتصادية، وتكنولوجيا المعلومات، الأمر الذي يتطلب إعادة هيكلة قطاع الاتصال، وتدعيم دور الدولة في حماية المستخدمين تكنولوجيا الاتصالات، من خلال إجراءات تتميز بالشفافية الكاملة، خاصة أننا نواجه تحديات جديدة بما يعرف بالجريمة الإلكترونية، التي يجب مكافحتها، لتشجيع الاستثمار وحماية حقوق الملكية الفكرية، الأمر الذي يستلزم ألا يتم بمعزل عن الثوابت التشريعية والقانونية (الأدلة القضائية في امن الفضاء الحاسوبي ،2007) أن التقدم التكنولوجي أفرز أنماطا جديدة من الجريمة، وكذا من المجرمين، فكان للتقدم في العلوم المختلفة أثره عل ى نوعية الجرائم، واستغل المجرم ثمرات هذه العلوم في تطويع المخترعات العلمية الحديثة لخدمة أهدافه الإجرامية، فالمشكلة الرئيسية لا تكمن في استغلال المجرمين الإنترنت، وإنما في عجز أجهزة العدالة عن ملاحقتهم، وعدم ملاحقة القانون لهم ومسايرة التكنولوجيا الجديدة لتشريعاته (سعدون، سلمان، عبد الرحمن: دت، ص.04).

أن مبدأ الشرعية الجنائية يفرض عدم جواز التجريم والعقاب عند انتفاء النص. الأمر الذي يمنع مجازاة مرتكبي السلوك الضار أو الخطر على المجتمع بواسطة الحاسوب (الكمبيوتر) أو الإنترنت؛ طالما أن المشرع الجنائي لم يقم بسن التشريعات اللازمة لإدخال هذا السلوك ضمن دائرة التجريم والعقاب.

يعتبر مبدأ الإقليمية هو المبدأ المهيمن على تطبيق القانون الجنائي من حيث المكان؛ غير أن هذا المبدأ يفقد صلاحيته للتطبيق بالنسبة للجرائم المعلوماتية؛ التي تتجاوز حدود المكان؛ فجرائم الإنترنت عابرة للحدود وانعدام وجود تصور واضح المعالم للقانون والقضاء تجاه جرائم الانترنت لكونها من الجرائم الحديثة وتلك مشكلة أكثر من كونها ظاهرة، ولانعدام وجود تقاليد بشأنها كما هو الشأن في الجرائم الأخرى، ويساعد على ذلك انعدام وجود مركزية وملكية عبر الانترنت و رغم صدور عدد من التشريعات العربية بشأن حماية الملكية الفكرية والصناعية التي تضمنت النص على برامج الحاسب واعتبرتها من ضمن المصنفات المحمية في القانون إلا أنه مكافحة الجرائم المعلوماتية في الدول العربية مازالت بلا غطاء تشريعي يحددها ويجرم كافة صورها(آل سعود: 2007، ص.50)

خاتمة:

وبناء على ما تم دراسته سابقا توصلنا إلى النتائج التالية:

- ✓ الحاسوب هو أساس ارتكاب الجريمة الإلكترونية وأهم دوافع ارتكاب الجريمة هو تحقيق عائد مادي
- ✓ عجز التشريعات عن مكافحة الجريمة الإلكترونية بما فيها التشريع الجزائري يؤدي إلى إفلات مرتكب الجريمة من العقاب
- ✓ أن الإجرام المعلوماتي الذي يقع عن طريق الشبكة العالمية (الأنترنت) له طبيعة من نوع خاص على خلاف الجرائم الأخرى التقليدية، وقد تستمد هذه الطبيعة الخاصة من المجال الذي يمكن أن ترتكب فيه أو من المحل الذي يقع عليه الإعتداء.

وفي ضوء النتائج السابقة التي أظهرتها الدراسة نوصي ببعض التوصيات المتمثلة في:

- ✓ ضرورة الإسراع في إقرار التشريعات المتعلقة بالمعاملات الإلكترونية وبيانات التعريف الشخصية الإلكترونية

- ✓ ضرورة مواصلة تطوير الخبرات والوسائل التقنية اللازمة لدى مكتب مكافحة الجرائم المعلوماتية وحماية الملكية الفكرية لمكافحة الجريمة الإلكترونية واعتماد السياسات والإجراءات والنظم المناسبة لتصدي الجريمة الإلكترونية
- ✓ ضرور اتخاذ التدابير اللازمة لحماية الأجهزة الإلكترونية والبريد الإلكتروني من الفيروسات ومن أي عمليات القرصنة

وأخيرا توعية المجتمع باستخدام كلمة مرور قوية للمواقع الإلكترونية والتأكد من المواقع الرسمية وتجنب المشبوهة منها، وكذا توعيتهم بعدم مسايرة الرسائل العشوائية أو التي تطلب معلومات سرية.

قائمة المراجع:

1) إبراهيم رمضان إبراهيم عطايا (2015): الجريمة الإلكترونية وسبل مواجهتها في الشريعة الإسلامية والأنظمة الدولية، العدد 30 الجزء 2، كلية الشريعة والقانون بطنطا.

2) أحمد حسام طه تمام (د.ت.): الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة.

3) الأدلة القضائية في أمن الفضاء الحاسوبي إحصاءات وزارة الاقتصاد الوطني في مجال الاتصالات حتى ديسمبر، 2007سلطنة عمان، وزارة العدل.

4) إسراء جبريل رشاد مرعي، الجرائم الالكترونية-الأهداف-الأسباب-طرق الجرائم ومعالجتها، مقال منشور على الموقع الالكتروني للمركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، قسم الدراسات المتخصصة، على الرابط http://democraticac.de/?p=35426 :تاريخ الاطلاع 2022/03/30م

5) إسراء جبريل رشاد مرعي، الجرائم الالكترونية- الأهداف-الأسباب-طرق الجرائم ومعالجتها، مقال منشور على الموقع الالكتروني للمركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية، قسم الدراسات المتخصصة، على الرابط http://democraticac.de/?p=35426 :تاريخ الاطلاع2022/03/30م.

6) براهيمي جمـال(دت.): مكافحة الجرائم الإلكترونية في التشريع الجزائري، المجلة النقدية، كلية الحقوق والعلوم السياسية، جامعة مولو د معمري، تيزي وزو،ب.س

7) بولحية شهرزاد، خلوفي رشيد(2019): تحديات الجريمة الإلكترونية في الجزائر، مجلة الاستاذ الباحث للدارسات القانونية والسياسية - المجلد 04 - العدد 02، جامعة الجزائر1.

8) حفوظة الأمير عبد القادر، غرداين حسام(2017): مخبر الحوكمة العمومية والاقتصاد الاجتماعي جامعة أبو بكر بلقايد تلمسان. كتاب أعمال ملتقى آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري المنعقد في الجزائري العاصمة يوم 29 مارس 2017، اطلع عليه يوم 2022/04/02م، على الموقع https://www.politics-dz.com على الساعة 15:30 مساءا.

9) الحيسناوي علي جبار(2009): جرائم الحاسوب والانترنيت، دار اليازوري العلمية للنشر والتوزيع، الاسكندرية.

10) دمان ذبيح عماد، بهلول سمية(2020): الأليات العقابية لمكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة الحقوق والعلوم السياسية الصادرة عن جامعة عباس لغرور، خنشلة، العدد 13.

11) رستم هشام(2000): الجرائم المعلوماتية: أصول التحقيق الجنائي الفني واقتراح بإنشاء آلية عربية موحدة للتدريب التخصصي، بحوث مؤتمر القانون والكمبيوتر والإنترنت، دولة الإمارات العربية المتحدة.

12) سمير سعدون مصطفى، محمود خضر سلمان (دت.): حسن كريم عبد الرحمن، الجريمة الإلكترونية عبر الانترنيت أثرها وسبل مواجهتها.

13) شيخ سناء، شيخ محمد زكرياء، (دت.): مكافحة الجرائم الإلكترونية في القانون الجزائري، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم،

14) علي عبد القادر القهوجي(1999): الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، مصر.

15) قاسمي.أ،160 مليار دولار سنويا مكاسب عصابات الجريمة المنظمة عبر الإنترنت، مقال منشور على موقع يومية السلام اليوم، بتاريخ 2014/01/25، على الرابطhttp://essalamonline.com/ara/permalink/32212.html :.، تاريخ 2022/04/02م، على الساعة 15:30 مساءا.

16) قانون رقم 04-15 مؤرخ في 2004/11/10 يعدل ويتمم الامر رقم 66 -156، يتضمن قانون العقوبات، جريدة رسمية عدد 71، صادر بتاريخ 2004/11/10، معدل ومتمم.

17) كامل فريد السالك (21-23أكتوبر، 2000): الجريمة الالكترونية، محاضرة ألقيت في ندوة التنمية ومجتمع المعلوماتية الجمعية السورية للمعلوماتية، حلب، سورية

18) ليندة شرابشة (2009): السياسة الدولية والإقليمية في مجال مكافحة الجريمة الإلكترونية، الإتجاهات الدولية في مكافحة الجريمة الإلكترونية، مجلة دراسات وأبحاث الصادرة عن جامعة زيان عاشور بالجلفة، العدد 01 المجلد01

19) محمد خليفة(2009): خصوصية الجريمة الإلكترونية وجهود المشرع الجزائري في موجهتها، مقال بمجلة دراسات وأبحاث الصادرة عن جامعة زيان عاشور بالجلفة الجزائر، العدد01، المجلد 01 .

20) محمود رجب فتح الله(2018): التحديات العملية للجرائم الالكترونية، الحوار المتمدن-العدد: 6012 - 2018 / 10 / 3، مقال منشور على الموقع https://www.ahewar.org اطلع عليه يوم 2022/04/02م، على الساعة 15:42.

21) موضي بنت عبد الله آل سعود(2007): دور مراكز المعلومات في دعم القرار السياسي ورقة عمل مقدمة إلى مؤتمر تقنية المعلومات والأمن الوطني الرياض.

الإطار القانوني لمكافحة الجريمة المعلوماتية في التشريع الجزائري

The legal framework for the fighting computer crime in Algerian legislation

د. محمد السعيد زناتي/ جامعة باتنة 1 /الجزائر
Dr.Mohammed Said ZENATI/ University of Batna1/ Algeria
د.يمينة جواج/ جامعة عبد الحميد بن باديس، مستغانم/ الجزائر
Dr.Yamina DJouaJ /University Abdelhamid ben badis, Mostaghanem/ Algeria

ملخص الدراسة:

إن التطورات والثورات المعرفية والعلمية التي شهدتها مختلف مجالات العلوم، خاصة ما تعلق منها بالجانب التكنولوجي ووسائل الإتصال الحديث السلكية منها واللاسلكية وكذا ما يتصل بالشبكة العنكبوتية العالمية، على اعتبار أن هذه الوسائل الحديثة التي عرفتها المجتمعات لم تكن متداولة فيما سبق، لذا انجر عن استخدامها مساس بحقوق وحريات الآخرين وهو ما يشكل جريمة في مفهوم القانون الجنائي.

غير أن حداثة هذه الوسائل وقلة استخدامها سابقا لم يكن يطرح إشكالا كبيرا لدى مختلف المجتمعات أو الدول، أما في هذا العصر الحديث ونظرا لتشعب الاتصالات وتعقد المعاملات بين الأفراد والاعتماد اليومي والكلي علي مثل هذه الوسائل في الحياة اليومية، منها وسائل الاتصال الحديث وكذا مختلف الشبكات علي غرار الإنترنت وكل ما يتعلق منها بالمعلوماتية أو ما يطلق عليه الفضاء السبراني، حتم علي الدول المجتمعات تنظيم هذا المجال وتأطيره وتحديد الأفعال والتصرفات المسموح منها والممنوع بموجب قوانين وأنظمة واتفاقات إقليمية ودولية.

حيث أحاول في هذه الورقة البحثية تسليط الضوء علي تعامل المشرع الجزائري مع هذه الظاهرة وكيف عالجها، على غرار التشريعات والقوانين الدولية الأخرى، على اعتبار أنه لم تكن هناك سوابق تشريعية في هذا المجال في الجزائر إضافة الي خصوصية هذه الأفعال وتميزها عن الجرائم العادية، وذلك من خلال الإجابة على الإشكالية التالية: ما هي الجريمة المعلوماتية حسب التشريع الجزائري؟ وكيف واجه المشرع الجزائري هذه الجرائم الحديثة تشريعيا؟ خاصة في ظل التعديل الأخير لقانون العقوبات الجزائري.

الكلمات المفتاحية: الجريمة الالكترونية، تكنولوجيا الإعلام والاتصال، السياسة الجنائية، الانترنت، الفضاء السبراني، الجريمة المعلوماتية، المشرع الجزائري.

Abstract:

The developments and scientific and scientific revolutions witnessed in various fields of science, especially those related to the technological aspect and the modern means of communication, both wired and wireless, as well as related to the World Wide Web, considering that these modern methods known by the societies have not been discussed in the past. Prejudicial to the rights and freedoms of others, which constituted a crime in the sense of criminal law.

However, in modern times, due to the complexity of communication and the complexity of transactions between individuals and the daily and total dependence on such means in daily life, including modern means of communication as well as various networks Like the Internet and everything related to informatics or so-called cyberspace, it is imperative for the member states

to regulate and regulate this area and to identify the acts and behaviors permitted and prohibited by regional and international laws, regulations and agreements.

In this paper, I try to highlight the Algerian legislator's treatment of this phenomenon and how he treated it, in line with other international laws and laws, considering that there were no legislative precedents in this field in Algeria, in addition to the specificity of these acts and their distinction from ordinary crimes. During the answer to the following problem: What is informational crime according to Algerian legislation? And how did the Algerian legislator deal with these modern crimes legislatively? Especially in light of the recent amendment to the Algerian Penal Code.

Keywords: Cyber Crime , Information and Communication Technology , Criminal Policy, Internet , Cyberspace , Information Crime , Algerian Legislator.

مقدمة:

إن التطورات والثورات المعرفية والعلمية التي شهدتها مختلف مجالات العلوم، خاصة ما تعلق منها بالجانب التكنولوجي ووسائل الاتصال الحديث السلكية منها واللاسلكية على غرار اجهزة الكمبيوتر والهواتف النقالة الذكية واللوحات الذكية....الخ، وكذا كل ما يتصل بالشبكة العنكبوتية العالمية من برامج وكيفيات للاتصالات مثل البريد الإلكتروني ومواقع التواصل الاجتماعي (فيس بوك، تويتر...الخ)، على اعتبار أن هذه الوسائل الحديثة التي عرفتها المجتمعات لم تكن متداولة فيما سبق، لذا انجر عن استخدامها والتعامل بها سواء بشكل حسن أو سيء النية مساس بحقوق وحريات الآخرين وهو ما يشكل جريمة في مفهوم القانون الجنائي.

غير أن حداثة هذه الوسائل وقلة استخدامها سابقا لم يكن يطرح إشكالا كبيرا لدى مختلف المجتمعات أو الدول، أما في الآونة الأخيرة ونظرا لتشعب الاتصالات وتعقد المعاملات بين الأفراد والاعتماد اليومي والكلي على مثل هذه الوسائل في الحياة اليومية، منها وسائل الاتصال الحديث وكذا مختلف الشبكات وكل ما يتعلق منها بالمعلوماتية أو ما يطلق عليه الفضاء السبراني، حتم على الدول المجتمعات تنظيم هذا المجال و تأطيره وتحديد الأفعال و التصرفات المسموح منها والممنوع بموجب قوانين وأنظمة واتفاقيات إقليمية ودولية.

حاول المشرع الجزائري علي غرار بقية التشريعات الوطنية معالجو هذه الظاهرة وتنظيمها بموجب قوانين منها ما هو خاص بما يتعلق بجانب الاتصالات كالقانون رقم 09-04 المؤرخ في في 05 اوت 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ومنها ما هو تحديث ومواكبة للقانون الجنائي الجزائري (قانون العقوبات وقانون الإجراءات الجزائية) كالقانون رقم 16-02 المؤرخ في 19 جوان 2016 المتمم للأمر رقم 66-156 المتضمن قانون العقوبات.

قد يرى البعض ان تنظيم هذا النوع من الجرائم وتأطيرها في الجزائر كان متأخرا مقارنة بالتشريعات العالمية الاخرى، غير ان المشرع الجزائري كيف قوانينه الجنائية تماشيا مع التطورات الدولية في هذا المجال وما انبثق عنها من معاهدات واتفاقيات دولية واقليمية في اطار مكافحة الجريمة المعلوماتية، حيث سنحاول في هذه الورقة البحثية تسليط الضوء علي تعامل المشرع الجزائري مع هذه الظاهرة وكيف عالجها، على غرار التشريعات والقوانين الدولية

الأخرى، على اعتبار أنه لم تكن هناك سوابق تشريعية في هذا المجال في الجزائر إضافة إلىخصوصية هذه الأفعال وتميزها عن الجرائم العادية، وذلك من خلال الإجابة علي الإشكالية التالية: ما هي الجريمة المعلوماتية حسب التشريع الجزائري؟ وكيف عالج المشرع الجزائري هذه الجرائم الحديثة مقارنة مع الاتفاقيات الدولية؟ وذلك ضمن خطة منهجية مكونة من محورين رئيسيين، نتناول في المحور الأول الجناب المفاهيمي للجريمة المعلوماتية عموما وفي التشريع الجزائري خصوصا، وفي المحور الثاني نتطرق إلى أهم الاتفاقيات الدولية والإقليمية التي تناولت موضوع الجرائم المعلوماتية، وكيف تأثر بها المشرع الجزائري.

المحور الأول: الجانب المفاهيمي للجريمة المعلوماتية

في هذا المحور المتضمن الجريمة المعلوماتية في التشريع الجزائري، نتطرق الي ماهية هذه الجريمة أولا من خلال التعريف والخصائص في فرع اول، ثم نتطرق الي القوانين التي سنها المشرع الجزائري لمكافحة هذا النوع من الإجرام في فرع ثان، وفي الفرع الثالث نتطرق الآليات الميدانية التي اعتمدها المشرع الجزائري في محاربة الإجرام ألمعلوماتي.

الفرع الأول: تعريف الجريمة المعلوماتية وخصائصها

في هذا الفرع نتناول أولا تعريف الجريمة المعلوماتية، ثم ثانيا نتطرق إلى خصائص هذا النوع من الجرائم.

أولا: تعريف الجريمة المعلوماتية:

تعددت الآراء بشأن تعريف الجريمة المعلوماتية، كل رأي تبنى مفهوما بالنظر إلى الزاوية التي رآها، فهناك جانب من الفقه عرفها من زاوية فنية، وأخرى قانونية، وهناك جانب آخر يرى تعريفها بالنظر إلى وسيلة ارتكابها أو موضوعها أو حسب توافر المعرفة بتقنية المعلومات لدى مرتكبها أو استنادا لمعايير أخرى حسب القائلين بها، وهذا ما حدا بالأمم المتحدة – مدونتها بشأن الجريمة المعلوماتية – إلى عدم التوصل لتعريف متفق عليه دوليا.

ولكن ورغم صعوبة وضع تعريف لظاهرة هذه الجريمة وحصرها في مجال ضيق، إلا أن مكتب تقييم التقنية في الولايات المتحدة الأمريكية عرفها من خلال تعريف الحاسب الآلي بأنها " الجرائم التي تقوم فيها بيانات الحاسب الآلي والبرامج المعلوماتية بدور رئيسي "، كما عرفت أيضا بأنها " نشاط جنائي يمثل اعتداءً على برامج وبيانات الحاسب الإلكتروني "، وعرفت أيضا بأنها " كل استخدام في صورة فعل أو امتناع غير مشروع للتقنية المعلوماتية، ويهدف إلى الاعتداء على أي مصلحة مشروعة، سواء أكانت مادية أو معنوية "(المطردي،2012)

ويرجح الأستاذ مفتاح بوبكر المطردي المستشار بالمحكمة العليا الليبية التعريف القائل بأن الجريمة الإلكترونية هي عبارة عن أفعال غير مشروعة، يكون الحاسب الآلي محلا لها أو وسيلة لارتكابها. (المطردي،2012)

ورغم الفارق بين ميدان جرائم الحاسب الآلي وميدان جرائم الإنترنت، فبينما تتحقق الأولى بالاعتداء على مجموعة الأدوات المكونة للحاسب وبرامجه والمعلومات المخزنة به، فإن جرائم الإنترنت تتحقق بنقل المعلومات والبيانات بين أجهزة الحاسب عبر خطوط الهاتف أو الشبكات الفضائية، إلا أن الواقع التقني أدى إلى اندماج الميدانين (الحوسبة والاتصالات) وظهور مصطلح (Cybercrime)، ولكن هذا الاندماج لم يثن جانب من الفقه عن تقسيم تلك الجرائم إلى أربعة أنواع تبعا للمفهوم الذي يتبناه كل منهم(المطردي،2012):

1.جرائم الحاسب الآلي : ويقصد بها الأفعال التي تشكل اعتداء على أجهزة الحاسب الآلي، سواء على مكوناته المادية (Hardware) كوحدات الإدخال والإخراج، ووسائل التخزين المرنة والصلبة أو الشاشة والطابعة أو على مكوناته المعنوية (Software data bases) كالبيانات والمعلومات المخزنة داخل الحاسب الآلي، وعلى ذلك فإن جرائم الحاسب تختلف حسب طبيعة الشيء محل الاعتداء، فالاعتداء أحياناً يقع على أدوات وآلات الحاسب الآلي وأحياناً أخرى يقع على برامج ومعلومات داخل الحاسب الآلي، وفي كلتا الحالتين فإن الحاسب ومحتوياته هو هدف السلوك الإجرامي.

2. جرائم الإنترنت: وهي كل فعل غير مشروع يقع على المواقع بقصد تعطيلها أو تشويهها أو تعديلها والدخول غير المشروع لمواضع غير مصرح بالدخول إليها، واستخدام عناوين غير حقيقية للدخول في شبكة المعلومات واقتحام الشبكات ونقل الفيروسات، وإرسال الرسائل بكافة أنواعها عبر البريد الإلكتروني كالمساسة بكرامة الأشخاص أو المستهدفة ترويج مواد أو أفعال غير مشروعة.

3.جرائم شبكة المعلومات: وهي كل فعل غير مشروع يقع على وثيقة أو نص موجود بالشبكة ومن أمثلته انتهاك الملكية الفكرية للبرامج والإنتاج الفني والأدبي والعلم، وارتكاب هذه الجرائم عبر شبكة المعلومات يتطلب اتصال بالأنترنت واستخدام الحاسب الآلي للوصول إلى قواعد البيانات للاطلاع عليها أو تغييرها.

4.الجرائم المتعلقة باستخدام الحاسب الآلي: وهي الجرائم التي يكون الحاسب الآلي وسيلة لارتكابها كالاحتيال والتزوير بواسطة الحاسب، ولقد كانت هذه الجريمة مندمجة في جرائم الحاسب الآلي وتعتبر جزء منها، إذ كان مصطلح جرائم الحاسب يستخدم للدلالة على كل صور جرائم الحاسب الآلي سواء أكان الحاسب هدفا صريحاً للفعل الإجرامي أو وسيلة له، إلا أنه بعد اتساع جرائم الحاسب وولادة جرائم الانترنت أصبح مصطلح الجرائم المتعلقة بالحاسب الآلي يعتبر من الجرائم التي يكون الحاسب وسيلة لارتكابها، أي أنها كل فعل غير مشروع يستخدم الحاسب الآلي في ارتكابه كأداة رئيسية.

وفي المؤتمر العاشر لهيئة الأمم المتحدة لمنع الجريمة ومعاقبة المجرمين المنعقد في فينا خلال الفترة من 10 الي 17 افريل 2000، تم تبني تعريفا جامعا للجريمة المعلوماتية بأنها اية جريمة يمكن ارتكابها بواسطة نظام حاسوبي او شبكة حاسوبية أو داخل نظام حاسوب، وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية. (الشوابكة، 2004، ص.10)

وبدوره الأستاذ محمد امين الشوابكة يعرف الجريمة المعلوماتية على أنها كل اعتداء يقع علي نظم الحاسب الآلي وشبكاته او بواسطتها. (الشوابكة، 2004، ص.10)

وقد عرف جريمة الكمبيوتر خبراء متخصصون من بلجيكا في معرض ردهم على استبيان منظمة التعاون الاقتصادي والتنمية OECD، بأنها " كل فعل أو امتناع من شانه الاعتداء على الأموال المادية او المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية " (عرب، 2002)

والتعريف البلجيكي السالف، متبنى من قبل العديد من الفقهاء والدارسين بوصفه لديهم أفضل التعريفات لأن هذا التعريف واسع يتيح الاحاطة الشاملة قدر الامكان بظاهرة جرائم التقنية، ولأن التعريف المذكور يعبر عن الطابع

التقني أو المميز الذي تنطوي تحته أبرز صورها، ولأنه أخيرا يتيح امكانية التعامل مع التطورات المستقبلية التقنية. (عرب، 2002)

وهناك من يرى انها جرائم الحاسب الآلي والأنترنات ويعرفها بانها الجريمة التي يتم ارتكابها إذا قام شخص ما باستخدام معرفته بالحاسب الآلي بعمل غير قانوني. (عياد، 2006، ص.12)

أما المشرع الجزائري فقد عرف هذا النوع من الجرائم في الفقرة الأولي من المادة الثانية من القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، حيث أطلق عليها مصطلح الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وعرفها (بأنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب او يسهل ارتكابها عن طريق منظومة معلوماتية او نظام للاتصالات الالكترونية).(القانون 04-09)

وبالتمعن في تعريف المشرع الجزائري علي غرار التعاريف الأخرى التي سبق التعرض إليها يتضح لنا أن المشرع الجزائري أعطي مفهوما موسعا لهذا النوع من الجرائم، فبالرغم من تحديده لمجالها من خلال كونها متصلة بتكنولوجيات الإعلام والاتصال إلا أنه ترك فيما بعد المجال وسعا لتضم اليها أي نوع من الجرائم التي قد يسفر عنها التطور التكنولوجي، حيث نصت المادة علي العبارة التالية (أو أي جريمة اخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية او نظام للاتصالات الالكترونية)، ونحن نعلم أن هذا الميدان او الحقل يشهد تطورا وتناميا متسارعا.

ثانيا: خصائص الجريمة المعلوماتية:

تتميز الجريمة المعلوماتية بطبيعة خاصة تميزها عن غيرها من الجرائم التقليدية وذلك نتيجة لارتباطها بتقنية المعلومات والحاسب الآلي مع ما يتمتع به من تقنية عالية وقد كان لظهور شبكة الإنترنت في إضفاء شكل جديد للجريمة المعلوماتية هو الطبيعة الدولية أو متعددة الحدود (مزيود، 2014) حيث سنبين أهم الصفات المشتركة بين الجريمة المعلوماتية وغيرها من الجرائم العادية ثم نتعرض لما تنفرد به من خصائص لوحدها:

1.خصائص تشترك فيها مع بعض الجرائم:

أ.خطورة الجرائم المعلوماتية: وذلك لمساسها بالإنسان في فكره وحياته، وتمس المؤسسات في اقتصادها والبلاد في أمنها القومي والسياسي والاقتصادي، ومن شأن ذلك أن يضفي أبعادا خطيرة غير مسبوقة على حجم الإضرار والخسائر التي تنجم عن ارتكاب هذه الجرائم على مختلف القطاعات والمعاملات. (مزيود، 2014)

ب. الطبيعة المتعدية الحدود: من أهم خصائص التي تميز الجريمة المعلوماتية هي تخطيها للحدود الجغرافية، ذلك ان الشبكات المعلوماتية جعلت من العالم قرية صغيرة ومحت كل الحدود الوهمية بين الدول.

وقد أثارت الطبيعة الدولية للجرائم المعلوماتية تساؤلا مهما يتعلق بتحديد الدولة التي يختص قضاؤها بملاحقة الجريمة، أم تلك التي أضرت مصالحها نتيجة لهذا التلاعب، كما أثرت هذه الطبيعة أيضا الشكوك حول مدى فاعلية القوانين القائمة في التعامل مع الجريمة المعلوماتية وبصفة خاص فيما يتعلق بجمع وقبول الأدلة.

2.خصائص تنفرد بها الجريمة المعلوماتية عن الجرائم الأخرى: تختلف الجريمة المعلوماتية عن باقي أنواع الجرائم في:

ا. تتطلب لارتكابها وجود كمبيوتر ومعرفة تقنية باستخدامه: حيث يعتبر الاستعانة بجهاز الكمبيوتر أساسا لارتكاب الجريمة المعلوماتية وليس سرقة الجهاز أو إتلافه لأنه يدخل في نطاق الاعتداء أو سرقة الأموال المادية المنقولة، وترتكب الجريمة بتدمير برامج) الكمبيوتر أو سرقتها أو العبث بالبيانات أو المعلومات المخزنة.

كما تعتمد هذه الجرائم على قمة الذكاء في ارتكابها ويصعب على المحقق التقليدي التعامل مع هذه الجرائم، إذ يصعب عليه متابعة الجرائم المعلوماتية والكشف عنها وإقامة الدليل عليها، فهي جرائم تتسم بالغموض وإثباتها بالصعوبة بمكان والتحقيق فيها يختلف عن التحقيق في الجرائم التقليدية، كما انه كلما تقدمت المعرفة التقنية كلما زادت احتمالية توظيف هذه المعارف بشكل غير مشروع وزيادة خطورة الجرائم المعلوماتية. (مزيود، 2014)

ب. صعوبة اكتشافها وإثباته: تتسم الجريمة المعلوماتية بأنها علاوة على صعوبة الاحتفاظ الفني بأثارها إن وجدت، لا تترك أثرا بعد ارتكابها فليس هناك أموال مادية منقولة تم اختلاسها وإنما هي أرقام تتغير في السجلات، كما أن معظم الجرائم المعلوماتية تم اكتشافها بالمصادفة وبعد مرور وقت طويل إضافة انه لا يتم في الغالب الإبلاغ عن الجرائم المعلوماتية أما لعدم اكتشافها من طرف الضحية أو خوفا من التشهير به لذلك ما يرتكب فعلا من جرائم معلوماتية اكبر بكثير ما يصرح به.

ج. خصوصية المجرم المعلوماتي عن غيره من المجرمين: يتصف مرتكبو الجرائم المعلوماتية بعدة صفات تميزهم عن غيرهم من المتورطين في أشكال الإجرام الأخرى والمتمثلة في: المهارة، المعرفة، الوسيلة، السلطة: فيقصد بها الحقوق أو المزايا التي يتمتع بها المجرم المعلوماتي والتي تمكنه من ارتكاب جريمته كامتلاك الشفرة الخاصة بالدخول الي النظام. (مزيود، 2014)

الفرع الثاني: القوانين التي سنها المشرع الجزائري لمكافحة الجريمة المعلوماتية

جدير بالذكر الإشارة الي ان المجتمع الجزائري لم يعرف هذا النوع من الجرائم في السابق ولم يسن المشرع الجزائري لها قوانين خاصة إلا حديثا منذ سنة 2009 من خلال سنه للقانون رقم 09-04 المؤرخ في 05 اوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، غير ان هذا لا يعني عدم وجود نصوص قانونية متفرقة تجرم وتعاقب على الإجرام المعلوماتي.

حيث صدر اول نص تشريعي جزائري يعاقب على الإجرام المعلوماتي في 26 جوان 2001، من خلال تعديل قانون العقوبات الجزائري بموجب القانون 01-09 المؤرخ في 26 جوان 2001 المتضمن تعديل قانون العقوبات الجزائري، (ج.ر،2001) ضمن المواد 144 مكرر و 146 مكرر و 144 مكرر1، و 144 مكرر2، و 146، من قانون العقوبات الجزائري والمتعلقة بجريمة القذف والسب التي تطال رئيس الجمهورية او الدين الاسلامي او الهيئات العمومية. (نمديلي، 2017، ص96)

وفي تعديل آخر لقانون العقوبات الجزائري بموجب القانون 04-15 المؤرخ 10 نوفمبر 2004، وفي الفصل السابع مكرر المعنون بـ: المساس بأنظمة المعالجة الآلية للمعطيات تضمن المواد من 394 مكرر الي 394 مكرر 7،(ج.ر، 2004) حيث نص المشرع الجزائري ضمن هذه المواد علي التجريم والمعاقبة للأفعال المخالفة للقانون والتي تشكل مساسا بأنظمة المعالجة الآلية للمعطيات. (نمديلي، 2017، ص97)

وبموجب القانون رقم 09-04 المؤرخ في 05 اوت 2009، المتضمن تعديل قانون العقوبات الجزائري، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والذي يعتبر او نص تشريعي جزائري خاص بمكافحة الجريمة المعلوماتية والذي تضمن 19 مادة، و 06 فصول تناولت الهدف من القانون والتعريف بالمصطلحات الخاصة بهذا القانون، مجال التطبيق، مراقبة الاتصالات، القواعد الإجرائية لتفتيش المنظومات المعلوماتية ...الخ.

وفي سنة 2016 وفي اطار تكيف المشرع الجزائري وتحيين منظومته التشريعية مع التطورات القانونية الدولية، خاصة ما تعلق منها بمكافحة جرائم الإرهاب التي عرفت هي كذلك تطورا مطردا وأصبح مجرمو الإرهاب يعتمدون في تنفيذ جرائمهم على تكنولوجيات الاعلام والاتصال، ذلك ما حدا بالمشرع الجزائري الي تعديل قانون العقوبات الجزائري بموجب القانون رقم 16-02 المؤرخ في 19 جوان 2016، (ج.ر، 2016) الذي تضمن 03 مواد نصت علي اضافة المواد 87 مكرر 11، و 87 مكرر12، و 394 مكرر8 لقانون العقوبات الجزائري.

الفرع الثالث: الآليات التي اعتمدها المشرع الجزائري لمكافحة الجريمة المعلوماتية

بعد أن عرجنا في الفرع السابق الي الترسانة القانونية التي اعتمدها المشرع الجزائري لمواجهة الجريمة المعلوماتية، نتطرق في هذا الفرع الي الآليات والهيئات التي استحدثها المشرع الجزائري في سبيل مكافحة هذا النوع من الاجرام وذلك كما يلي:

1. الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال: وقد استحدثها المشرع بموجب القانون رقم 09-04 المؤرخ في 05 اوت 2009، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وتم تنظيم عملها بموجب المرسوم الرئاسي رقم 15-261 المؤرخ 08 اكتوبر 2015،(ج.ر، 2015) ومن مهامها تفعيل التعاون القضائي والأمني الدولي وإدارة وتنسيق العمليات الوقاية والمساعدة التقنية للجهات القضائية والامنية مع إمكانية تكليفها بالقيام بخبرات قضائية في حال الاعتداءات علي منظومة معلوماتية على نحو يهدد مؤسسات الدولة او الدفاع الوطني او المصالح الاستراتيجية للاقتصاد الوطني.(عاقلي، 2017)

2.الهيئات القضائية الجزائية المتخصصة: ويقصد بها الاقطاب الجزائية المتخصصة المنشاة بموجب القانون 04-14 المؤرخ في 10 نوفمبر 2004، (ج.ر، 2004) وتختص هذه الجهات القضائية بموجب المواد 37-40-329 من قانون الإجراءات الجزائية بالنظر في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، بالإضافة الي الصلاحيات الأخرى الممنوحة للجهات القضائية او للضبطية القضائية في إطار معالجة مثل هذه الجرائم. (بعرة،2016)

3.جهازي الأمن الوطني والدرك الوطني: حيث سعت المديرية العامة للأمن الوطني وكذا جهاز الدرك الوطني التي إنشاء فرق خاصة لمكافحة الجرائم المعلوماتية، وكذا تكوين عناصر متخصصة في هذا المجال سواء على المستوى الداخلي او المستوى الخارجي، بالإضافة إلى يتوفر عليه هاذين الجهازين من مخبرين علميين للشرطة العلمية والتقنية يتوفرون على أحدث الأجهزة ذات تكنولوجيا متطورة لكشف هذا النوع من الإجرام. (حملاوي، 2015)

المحور الثاني: الاتفاقيات الدولية والإقليمية لمكافحة الجريمة المعلوماتية ومدى تأثر المشرع الجزائري بها.

في هذا المحور نتناول أهم الاتفاقيات والمعاهدات الدولية والإقليمية التي تناولت موضوع مكافحة الجرائم المعلوماتية، ومدى تأثر المشرع الجزائري بها، باعتبار أن أغلب التشريعات الوطنية تتأثر دائما بالتطورات الدولية الحاصلة في أي ميدان من التشريع وبالخصوص المجال المعلوماتي وما يتبع ذلك من ظهور جرائم متصلة بهذا التطور، وذلك ضمن ثلاثة فروع نتطرق في الفرع الأول إلى أهم الاتفاقيات الدولية، وفي الفرع الثاني الي الاتفاقيات العربية كنموذج عن الاتفاقيات الإقليمية لمكافحة الإجرام المعلوماتي، وفي الفرع الثالث نبين مدى تأثير هذه الاتفاقيات علي التطور التشريعي الجزائري في مجال مكافحة الجريمة المعلوماتية.

الفرع الأول: الاتفاقيات الدولية في مجال مكافحة الجريمة المعلوماتية

نحاول في هذا الفرع أن نوجز أهم الاتفاقيات الدولية التي أبرمت في إطار مكافحة الجريمة المعلوماتية والتي كان لها الأثر البارز على مختلف التشريعات الوطنية الداخلية وبالخصوص التشريع الجزائري.

القرار الصادر عن مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة السجناء هافانا 1990 بشأن الجرائم ذات الصلة بالكمبيوتر:

يعد هذا القرار من الجهود التي بذلتها الأمم المتحدة حيث عقد هذا المؤتمر في هافانا سنة 1990 قد حث في قراره المتعلق بالجرائم ذات الصلة بالكمبيوتر الدول الأعضاء:

- ✓ تكثف جهودها لمكافحة إساءة استعمال هذا الجهاز وبتجريم تلك الأفعال جنائيا اتخاذ الإجراءات التالية متى دعت الضرورة لذلك:
- ✓ ضمان أن الجزاءات والقوانين الراهنة بشأن سلطات التحقيق الأدلة في الإجراءات القضائية تنطبق على نحو ملائم إدخال تغييرات مناسبة عليها إذا دعت الضرورة لذلك.
- ✓ النص على جرائم وجزاءات إجراءات تتعلق بالتحقيق الأدلة حيث تدعو الضرورة للتصدي لهذا الشكل الجديد والمعقد من أشكال النشاط الإجرامي في حالة عدم وجود قوانين تنطبق على نحو ملائم.

كما حث أيضا الدول الأعضاء على مضاعفة الأنشطة التي تبذلها على الصعيد الدولي من أجل مكافحة الجرائم المتصلة بالكمبيوتر بما في ذلك دخولها كأطراف في المعاهدات المتعلقة بتسليم المجرمين وتبادل المساعدة في المسائل الخاصة المرتبطة بهذه الجريمة، نصح هذا القرار الدول الأعضاء بالعمل على أن تكون تشريعاتها ذات العلاقة بتسليم المجرمين وتبادل المساعدة في المسائل الجنائية تنطبق بكل تام على الأشكال الجديدة للإجرام مثل الجرائم الالكترونية، وأن تتخذ خطوات محددة نحو تحقيق هذا الهدف.

ب. مقررات وتوصيات المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات بشأن جرائم الكمبيوتر:

انعقد هذا المؤتمر سنة 1994 بالبرازيل حيث نص على الأفعال المجرمة التي يمكن اعتبارها جرائم معلوماتية كالاحتيال، الغش المرتبط بالكمبيوتر من خلال إتلاف محو المعطيات، أيضا ما يعرف بالتزوير المعلوماتي يشمل إتلاف محو البرامج

والبيانات وتعطيل وظائف الكمبيوتر ونظام الاتصالات(الشبكات) ، أو الدخول غير المصرح به عن طريق انتهاك إجراءات الأمن.

أما من الناحية الإجرائية فان القرار الصادر عن المؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات تضمن جملة من القواعد الإجرائية في بيئة الجرائم المعلوماتية تتمثل فيما يلي:

- ✓ القيام بإجراء التفتيش والضبط في بيئة تكنولوجيا المعلومات، وأيضا تفتيش شبكات الحاسب الآلي.
- ✓ التعاون الفعال بين المجني عليهم والشهود كذا مستخدمي المعلومات من أجل إتاحة استخدام المعلومات للأغراض القضائية.
- ✓ اعتراض الاتصالات داخل نظام الحاسب الآلي ذاته وممارسة الرقابة عليها.

ج. اتفاقية برن الدولية لحماية المصنفات الأدبية الفنية:

بهدف حماية حقوق المؤلفين على مصنفاتهم الأدبية بأكثر الطرق فعالية تم إبرام اتفاقية برن الدولية في 9 سبتمبر 1886، المكملة بباريس في ماي1896 ، والمعدلة في برلين في 13 سبتمبر1908 والمكملة ببرن في 20 مارس1914 ، والمعدلة بروما في جوان 1928، بروكسل سنة1948 ، واستوكهولم في جويلية 1967 وباريس في جويلية 1971، حيث تشكل الدول الأطراف في هذه الاتفاقية اتحادا لحماية حقوق المؤلفين على مصنفاتهم الأدبية الفنية.

وبموجب اتفاقية برن الدولية تتمتع برامج الحاسب الآلي "الكمبيوتر "سواء كانت بلغة المصدر أو بلغة الآلة بالحماية باعتبارها أعمالا أدبية وفقا لما جاء فيها إضافة إلى اتفاقية " TRIPIS " المتعلقة بالجوانب المتصلة بالتجارة الدولية حيث تسعى الدول الأطراف في الاتفاقية إلى تشجيع الحماية الفعالة والملائمة لحقوق الملكية الفكرية من أجل التخفيف العراقيل التي تعوق التجارة الدولية.

د. اتفاقية بودابست لمقاومة جرائم المعلوماتية الاتصالات2001 :

إدراكا من الدول بمدى خطورة الجريمة المعلوماتية بوصفها جريمة عابرة للحدود فقد تم التوقيع عليها من طرف ثلاثون دولة في العاصمة المجرية " بودابست "نذكر منها :دول أعضاء من الاتحاد الأوروبي ، إضافة إلى كندا، اليابان، جنوب إفريقيا، أمريكا، و جاءت هذه الاتفاقية لتعالج إشكالية دولية الجريمة الالكترونية تجاوزها للحدود الدولية بما يساعد الدول على مكافحة هذه الجريمة وتعقب مرتكبيها والمساعدة على الاستدلال عليهم وضبطهم كما تحدد أفضل الطرق الواجب إتباعها في التحقيق في جرائم الانترنت التي تعهد الدول الموقعة بالتعاون الوثيق من أجل محاربتها.

واشتملت الاتفاقية الأوروبية لجرائم الحاسب الآلي والإنترنت المسماة باتفاقية بودابست، الموقعة في 11/23 /2001 على خمسة عناوين، الأربعة الأول تناولت أربعة أنواع من الجرائم هي:

- ✓ الجرائم التي تمس سرية وأمن وسلامة وتوفير بيانات الحاسب ومنظوماته وهي تضم (الدخول غير المشروع - والإعراض غير المشروع - والتدخل في البيانات - والتدخل غير المشروع في المنظومة - وإساءة استخدام الأجهزة).
- ✓ والجرائم المتصلة بالحاسب الآلي وتضم (جريمة التزوير المتعلقة بالحاسب -وجريمة التدليس المتعلقة بالحاسب).

- ✓ والجرائم المتصلة بالمواد الإباحية للأطفال (الإنتاج أو النشر غير المشروع للمواد الإباحية وصور الأطفال الفاضحة).
- ✓ والجرائم المتصلة بالاعتداءات الواقعة على الملكية الفكرية والحقوق المرتبطة بها (الطبع والنشر).
- ✓ والعنوان الخامس خصص للمسؤولية وللجزاءات، وهو يشتمل على بنود إضافية يشان الشروع والاشتراك، وأيضا الجزاءات أو التدبير وذلك طبقا للاتفاقيات أو المعايير الدولية الحديثة بالنسبة لمسؤولية الأشخاص المعنوية. (هلالي، 2007، ص.47)

وتعتبر هذه الاتفاقية أحد محاولة وأكثرها تنوعا من أجل تنسيق قوانين جديدة في دول عديدة ضد إساءة استخدام الانترنت.كما نشير إلى أنها تأتي بعد فترة طويلة من المشاورات بين الحكومات أجهزة الشرطة وقطاع الكمبيوتر وقد صاغ نصها عدد من الخبراء القانونين في مجلس أوروبا بمساعدة دول أخرى. (هلالي، 2007، ص.47)

الفرع الثاني: الاتفاقيات الإقليمية في مجال مكافحة الجريمة المعلوماتية

في هذا الفرع سوف نتطرق إلى اهم الجهود والاتفاقيات العربية التي سنت لمكافحة الإجرام المعلوماتي، وذلك كنموذج عن الاتفاقيات الإقليمية في هذا المجال، ونتناول اهمها كما يلي:

الاتفاقية العربية لمكافحة جرائم تقنية المعلومات: جاءت هذه الاتفاقية في إطار تعزيز التعاون بين الدول العربية لمكافحة جرائم تقنية المعلومات التي تهدد امنها ومصالحها وسلامة مجتمعاتها، وفي إطار مواكبة الاتفاقيات الدولية في مجال مكافحة الإجرام السبراني، عقدت هذه الاتفاقية بمدينة القاهرة بجمهورية مصر العربية بتاريخ 21 ديسمبر 2010، في إطار انعقاد مجلسي وزراء الداخلية والعدل العرب المشترك بمقر جامعة الدول العربية بالقاهرة.

حررت هذه الاتفاقية في ثلاثة واربعون مادة ضمن خمسة فصول، تناول الفصل الاول الاحاكم العامة والتعريفات، وفي الفصل الثاني المعنون بالتجريم تم فيه تحديد اصناف الافعال المجرمة في هذا الإطار والتي صنف الي 12 جريمة، اما الفصل الثالث فتطرق إلى الأحكام الاجرائية في تطبيق احكام وبنود هذه الاتفاقية، وفي الفصل الرابع تم توضيح سبل التعاون القانوني والقضائي بين الدول الأعضاء في هذه الاتفاقية، وتناول الفصل الخامس والاخير أحكاما ختامية.

وقعت الجزائر على هذه الاتفاقية فور صدورها بنفس التاريخ، وبذلك أصبحت هذه الاتفاقية رافدا من روافد التشريع الوطني في إطار مكافحة الاجرام الإلكتروني.

الفرع الثالث: تأثر المشرع الجزائري بالجهود الدولية والإقليمية في مجال مكافحة الجريمة المعلوماتية

إن المحيط الدولي والإقليمي في مجال التشريعات القانونية في إطار مكافحة الجرائم الالكترونية أو المعلوماتية يمكن اعتباره الملهم الحقيقي أن صح التعبير للمشرع الجزائري في هذه المجال، وذلك لضرورة مواكبة التطورات الدولية أو الإقليمية في هذا الميدان، وكذلك للموقع القانوني للاتفاقيات الدولية الموقعة من طرف الجزائر حيث تسمو علي

القوانين الداخلية وبالتالي تدعو المشرع الجزائري الي تعديل القوانين الداخلية بما يتماشي مع هذه الاتفاقيات أو سن قوانين جديدة لمواكبة هذه التشريعات.

حيث أن أهم ما يلاحظ علي التعديلات المتعاقبة للقانون الجنائي الجزائري (قانون العقوبات وقانون الإجراءات الجزائية)، أنه دائما ما يتم عقب توقيع الجزائر علي اتفاقيات دولية او اقليمية في هذا المجال وذلك في اطار مواكبة التطورات التشريعية على المستوى الدولي والاقليمي أو لضمان عدم التناقض مع هذه الأخيرة، خاصة وأن المجرمون المعلوماتيون أصبحو كثيرا ما يستهدفون الدول والأرضيات الرقمية المتواجدة بالدول التي لا تجرم هذا النوع من الأفعال سواء بسبب عدم تحديث منظومتها القانونية او عدم تعديلها بما يتوافق مع المعاهدات والاتفاقيات الدولية.

أما بخصوص التعديل الاخير لقانون العقوبات الذي جاء ضمن القانون 16-02 المؤرخ في 19 جوان 2016، (ج.ر، 2016) المتمم للأمر رقم 66-156 المتضمن قانون العقوبات، والذي نص ضمن المادة الثانية منه على تتميم الفصل السابع مكرر من قانون العقوبات الجزائري المعنون بالمساس بالمعالجة الآلية للمعطيات بالمادة 394 مكرر8 والتي نصت على العقوبات المسلطة علي مقدم خدمة الانترنت.

حيث بعد تعريف هذا الاخير بموجب القانون رقم 09-04 المؤرخ في 05 أوت 2009، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها والذي جاء زمنيا عقب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 الذي نص علي الفصل السابع مكرر بمواده من 394 مكرر الي المادة 394 مكرر7، وجد المشرع الجزائري نفسه مضطرا الي تكملته بالمادة 394 مكرر8 في إطار تحديد المسؤوليات وتدقيقها خاصة مسؤولية مقدمو خدمة الانترنت، كونهم يمتلكون القدرة على الدخول إلى الأرضيات الرقمية والقدرة علي التصرف في البيانات والمعطيات المنشورة او المخزنة في شبكة الأنترنيت، كما ان مقدمي خدمات الانترنت قد يكونون اشخاصا طبيعيين كما قد يكونون أشخاصا معنوية.

خاتمة:

حاولنا من خلال هذه الوقة البحثية التطرق الي الجرائم المعلوماتية باعتبارها نوعا مستحدثا من الاجرام سعت الدول ولاتزال تسعي من اجل محاربته ومكافحته أو التقليل من الاضرار السلبية لهذه الجرائم أن على مستوى الافراد وحقوقهم وحرياتهم الخاصة أو على مستوى المجتمعات أو على مستوى الدولة والمجتمع الدولي ككل وما تخلفه هذه الجرائم من اضرار اقتصادية او مالية او حتى اخطار اصبحت تهدد كيانات الدول وحدودها وامنها الداخلي والخارجي عموما.

مبرزين ماهية هذه الجرائم وخصائصها واهم الاتفاقيات الدولية والاقليمية التي تناولت مكافحة هذا الإجرام، وكذا ما استحدثه المشرع الجزائري في هذه الإطار في محاولة منه للتكيف مع التطور التشريعي الدولي، ويمكن ان نخلص الي النتائج والتوصيات التالية:

- ✓ ضرورة تكاثف جميع الجهود في مكافحة الجرائم المعلوماتية، خاصة المجتمع المدني بكل اطيافه بداء من الاسرة، المدرسة، الجمعيات...الخ، والتحسيس والتوعية بمخاطر الاستعمال السئ لشبكات الاعلان والاتصال بمختلف انواعها.
- ✓ ضرورة المواكبة في سن قواعد جديدة لمكافحة الجرائم المعلوماتية، تأخذ بعين الاعتبار الطبيعة الخاصة لهذه الجرائم ولا سيما ما يتعلق بالإثبات في الدعاوى الناشئة عن هذه الجرائم، خاصة في ظل التطور المتسارع لهذا الميدان (ميدان تكنولوجيات العلام والاتصال).
- ✓ ضرورة تكثيف وزيادة التعاون والتنسيق الدولي والإقليمي في ميدان مكافحة الجرائم المعلوماتية، نظرا للطبيعة اللاحدودية لهذه الجرائم التي يستخدم في ارتكابها شبكات لا تعرف حدودا ولا قيودا.
- ✓ ضرورة التفعيل الميداني للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال المستحدثة بموجب القانون رقم 09-04 المؤرخ في 05 أوت 2009.
- ✓ ضرورة تخصيص جهاز قضائي وضبطية قضائية متخصصة لمكافحة هذا النوع من الاجرام، مع المتابعة المستمرة للتكوين وتحيين المعلومات لأشخاصها للتمكن من مواكبة التطور المتسارع في مجال تكنولوجيات الاعلام والاتصال.

قائمة المراجع:

1) بعرة سعيدة (2016): الجريمة الإلكترونية في التشريع الجزائري-دراسة مقارنة-، مذكرة استر قانون جنائي، جامعة بسكرة.

2) الجريدة الرسمية للجمهورية الجزائرية عدد رقم 34 بتاريخ 27 جوان 2001.

3) الجريدة الرسمية للجمهورية الجزائرية عدد رقم 71 الصادر بتاريخ 10 نوفمبر 2004.

4) حملاوي عبد الرحمان (2015): دور المديرية العامة للأمن الوطني في مكافحة الجرائم الإلكترونية، مداخلة ملقاة خلال الملتقي الوطني الجريمة المعلوماتية بين الوقاية والمكافحة، المنعقد بجامعة بسكرة خلال الفترة 16-17 نوفمبر 2015.

5) سامي علي حامد عياد (2006): الجريمة المعلوماتية واجرام الانترنت، دار الفكر الجامعي، الإسكندرية.

6) فضيلة عاقلي (2017): الجريمة الإلكترونية واجراءات مواجهتها من خلال التشريع الجزائري، دراسة منشورة بكتاب اعمال الملتقى الدولي الرابع عشر الجرائم الالكترونية، المنعقد خلال الفترة من 24 الي 25 مارس 2017 طربلس لبنان.

7) القانون 04-14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66-155 المؤرخ في 08 جوان 1966 المتضمن قانون الإجراءات الجزائية، الصادر بالجريدة الرسمية للجمهورية الجزائرية، عدد 71، بتاريخ 10 نوفمبر 2004.

8) القانون 04-14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66-155 المؤرخ في 08 جوان 1966 المتضمن قانون الإجراءات الجزائية، الصادر بالجريدة الرسمية للجمهورية الجزائرية، عدد 71، بتاريخ 10 نوفمبر 2004.

9) محمد امين احمد الشوابكة (2004): جرائم الحاسوب والانترنت (الجريمة المعلوماتية)، ط1، مكتبة دار الثقافة، عمان.

10) المرسوم الرئاسي رقم 15-261 المؤرخ في 08 اكتوبر 2015 المتضمن تحديد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، الصادر في الجريدة الرسمية للجمهورية الجزائرية عدد 53 بتاريخ 08 اكتوبر 2015.

11) مزيود سليم (2014): الجرائم المعلوماتية في الجزائر واقعها وآليات مكافحتها، مقال منشور بالمجلة الجزائرية للاقتصاد والمالية، عدد01، أفريل 2014، جامعة المدية.

12) مفتاح بوبكر المطردي (25 سبتمبر، 2012): الجريمة الإلكترونية والتغلب على تحدياتها، ورقة بحثية مقدمة في المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية، المنعقد بجمهورية السودان خلال الفترة من 23 الي 25 سبتمبر 2012.

13) نمديلي رحيمة (2017): خصوصية الجريمة الإلكترونية في القانون الجائري والقوانين المقارنة، دراسة منشورة في كتاب اعمال المؤتمر الدولي الرابع عشر (الجرائم الالكترونية)، المنعقد بطرابلس لبنان في الفترة 24-25 مارس 2017.

14) هلالي عبد اللاه أحمد (2007)، اتفاقية بودابست لمكافحة جرائم المعلوماتية (معلقا عليها)، دار النهضة العربية، الطبعة الأولى، القاهرة

15) يونس عرب (10-12فيفري، 2000): جرائم الكمبيوتر والانترنيت، ورقة بحثية مقدمة في مؤتمر الامن العربي المنظم من قبل المركز العربي للدراسات والبحوث الجنائية بأبوظبي

الجريمة الإلكترونية: وطرق إثبات الدليل الرقمي في الشريعة الإسلامية

Electronic crime: and methods of proving digital evidence, in Islamic Sharia

ط.د. حليم مدبر/ جامعة السلطان محمد الفاتح، إسطنبول/ تركيا
PhD.Halim Medebbeur/ Sultan Mehmet Al-Fateh University, Istanbul/Turkey.

ملخص الدراسة:

كان للتطور الإلكتروني في العالم آثاره الإيجابية الكبيرة على حياة الناس، وبالمقابل كان هذا التوسع المعرفي له آثره في ظهور "الجرائم الإلكترونية"، التي كثرت، وتنوعت أساليبها، ولكون هذا النوع من الجرائم حادث، كانت هذه المسألة عند الفقهاء من باب النوازل الشرعية، التي تحتاج لتوضيح وبيان.

وأهم شيء في هذا النوع من الجرائم هو: طرق إثباتها، لصعوبة إثبات الجريمة، في عالم إلكتروني واسع جداً، ولهذا قامت هذه الدراسة على المنهج الاستقرائي بجمع الأسس الشرعية في طرق إثبات هذا النوع من الأدلة، ثم المنهج التحليلي ببيان تكييفها الشرعي، وضوابط ذلك، للخروج برؤية واضحة حول طرق الإثبات في الشريعة الإسلامية للجرائم الإلكترونية.

وقسمت هذه الدراسة لمقدمة، ولمبحثين، فأول المباحث: الدليل الرقمي للجريمة الإلكترونية في الفقه الإسلامي والثاني: حجية الدليل الرقمي في الشريعة الإسلامية، ثم خاتمة تضمنت أهم النتائج والتوصيات، مع قائمة للمراجع والمصادر.

الكلمات المفتاحية: الجريمة الإلكترونية، طرق الإثبات، النوازل الشرعية، الأنترنيت. البيِنَة.

Abstract:

The electronic development in the world had great positive effects on people's lives, and on the other hand, this expansion of knowledge had its effect in the emergence of "electronic crimes", which abounded and their methods varied , also because this type of crime is an accident, this issue was among the jurists from the door of legal calamities, which Need to clarify and indicate.

The most important thing in this type of crime is: "methods of proving it", due to the difficulty of proving the crime, in a very wide electronic world, and for this reason this study was based on the inductive method, collecting the legal foundations in the methods of proving this type of evidence, then the analytical method by showing its legal adaptation, and controls That to come up with a clear vision about the methods of proof in Islamic law for electronic crimes.

This study was divided into an introduction and two investigators, the first investigation: the digital evidence of electronic crime in Islamic jurisprudence, and the second: the authenticity of the digital evidence in Islamic law, then a conclusion that included the most important results and recommendations, with a list of references and sources.

Keywords: electronic crime, methods of proof, legal calamities, the Internet. The evidence

المدخل:

مع التطور الإلكتروني الهائل الذي يعيشه البشر في هذا العصر، كان للجرائم تطورها كذلك، وفتح هذا التطور آفاق بحيثية وعلمية في الشريعة الإسلامية، والتي تُعرف بمرونتها في تناول قضايا العصر، وبالتالي انصب عمل المعاصرين على تجلية أحكام هذا النوع من الجرائم في الشريعة.

أولا. إشكالية البحث:

يقع الإشكال دائماً في بيان وجوه المرونة في الشريعة الإسلامية، مع قضايا العصر، وحينئذٍ يُستشكل الكثير من الأسئلة في هذه الدراسة، ولكن أهم تلك الأسئلة هي:

1. ما معنى الجريمة الإلكترونية في الفقه الإسلامي؟

2. هل في الشريعة الإسلامية ما يُمكن أن يستدل به على إثبات الجريمة الإلكترونية؟

3. ما كيفية تطبيق أدلة إثبات الجريمة الإلكترونية في الشريعة، وما مدى قدرتها على مواجهة معوقات التطبيق؟

ثانياً: أهداف الدراسة: والتي تتمثل في:

1. بيان معنى الجريمة الإلكترونية في الفقه الإسلامي.

2. بيان ماهية الدليل الرقمي في الجريمة الإلكترونية في الشريعة الإسلامية

3. توضيح كيفية تطبيق أدلة إثبات الجريمة الإلكترونية في الشريعة

ثالثاً. الدراسات السابقة: الجريمة الإلكترونية من النوازل الحادثة، لكن البحوث فيها كثيرة؛ لكثرة هذه الجريمة وارتباطها بالقضاء الجنائي، إلا أن عدم ثبوت القضاء الشرعي في الكثير من الدول الإسلامية جعل البحوث المتعلقة بهذا الجانب قليلة، ومن البحوث التي تطرقت لموضوع الدليل الإلكتروني وكونه من وسائل الإثبات الشرعية:

1. الجريمة الإلكترونية وسبل مواجهتها في الشريعة الإسلامية، بحث للدكتور عطايا، إبراهيم، منشور في مجلة الشريعة والقانون، بطنطا بمصر، ع30، م2، سنة 2015، ولكن كان تطرقه لبيان وسائل الإثبات مجملاً، ولم يتوسع فيه بالقدر الكافي.

2 حجية الأدلة الرقمية في النظام القضائي الإسلامي، للدكتور بهاء الدين الجاسم، وهو بحث منشور في مجلة البحوث الفقهية الإسلامية، ع37، سنة 2021، وهو بحث جيد وفّى صاحبه بأهداف البحث وإن كان لم يتطرق لبعض المسائل التي تتعلق بالدليل الرقمي، وحجيته في الشريعة.

ولهذا الإضافة في هذه الدراسة هو: بيان ماهية الدليل الرقمي، وتكييفه الشرعي، وشروط هذا التكييف.

رابعاً. حدود البحث:

نطاق البحث سيكون مقتصراً، على بيان أدلة إثبات الجريمة الإلكترونية -دون التطرق لغيرها من مجالات الجريمة الإلكترونية-وعلاقة الشريعة الإسلامية بذلك.

خامساً. منهج البحث: اقتضت طبيعة البحث أن يقام على المناهج التالية:

أ. المنهج الاستقرائي: باستقراء أدلة إثبات الجريمة الإلكترونية في الشريعة

ب. المنهج التحليلي: بتحليل تلك الأدلة وتجلية طريقة عملها

سادساً. خطة البحث:

قسمت الدراسة إلى مقدمة ومبحثين، على النحو الآتي:

المقدمة: وفيها فكرة البحث، وخطته.

المبحث الأول: الدليل الرقمي للجريمة الإلكترونية في الفقه الإسلامي، وفيه مطالب:

المطلب الأول: الجريمة الإلكترونية في الفقه الإسلامي

المطلب الثاني: ماهية الدليل الرقمي في الجريمة الإلكترونية، وأشكاله وخصائصه

المطلب الثالث: إجراءات الحصول على الدليل الإلكتروني:

المبحث الثاني: حجية الدليل الرقمي في الشريعة الإسلامية، وفيه مطالب:

المطلب الأول: مشروعية الدليل الرقمي في الشريعة الإسلامية

المطلب الثاني: التكييف الفقهي في الشريعة الإسلامية للدليل الرقمي

المطلب الثالث: الخصوصية في الدليل الرقمي ومشروعية الحصول عليه

المطلب الرابع: القوة الإثباتية للدليل الرقمي

الخاتمة: وفيها أهم النتائج والتوصيات

قائمة المصادر والمراجع

وسرت في هذه الدراسة على الجادة والمسلك البحثي المعروف في العزو، وتوثيق النصوص من مصادرها الأصلية، مع التركيز على نقطة البحث وحدوده، والتنكيب عما قد يكون شاذا من الأمثلة، وترك الاستطراد المخل بالموضوع.

3. المبحث الأول: الدليل الرقمي للجريمة الإلكترونية في الفقه الإسلامي

3.1. المطلب الأول: الجريمة الإلكترونية في الفقه الإسلامي

الجريمة عند الفقهاء هي المحظورات الشرعية، التي نهي الشرع عنها بحدٍ شرعي، أو حكم التعزير (عودة، (د.ت)، صفحة 66/1)، وبناء عليه؛ فالجريمة الإلكترونية لابُدَّ أن يتوفر فيها الشروط المعتبرة شرعاً، في الجريمة، وهي:

1. أن يكون فعل الجاني غير شرعي. وفقاً لأحكام الشريعة.
2. أن يكون الفاعل ذا أهلية، وإلا عُدَّ فعله من باب العقوبة المدنية، لا الجنائية.
3. أن تكون العقوبة الشرعية مقررة شرعاً، سواء كانت العقوبة مقدرة بحِّد، أو بغير حدٍّ، بل تعزيراً.
4. أن يكون الفعل صادراً بإرادة الفاعل، لا بالإكراه (عودة، (د.ت)، صفحة 66/1) .

وينبني كل هذا على أركان ثلاثة هي أركان الجريمة في الشريعة، وهي:

1. **الركن الشرعي**: فتُعتبر الجريمة في الشريعة إذا قابلها النص المحرم، وينجر عليه ثبوت العقوبة الرادعة شرعاً، ويكون النص الشرعي المحرم للفعل، نافذاً زمن الفعل، ويكون سارياً على مكان الجريمة، وعلى الشخص المرتكِب لها، وفي حالة عدم توفر شرطٍ من هذه الشروط يسقط هذا الركن، ولهذا لابُدَّ من ربط الجريمة الإلكترونية بهذه الشروط الشرعية ليتم هذا الركن، ويكون صحيحاً شرعاً (عودة، (د.ت)، صفحة 112/1) .

2. **الركن المادي**: وهو الذي يتناول النظر في الجريمة، من جهة الابتداء، والشروع، والمشاركة، وعدم الاشتراك، وبكل جهة من هذه الجهات يُمكن الحكم على فعل الجاني. (عودة، (د.ت)، صفحة 342/1) .

3. **الركن المعنوي**: وهي الصلة النفسية بين الركن المادي وبين ما يقوم به المكلَّف، وهي تقوم على أمرين اثنين، هما:

الأهلية، والاختيار (عودة، (د.ت)، صفحة 380/1).

3.2. المطلب الثاني: ماهية الدليل الرقمي في الجريمة الإلكترونية، وأشكاله، وخصائصه

يُعَّد إثبات الدليل الجنائي في الجرائم الإلكترونية، من النوازل الفقهية الحديثية، وصار البحث فيها متلائم مع التطور الجنائي المعاصر، وزاد هذا التطور الجنائي الأعباء على السلطات الأمنية؛ للوصول إلى أركان الجريمة. وأول ما يجب النظر فيه هنا، هو إقامة الدليل المادي على ثبوت الجريمة نفسها، بإثبات الوقائع، ولا يكون ذلك إلا بإثبات الأدلة، بالاستعانة بوسائل الإثبات،

والدليل الإلكتروني هو: "المعلومات التي يقبلها المنطق والعقل، ويعتمدها العلم، يتم الحصول عليها بالإجراءات القانونية، بترجمة البيانات الحسابية، المخَّزنة في أجهزة الحاسب الآلي، وملحقاتها، وشبكات الاتصال، ويمكن استخدامها في أيّ مرحلة من مراحل التحقيق والمحاكمة" (يوسف، 2006، صفحة 2)".

وليس كل ما يظهر في المجال الإلكتروني يكون دليلاً، بل الأدلة فيه على نوعين:

أ. ما يصلح ليكون دليلاً للإثبات: وهي قسمان:

- ✓ السجلات التي تم إنشاؤها بواسطة الآلات تلقائياً، مثل سجلات الهاتف، وفواتير الحاسوب.
- ✓ السجلات التي جزء منها تم حفظه بالإدخال، وجزء منه تم إنشاؤه بواسطة الآلات

ب. ما لا يصلح ليكون دليلاً للإثبات: وهو الناشئ من الجاني دون أن يرغب في إنشائه، وهو المعروف بالبصمة الرقمية، وهي تتجسد في الآثار التي يتركها مستخدم الشبكات المعلوماتية، بسبب التسجيل، والاتصال الرقمي، والتواصل الشبكي (فلاك، 2019، صفحة 207)

ويُمكنُ حصر أشكال الأدلة الإلكترونية في:

أ. الصور الرقمية: وهي التي تجسد الحقيقة المرئية للجريمة.

ب. التسجيلات الرقمية: من محادثات صوتية تم تخزينها في الحاسوب، أو الهاتف.

ت. النصوص المكتوبة: وتشمل كل النصوص المكتوبة عبر الرسائل الهاتفية، وبالبريد الإلكتروني وغيرها.

وبهذا يظهر أن للدليل الإلكتروني خصائصاً، تُمَّيزه عن الدليل التقليدي، وهي:

أ. أن الأدلة الإلكترونية تتكون من البيانات لا تدرك بالحواس، بل يُتطلب إدراكُها الاستعانة بالأجهزة الإلكترونية واستخدام المعدات الخاصة بها.

ب. الأدلة الرقمية تُصوِّر وقائع الإجرام بأكثر دقة، بل قد تصل إلى تصوير الجريمة نفسها.

ت. الأدلة الرقمية يمكن استخراجها بنسخ مطابقة للواقع للأصل، مما يُشَّكل ضمانة عالية ضد الفقد، والتلف، والتغيير (فلاك، 2019، صفحة 208).

3.3. المطلب الثالث: إجراءات الحصول على الدليل الإلكتروني:

وهي الإجراءات التي تستعمل غالباً في الطريقة التقليدية، لكن يقع التمايز بينهما في بعض الجزئيات:

1. المعاينة:

فعند وقوع الجريمة، تكون الهيئات المسند لها التحقيق في الجريمة، بمعاينة مسرح الجريمة المعلوماتية، وهذا برؤيا المكان، أو الشخص، والأشياء المتصلة بالواقعة، وهذه المعاينة كما تكون بتنقل المحققين إلى أمكنة الجريمة، فقد يُنقل إليهم العتاد الذي قامت به الجريمة.

فالمعاينة هي الوسيلة الأولى التي يمكن المحققين من البحث الجنائي، ويتم تقيد الهيئات المحققة بما يلي:

أ. تصوير الآلات التي وقعت بيد المحققين، بذكر تاريخ الحصول عليها تفصيلا.

ب. إخطار الفرق التقنية بالمعاينة الإلكترونية؛ للاستعداد من الناحية الفنية والعملية.

ت. التحفظ على كل المستندات الورقية وغير الورقية للآلات.

ث. عدم نقل أي مادة من الآلات التي وقعت بيد المحققين، والتحفظ عليها بالشكل الذي يجعلها محفوظة من التلف الكلي أو الجزئي (بيومي، 2008، صفحة 92).

2. التفتيش:

وهو إجراء من إجراءات التحقيق، يهدف إلى البحث عن الأشياء المتعلقة بالجريمة، وله شروطه التي تجعله موافقاً لإجراءات التحقيق، وهي:

أ. أن يكون الأمر بالتفتيش مسبباً، وله دواعيه القائمة على القرائن.

ب. حضور المتهم، أو المشكوك فيه، أو من ينوب عنه لإثبات الصفة.

ت. تحرير محاضر التفتيش التي تجمع حيثيات ما قامت به لجنة التفتيش تفصيلاً.

وهذه الوسائل التقنية لا تتعارض مع أصول الشريعة الإسلامية، من ثَمَّ فالقضاء الشرعي يُعملها، ويراها صحيحة (الزحيلي و.، (د.ت)، صفحة 6288/8).

3. الخبرة:

وهي الوسيلة التي يُمكن بها تحديد التفسير الفني للأدلة، فهي في الحقيقة تقييم للأدلة، وتكون بعد التفتيش، وترجع في معناها لعمل الخبير، وللخبرة أنواع، أهمها:

أ. الخبرة الخاصة: وهي التي تعود لجهود المحققين الشخصية والتي تتوفر فيهم من خلال الممارسة لهذا الفعل، يتبع القضايا الجنائية.

ب. الخبرة العامة: وهي التي تقوم بها الهيئات الفنية العامة، والتي يرجع لها المحققون غالباً في تتبع الكثير من القضايا الجنائية المستعصية (فلاك، 2019، صفحة 214)

وإن تقدم العلوم وتفرع البحوث، وزيادة التخصصات، وتقسيم الأعمال إلى نواحي كثيرة، يؤكد الحاجة إلى الخبرة وفائدتها وأهميتها، فالقاضي الآن في أشد الحاجة لمجموعة متخصصة في كل ما يتعلق بالعلوم الإلكترونية، يطلب منهم المساعدة؛ لتحصيل ما يراه دليلاً في القضايا التي تعرض عليه.

والخبير يبيّن حقيقة الشيء بعد التجارب والأبحاث العلمية التي استغرقت سنوات كثيرة في حياته، بحيث يزول معه العامل الشخصي تقريباً، وبذلك يكون رأي الخبير هو الخبرة ذاتها، ولا ينظر إلى التكوين الشخصي له، ويشترط في الخبير أن يكون ماهراً في التعاملات الإلكترونية، ولا يشترط أن يكون أكثر من واحد (الزحيلي م.، 1982، صفحة 597).

4. المبحث الثاني: حجية الدليل الرقمي في الشريعة الإسلامية

4.1. المطلب الأول: مشروعية الدليل الرقمي في الشريعة الإسلامية

فأما الإثبات عند الفقهاء فهو: إقامة الدليل الشرعي أمام القاضي في مجلس قضائه على حق أو واقعة من الوقائع" (وزارة الأوقاف الكويتية، 1427، صفحة 232/1).

ووسائل الإثبات عند الفقهاء كثيرة، لكن اختلف علماء الفقه هل هذه الوسائل محصورة بما هو مذكور في الكتاب والسنة أو لا؟، فأما جمهور الفقهاء فيرون أنها محصورة بذلك، واختلفوا في عددها عند كل مذهب:

فقال ابن عابدبن الحنفي:" الدعوى والحجة: وهي إما البينة أو الإقرار أو اليمين أو النكول عنه أو القسامة أو علم القاضي بما يريد أن يحكم به أو القرائن الواضحة التي تصير الأمر في حيز المقطوع به" (ابن عابدين، 1966، صفحة 5/354) .

وقال ابن جزي المالكي:" لا يقضي بعلمه، وإنما يحكم بحجة ظاهرة وهي سبعة أشياء وما يتركب منها وهي اعتراف أو شهادة أو يمين أو نكول أو حوز في الملك أو لوث مع القسامة في الذماء أو معرفة العفاص والوقاء في اللقطة" (ابن جزي، (د.ت)، صفحة 194) .

والأخذ بها مذهب الشافعية (الخطيب الشربيني، 1994، صفحة 425/6)، ونحوهم الحنابلة فلم يذكروا سوى ما ورد في النصوص الشرعية (ابن قدامة، 1997، صفحة 72/14)، ولهم حجج يمكن حصرها في:

أ. عن الأشعث بن قيس قال: كانت بيني وبين رجل خصومة في بئر، فاختصمنا إلى رسول الله صلى الله عليه وسلم، فقال رسول الله: شاهداك أو يمينة" (البخاري، 2002، صفحة 143/3، رقم: 2516)، فيُفهم منه حصر الأدلة.

ب. النصوص الشرعية ذكرت طرق البيان والإثبات، فيجب الوقوف عندها، دون مجاوزتها، وإلا فقد يدخل التغيير في أدلة الإثبات الشرعية (الزحيلي م.، 1982، صفحة 606).

ت. فتح الباب لدخول الأدلة غير الثابتة في القرآن والسنة، يجعل القضاة الظلمة يغيرون الأحكام الشرعية على أهوائهم (الزحيلي م.، 1982، صفحة 608).

وعُورضُوا ممن يرون عدم الحصر فيما ورد في نصوص الوحي، ومن هؤلاء شيخ الإسلام ابن تيمية (ابن تيمية، 1995، صفحة 394/35)، وتلميذه ابن القيم الذي يقول: " فالبينة اسم لكل ما يبين الحق ويظهره ومن خصها بالشاهدين، أو الأربعة، أو الشاهد لم يوف مسماها حقه، ولم تأت البيِّنة قط في القرآن مرادا بها الشاهدان، وإنما أتت

مرادا بها الحجة، والدليل والبرهان، مفردة مجموعة وكذلك قول النبي - صلى الله عليه وسلم -: «البينة على المدعي» المراد به: أن عليه بيان ما يصحح دعواه ليحكم له، والشاهدان من البينة ولا ريب أن غيرها من أنواع البينة قد يكون أقوى منها، لدلالة الحال على صدق المدعي" (ابن القيم، د.ت ، صفحة ص:11).

وهو قول ابن فرحون المالكي، فقال:" فمتى ظهر الحق وأسفرت طريق العدل، فثم شرع الله ودينه، ولما كانت البينات مرتبة بحسب الحقوق المشهود فيها، والمحتاج إلى إقامتها، وما هي عليه من التوسعة والتضييق والتثقيل والتخفيف، وإمكان التوثيق وتعذره، واختلاف مراتبها في القوة والضعف، احتجنا إلى ذكرها وعد أنواعها وتمثيل مسائلها" (ابن فرحون، 1986، صفحة 242/1).

وحجتهم في ذلك:

أ. عدم الدليل المقيد لهذا الحصر بحديث "شاهداك أو يمينك"، وجعلوا كل ما كان دليلاً للوصول للجاني – ما لم يكن أمراً محرماً شرعاً-فهو وسيلة للإثبات.

ب. أن الشرع جعل البيّنة هي دليل الإثبات، ولم يحصرها، فهي اسم قد يكون للشهود، أو اليمين، أو النكول واليمين، أو خمسين يميناً، أو أربعة أيمان، ونحو ذلك من الأدلة (ابن تيمية، 1995، الصفحات 35/395-397).

ت. استدلوا بنصوص كثيرة في قضايا متكاثرة عن الصحابة وغيرهم من القضاة زمن التابعين ومن بعدهم في حكمهم بالقرائن والبيات بما لا يوجد في المنصوص عليه شرعاً (ابن القيم، د.ت ، صفحة 9).

ث. أجابوا عن أدلة الجمهور، ب:

عن حديث البخاري السابق، فقال ابن دقيق العيد: "وقد يقال في هذا: إن المقصود من الكلام نفي طريق أخرى لإثبات الحق، فيعود المعنى إلى حصر الحجة في هذين الجنسين -أعني البينة واليمين -إلا أن هذا قليل النفع بالنسبة إلى المناظرة. وفهم مقاصد الكلام نافع بالنسبة إلى النظر. وللأصوليين في أصل هذا الكلام بحث، ولم ينبه على هذا حق التنبيه -أعني اعتبار مقاصد الكلام -وبسط القول فيه إلا أحد مشايخ بعض مشايخنا من أهل المغرب، وقد ذكره قبله بعض المتوسطين من الأصوليين المالكيين في كتابه في الأصول. وهو عندي قاعدة صحيحة، نافعة للناظر في نفسه، غير أن المناظر الجدلي: قد ينازع في المفهوم ويعسر تقريره عليه" (ابن دقيق العيد، د.ت، صفحة 260/2).

وقال الشوكاني:" ومن جملة ما استدل به المانعون حديث " شاهداك أو يمينه " وفي لفظ " وليس لك إلا ذلك " ويجاب بما تقدم من أن التنصيص على ما ذكر لا ينفي ما عداه وأما قوله: وليس لك إلا ذلك " فلم يقله النبي – صل الله عليه وسلم - وقد علم بالمحق منهما من المبطل حتى يكون دليلا على عدم حكم الحاكم بعلمه، بل المراد أنه ليس للمدعي من المنكر إلا اليمين وإن كان فاجرا حيث لم يكن للمدعي برهان" (الشوكاني، 1993، صفحة 322/8).

عن قولهم بمنع التوسع لأجل القضاة الظلمة، فهذا يمكن منعه من جهة وضع الضوابط العامة، والقواعد الكلية، في الإثبات وتتبع جزئيات الحكم القضائي، ويعود سبب الخلاف يرجع إلى أمرين:

1. لاختلاف في تفسير لفظ "البينة"، فمن فسر "أل" بالعموم جعل كل ما يوصل للحق بينة شرعية، ومن جعل "أل" عهدية بما نزله الشرع فجعل الأدلة ما يدل عليه النصوص الشرعية لا غير.

2. أن أدلة الإثبات عند الجمهور بمنزلة النصوص التعبدية التي لا يجوز الخروج عنها، بخلاف غيرهم الذين يرون أنها معقولة المعنى، فيجوز الخروج عنها،

والأدلة تدل على صحة القول لثاني:

فقال الشوكاني،:" والحق الذي لا ينبغي العدول عنه أن يقال: إن كانت الأمور التي جعلها الشارع أسبابا للحكم كالبينة واليمين ونحوهما أمورا تعبدنا الله بها لا يسوغ لنا الحكم إلا بها، وإن حصل لنا ما هو أقوى منها بيقين فالواجب علينا الوقوف عندها والتقيد بها وعدم العمل بغيرها في القضاء كائنا ما كان، وإن كانت أسبابا يتوصل الحاكم بها إلى معرفة المحق من المبطل والمصيب من المخطئ غير مقصودة لذاتها بل لأمر آخر وهو حصول ما يحصل للحاكم بها من علم أو ظن وأنها أقل ما يحصل له ذلك في الواقع فكان الذكر لها لكونها طرائق لتحصيل ما هو المعتبر" (الشوكاني، 1993، صفحة 332/8).

وقال محمد الزحيلي:" وبناء على ذلك، تكون وسائل الإثبات غير محصورة في عدد معين، وطرق خاصة، بل تكون مطلقة وغير محددة، وكل وسيلة تظهر الحق وتكشف الواقع يصح الاعتماد عليها في الحكم، والقضاء بموجبها، وإذا حددت وسائل الإثبات في قواعد عامة، وصنفت في ضوابط كلية، فإنما يقصد منه التنظيم وسد الذرائع في الحدود التي خوّلها الشارع لولي الأمر، يتصرف فيها بما يراه مناسباً للمصلحة العامة" (الزحيلي م.، 1982، الصفحات 615-616)".

4.2. المطلب الثاني: التكييف الفقهي في الشريعة الإسلامية للدليل الرقمي

فالتكييف الفقهي هو:" التصور المُحكم لحقيقة الواقعة؛ لإلحاقها بأصلٍ فقهي معتبر، بعد التحقق من المماثلة بينهما" (الريسوني، 2014، صفحة 286)، فيكون لهذا التكييف عناصر هي: الواقعة المستجدة، والأصل، وأوصاف الأصل الفقهية، والإلحاق (شبير، 2014، الصفحات 26-30)، وأهمها، هي:

أ. الواقعة المستجدة: وهي المسألة المستحدثة التي تُعرض على المجتهد، ليحكم فيها، وتشمل غالباً على المسائل التي لم تكن معروفة في عصور التشريع، أو الاجتهاد كالنقود الورقية، والمسائل التي تغيرت على الحكم فيها؛ لتغير الظروف كالتقابض الحكمي في صرف العملات.

ب. التعرف على الأصل الذي تُكيف عليه الواقعة: وهو محل الحكم الذي يريد المجتهد التسوية فيه بينه وبين الواقعة المعروضة، وهو إما نص من القرآن، أو السنة، أو إجماع، أو على قاعدة كلية، أو نص لفقيه من أصحاب المذاهب، ويجب هنا على المجتهد أن يتحقق من ثبوت الأصل، وأن يفهمه فهماً جيداً، مقروناً بظروفه وشروطه.

ت. المطابقة بين الواقعة المستجدة والأصل: وهو الجمع بين الواقعة المستجدة، والأصل في الحكم؛ لاتحادهما في العلة،

وهذا يتطلب مجانسة بينهما في الأركان، والشروط، والعلاقات بين أطراف الواقعة (شبير، 2014، صفحة 96).

الدليل الرقمي من القرائن التي يتحقق بها حكم القاضي، وهي من نوازل العصر، والتي يمكن إدراجها في أبواب القرائن، والقرنية: أمارة ظاهرة تقارن شيئاً خفياً فتدل عليه" (الزرقا، 2004، صفحة 936/2)، والدليل الرقمي قرينة واضحة وجلية على إثبات الحكم، فهو عندهم بمنزلة الوسائل الثابتة الذكر في نصوص الوحي (ابن فرحون، 1986، صفحة 117/2).

والقرائن من أدلة الإثبات عند جمهور الفقهاء، كالحنفية (ابن نجيم، د.ت، صفحة 205/7)، والمالكية (ابن فرحون، 1986، صفحة 93/2)، والشافعية (ابن عبد السلام، 1991، صفحة 50/2) ، والحنابلة (ابن القيم، د.ت ، الصفحات 3-4)، وإن اختلفوا في التوسع فيها، والتضييق، فقال محمد شلتوت:" ومما ينبغي المسارعة إليه، في هذا المقام، أن الناظر في كتب الأئمة يرى أنهم مجمعون على مبدأ الأخذ بالقرائن في الحكم والقضاء، وأن أوسع المذاهب في الأخذ بها مذهبا المالكية والحنابلة، ثم الشافعية، والحنفية" (شلتوت، 2001، صفحة 540).

وحجتهم في العمل بها أدلة كثيرة، منها:

1 . قال الله تعالى: "قال هِيَ رَٰوَدَتۡنِي عَن نَّفۡسِيۚ وَشَهِدَ شَاهِدٞ مِّنۡ أَهۡلِهَآ إِن كَانَ قَمِيصُهُۥ قُدَّ مِن قُبُلٖ فَصَدَقَتۡ وَهُوَ مِنَ ٱلۡكَٰذِبِينَ ٢٦ وَإِن كَانَ قَمِيصُهُۥ قُدَّ مِن دُبُرٖ فَكَذَبَتۡ وَهُوَ مِنَ ٱلصَّٰدِقِينَ ٢٧ فَلَمَّا رَءَا قَمِيصَهُۥ قُدَّ مِن دُبُرٖ قَالَ إِنَّهُۥ مِن كَيۡدِكُنَّۖ إِنَّ كَيۡدَكُنَّ عَظِيمٞ" [يوسف: 26-28]، وفيه إعمال القرائن في الحكم، قال ابن القرس:"احتج الفقهاء بهذا في أعمال الأمارات في مسائل كالقسامة بها في قول مالك، إلى غير ذلك" (ابن الفرس، 2006، صفحة 216/3)، ووافقه الشنقيطي، فقال :" يفهم من هذه الآية لزوم الحكم بالقرينة الواضحة الدالة على صدق أحد الخصمين، وكذب الآخر؛ لأن ذكر الله لهذه القصة في معرض تسليم الاستدلال بتلك القرينة على براءة يوسف يدل على أن الحكم بمثل ذلك حق وصواب، لأن كون القميص مشقوقًا من جهة دبره دليل واضح على أنه هارب عنها، وهي تنوشه من خلفه" (الشنقيطي، 2019، صفحة 82/3).

ونوقش هذا الدليل من وجهين:

أ. أن هذا شرع من قبلنا، فلا يستدل به، وتعقب هذا الدليل، فقال ابن الفرس:" فإن قال القائل إن تلك الشريعة لا تلزمنا. قلنا كل ما أنزله الله تعالى علينا فإنما أنزله لفائدة فيه ومنفعة لنا وقال تعالى: "أُوْلَٰٓئِكَ ٱلَّذِينَ هَدَى ٱللَّهُۖ فَبِهُدَاهُمُ ٱقۡتَدِهۡۗ قُل لَّآ أَسۡـَٔلُكُمۡ عَلَيۡهِ أَجۡرًاۖ إِنۡ هُوَ إِلَّا ذِكۡرَىٰ لِلۡعَٰلَمِينَ " [الأنعام: 90] فآيات يوسف مقتدى بها، معمول بها" (ابن الفرس، 2006، صفحة 218/3).

ب. قال ابن الفرس:" وأنكر أبو الحسن-أي الصغير-العمل بالعلامات وقال: إنه اتفق على أنه لا يعمل، في غير الزوجين إذا تنازعا في شيء بمثل ما عمل فيها، قال: والأشبه في حديث يوسف أن ذلك كان آية من الله تعالى فليس في ذلك دلالة إلا من جهة خرق الله تعالى العادة في إنطاق الصبي في المهد..." (ابن الفرس، 2006، صفحة 219/3) .

فكون الناطق طفل صغير ضعيف، فقال ابن الفرس:" ويضعف هذا أن البخاري ومسلم أنه يتكلم في المهد إلا ثلاثة عيسى ابن مريم وصاحب جريج وابن السوداء التي دعت له أن يكون كالفاجر الخبيث وأسقط صاحب يوسف، وأسند الطبري إلى ابن عباس أنهم أربعة وزاد صاحب يوسف" (ابن الفرس، 2006، صفحة 319/2)، وقال القرطبي:" ولو كان طفلا لكانت شهادته ليوسف صلى الله عليه وسلم تغني عن أن يأتي بدليل من العادة، لأن كلام الطفل آية معجزة، فكادت أوضح من الاستدلال بالعادة" (القرطبي، 1964، صفحة 172/9) .

2. قال الله تعالى: وَجَآءُو عَلَىٰ قَمِيصِهِۦ بِدَمٍ كَذِبٍۚ قَالَ بَلۡ سَوَّلَتۡ لَكُمۡ أَنفُسُكُمۡ أَمۡرًاۖ فَصَبۡرٞ جَمِيلٞۖ وَٱللَّهُ ٱلۡمُسۡتَعَانُ عَلَىٰ مَا تَصِفُونَ. [يوسف: 18]، فقال القرطبي:" استدل الفقهاء بهذه الآية في إعمال الأمارات في مسائل من الفقه كالقسامة وغيرها، وأجمعوا على أن يعقوب عليه السلام استدل على كذبهم بصحة القميص، وهكذا يجب على الناظر أن يلحظ الأمارات والعلامات إذا تعارضت، فما ترجح منها قضى بجانب الترجيح، وهي قوة التهمة، ولا خلاف بالحكم بها" (القرطبي، 1964، صفحة 150/9).

3. عن زيد بن خالد الجهني: "أن النبي صلى الله عليه وسلم سأله رجل عن اللقطة فقال: اعرف وكاءها، أو قال وعاءها، وعفاصها، ثم عرفها سنة، ثم استمتع بها، فإن جاء ربها فأدها إليه. قال: فضالة الإبل؟ فغضب حتى احمرت وجنتاه، أو قال احمر وجهه، فقال: وما لك ولها، معها سقاؤها وحذاؤها، ترد الماء وترعى الشجر، فذرها حتى يلقاها ربها. قال: فضالة الغنم؟ قال: لك أو لأخيك أو للذئب" (البخاري، 2002، صفحة 30/1، رقم: 90)، فقال ابن القيم:" فجعل وصفه لها قائما مقام البينة، بل ربما يكون وصفه لها أظهر وأصدق من البينة" (ابن القيم، د.ت ، صفحة 11).

وساق ابن القيم الجوزرية(ابن القيم، د.ت ، صفحة 99)، وابن فرحون (ابن فرحون، 1986، الصفحات 117/2-120) ، الكثير من الأدلة، وخولفوا في ذلك من طرف أبي بكر الجصاص الحنفي (الجصاص، د.ت، صفحة 385/3)، والنجم الرملي الحنفي (ابن عابدين م.، د.ت، صفحة 205/7)، وأبي الحسن الصغير المالكي (ابن الفرس، 2006، صفحة 219/3)، الذين منعول العمل بالقرائن، ويُمكن أن يستدل لهم بأدلة:

أ. أن القرائن من باب الظن، والقضاء يوجب اليقين، ويرد على هذا بقول العز بن عبد السلام:" وإنما عمل بالظنون في موارد الشرع ومصادره؛ لأن كذب الظنون نادر وصدقها غالب؛ فلو ترك العمل بها خوفا من وقوع نادر كذبها لتعطلت مصالح كثيرة غالبة خوفا من وقوع مفاسد قليلة نادرة، وذلك على خلاف حكمة الإله الذي شرع الشرائع لأجلها" (ابن عبد السلام، 1991، صفحة 60/2).

ب. القرائن لا يمكن ضبطها، وبالتالي لا يمكن العمل وفقها، ويرد على هذا أن القرائن كبقية الأدلة منها الواهي، والضعيف، والصحيح،

وعليه فقول الجمهور أصح، وقد ثبت العمل بالقرائن في مواطن كثيرة جدا زمن الخلفاء الراشدين، فمن دونهم، وقال عوض عبد الله:" مع هذا التقدم العلمي الذي يشهده عالم اليوم أمكن التوصل إلى قرائن قوية تبين الحق وتعين على فهم الدعوى كالتحليلات المعملية من فحص للدم وغيره ومطابقة بصمات الأصابع ومضاهاة الخطوط وغير ذلك.

فإننا إذا أهملنا هذه القرائن وألقينا بها في البحر بحجة ما يتطرق إليها من الاحتمال لعرضنا الشريعة الإسلامية لتهمة الجمود وعدم مسايرة العصر، وهذا ما لم يقله إلا المكابر، فهي شريعة كل وقت وقانون كل جيل، وما هذه الفتاوى المأخوذة من أصولها المعروفة إلا دليل مرونتها وقابليتها لحكم الأجيال المتعاقبة. وعليه فإنه لا مناص من الأخذ بالقرائن والرجوع إليها في بناء الأحكام القضائية إذا لم يكن من دليل غيرها وفقاً على فتوى الكثيرين من الفقهاء"(أبو بكر، 2002، الصفحات 138-139).

حينما يأخذ التحقيق بالقرائن، ويرى ضرورة مراعاتها عند بناء الأحكام القضائية، فلا يلقى هذا على عواهنه، فالقرائن التي يحتكم إليها يشترط لها شروط هي:

1. أن تكون القرينة قوية، ووقوع الوهم فيها قليل

2. أن تكون القرينة متصلة بالحق اتصالاً مباشراً، وأن يكون الارتباط بينهما وثيقاً.

3. أن تكون القرينة مشروعة، فالوسائل لها حكم المقاصد شرعاً. (الزحيلي م.، أصول المحاكمات الشرعية، 1997، صفحة 205).

ولكي تكون هذه القرينة – الدليل الرقمي-مشروعاً وموافقاً للوسائل المنصوص عليها، فيحتاج إلى:

أ. أن توجد القرينة الواضحة والجلية في الإثبات، والدليل الرقمي دليلٌ واضح، بل هو في الكثير من الأحيان الدليل الوحيد الظاهر في الجرائم الإلكترونية، وقد يفوق في قوته بعض الأدلة المنصوص عليها، وهذا لكون القرائن تختلف زماناً، ومكاناً، وحالاً، والتكنلوجيا المعاصرة تفتح آفاق كبيرة في معرفة الجاني من خلال القرائن التي تحف الجريمة

ب. أن يكون هناك صلة قوية بين الأمر الثابت والاستنتاج التي يستخرج بواسطة الدليل الرقمي، فلا يكتفى بالاستنتاج الذي تكون قرينته خفية، فحينئذ يضعف الدليل الرقمي أمام الأدلة الأخرى التي يتمسك بها القاضي، وكلما كانت الصلة اقوى قدم الدليل الرقمي من باب ترجيح أدلة الإثبات بعضها على بعض (الزحيلي م.، وسائل الإثبات في الشريعة الإسلامية، 1982، الصفحات 488-489).

4.3. المطلب الثالث: الخصوصية في الدليل الرقمي ومشروعية الحصول عليه:

الشريعة الإسلامية حرمت التجسس في عموم الأحوال، ومن ذلك حرمة استراق النظر، فعن سهل بن سعد قال: "اطلع رجل من جحر في حجر النبي صلى الله عليه وسلم، ومع النبي صلى الله عليه وسلم مدرى يحك به رأسه، فقال: لو أعلم أنك تنظر، لطعنت به في عينك، إنما جعل الاستئذان من أجل البصر" (البخاري، 2002، صفحة 54/8، رقم: 6241).

وحق الخصوصية التي تكفل الشرع بحفظها، ليس على إطلاقه إذا وجد ما يجعله سبباً لضياع حق، أو لوقوع ظلم، وهذا من باب تدافع الأدلة وتقديم الأقوى منها فالأقوى، وحينئذ يجوز تفتيش ما يقضي القاضي بجوازه مما يعتقد كونه صالحاً للمساعدة في تفكيك الجريمة.

ويستدل لذلك بما رواه علي بن أبي طالب رضي الله عنه، فقال: "بعثني رسول الله صلى الله عليه وسلم أنا والزبير والمقداد بن الأسود قال: انطلقوا حتى تأتوا روضة خاخ فإن بها ظعينة ومعها كتاب فخذوه منها فانطلقنا تعادى بنا خيلنا حتى انتهينا إلى الروضة فإذا نحن بالظعينة فقلنا: أخرجي الكتاب فقالت: ما معي من كتاب فقلنا لتخرجن الكتاب أو لنلقين الثياب فأخرجته من عقاصها فأتينا به رسول الله صلى الله عليه وسلم..." (البخاري، 2002، صفحة 59/4، رقم: 3007)،

بوب له البخاري باباً، فقال:" باب من نظر في كتاب من يحذر على المسلمين ليستبين أمره" (البخاري، 2002، صفحة 57/8)، ونكت الحافظ فقال:" كأنه يشير إلى أن الأثر الوارد في النهي عن النظر في كتاب الغير يخص منه ما يتعين طريقا إلى دفع مفسدة هي أكثر من مفسدة النظر والأثر المذكور أخرجه أبو داود من حديث بن عباس بلفظ من نظر في كتاب أخيه بغير إذنه فكأنما ينظر في النار وسنده ضعيف...وقال المهلب في حديث علي هتك ستر الذنب وكشف المرأة العاصية وما روي أنه لا يجوز النظر في كتاب أحد إلا بإذنه إنما هو في حق من لم يكن متهما على المسلمين وأما من كان متهما فلا حرمة له" (ابن حجر، 1957، صفحة 47/11).

فظهر أن العبرة في ذلك هو القرينة التي تجعل القاضي يأمر بالتفتيش في أغراض المتهم، للوصول إليها، كل هذا ضمن الشروط الشرعية والقانونية العامة للتفتيش، فالدليل الرقمي دليل كبقية الأدلة ويخضع لكل ما تخضع له تلك الأدلة من المسالك الشرعية والقانونية.

4.4. المطلب الرابع: القوة الإثباتية للدليل الرقمي:

الدليل الرقمي قرينة توصل التحقيق للوصول للحق، وهذا ما يجعله مبنياً على مصداقية هذه القرينة في نفسها، وصلتها المنطقية الواضحة للدلالة على النتائج الصحيحة للتحقيق، والمصداقية في القرائن، فهي من اختصاص الخبراء الذين يقومون بالإجراءات القضائية، ومنها فحص الدليل الرقمي، ثم الحكم عليه من جهة صحته وعدم صحته أولاً، ثم الحكم عليه من جهة قوته وضعفه ثانياً، وبعد ذلك يبنون رأيهم بناءً على الخبرة العلمية التي عندهم.

وأما الصلة المنطقية بين الدليل الرقمي والنتائج، فهي بيد القاضي، الذي يقرر هذه الصلة أولاً، ثم قوتها ثانياً، وكل هذا من هلال نظره في قوة القرينة وصلتها مع القضية من جهات متعددة، بناءً على خبرته.

وبعد ذلك يكون الليل الرقمي بين حالات:

أ. أن يكون قوياً ثابتاً قطعياً، وتكون دلالته على المقصود مثله في القطع، فيقرر القاضي أن الدليل الرقمي دليلٌ نهائي، قاضٍ على علكل الأدلة، التي قد تطرق القضية من جهة أخرى، وبالتالي يكون هو الذي يقرر القاضي بناءً على ما فيه تكييف القضية وجهات الجناية فيها، وهذا مثل أشرطة الفيديو، والتصوير التي تثبت الجهات والخبرات العلمية صحتها، وسلامتها.

ب. أن يكون الدليل الرقمي مشكوكاً فيه، لا يبلغ في قوته درجة اليقين، مثل التسجيلات الصوتية، أو التسجيلات المرئية التي يختلف الخبراء في صحتها، فالقاضي سيتوقف في الأخذ به؛ لضعفه وعدم صحته

ت. أن يكون الدليل الرقمي مفيداً لغالب الظن، كالتسجيلات الصوتية، أو المرئية، التي يتغلب على ظن الخبراء صحتها، دون الجزم القاطع، وهنا القاضي سيقوم بترجيح ما عنده من الحجج والأدلة، بهذا الدليل الرقمي، الذي سيكون دليلاً من أدلة الترجيح لا غير، قال الشنقيطي:" بين في موضع آخر أن محل العمل بالقرينة ما لم تعارضها قرينة أقوى منها، فإن عارضتها قرينة أقوى منها أبطلتها، وذلك في قوله تعالى: وَجَآءُو عَلَىٰ قَمِيصِهِۦ بِدَمٍ كَذِبٍۚ قَالَ بَلْ سَوَّلَتْ لَكُمْ أَنفُسُكُمْ أَمْرًاۖ **سجى** [يوسف:18]؛ لأن أولاد يعقوب لما جعلوا يوسف في غيابة الجب، جعلوا على قميصه دم سخلة؛ ليكون وجود الدم على قميصه قرينة على صدقهم في دعواهم أنه أكله الذئب" (الشنقيطي، 2019، صفحة 82/3).

ثم الدليل الرقمي، قد يُخالف غيره من الأدلة الشرعية في الجنايات في أمرين مهمين

أولاً: إن الدليل الرقمي ليس دليلاً مباشراً، وهذا راجع لطبيعته التقنية، مع كونه عرضة لتدخل الخبراء في الحكم عليه صحة وبطلاناً، وقوة وضعفاً، فهو دليل يلجأ إليه لمعاضدة الأدلة الأخرى، من باب الإرشاد والتدليل على صحتها، ولا يمنع هذا أن يكون الدليل مرشداً، أو مرجحاً قوياً، ويحق للقاضي أن يقَّوي حدة الدليل الرقمي من خلال أدلة شرعية أخرى، كتحليف المتهمين باليمين، على صحة الدليل الرقمي، أو على عدم صحته (حسام، 2021، صفحة 187).

ثانياً: الدليل الرقمي دليلٌ عام، يمكن استخدامه في كل القضايا، سواء كانت تتعلق بحقوق الله، أو حق الآدميين، أو بالقضايا الجنائية، أو القضايا المدنية، وقد يستثنى من ذلك:

أ. الحدود الشرعية: فالشريعة الإسلامية ضيقت الأدلة الشرعية في قضايا الحدود وربطتها بقاعدة "درء الحدود بالشبهات"، فقال ابن المنذر:" وأجمعوا على أن درء الحد بالشبهات" (ابن المنذر، 2004، صفحة 118)، وقال كذلك:" وكل من نحفظ عه من أهل العلم يرى أن يدرأ الحد في الشبهة" (ابن المنذر، الإشراف إلى مذاهب العلماء، 2004، صفحة 291/7).

فأيُّ شبهة تدخل الدليل المادي تكون عائقاً أمام تطبيق الحد الشرعي، بناءً على هذه القاعدة، وكل الأدلة الرقمية قد تعارض من جهتين:

أ. دخول التزييف والتزوير فيها، وهذا لتقدم التطور التكنولوجي الذي يكون مساعداً في مواضع كثيرة، لكنه في الوقت نفسه يكون عائقاً في مواطن أخرى، وقد وقع الخلط بين الأدلة الصحيحة والمزورة في قضايا كثيرة.

ب. عدم توسيع دائرة التجسس والتفتيش، واحترام خصوصية الناس؛ لأنه الأصل، فرعاية هذا الأصل لا يخرجه عنه غلا الدليل الجلي الواضح، وفتح هذا الباب قد يؤدي إلى انتهاك حرمة الناس.

ولهذا كان الإنصاف أن لا يكون الدليل الرقمي حجة في القضايا المتعلقة بالحدود، بل يكون مرجحاً، أو شاهداً مع غيره من الأدلة الشرعية (أبو صفية، 2009، صفحة 77).

5. خاتمة:

في ختام هذه الدراسة، تظهر بعض النتائج المهمة، وهي:

1. أن الجريمة الإلكترونية في الشريعة الإسلامية لها ثلاثة أركان، كباقي الجرائم، ركن شرعي، ومادي، وأدبي

2. أن الدليل الرقمي له طرق لتحصيله، كالمعاينة، والتفتيش، والخبرة التقنية.

3. أن أدلة الإثبات في القضاء الشرعي ليست محصورة في المنصوص عليه، بل كل ما يصح تسميته بالبيّنة الشرعية فهو دليل قضائي.

4. أن القرائن من أدلة إثبات الأدلة في القضاء الشرعي، والدراسة بيَّنت أن الدليل الرقمي يُكيَّف على أنه من باب القرائن الشرعية.

5. لكي تكون القرينة معتبرة لابد لها من ثلاثة شروط، وهي: أن تكون القرينة قوية، ووقوع الوهم فيها قليل، وأن تكون متصلة بالحق اتصالاً مباشراً، وأن يكون الارتباط بينهما وثيقاً، وأن تكون مشروعة، فالوسائل لها حكم المقاصد شرعاً.

6. أن الشريعة الإسلامية تحترم الخصوصية، ولهذا لا بدَّ ألا يتوسع في الدليل الرقمي لخرق هذا الأصل الشرعي.

7. القوة الإثباتية للدليل الرقمي تكون وفق قوة القرينة التي تدل عليه، وقوة اتصالها بالقضية، ولطبيعة الدليل الرقمي فالقاضي لا يمكنه الاستدلال به لوحده في القضايا المتعلقة بالحدود الشرعية لأنها منضبطة بقاعدة "درء الحدود بالشبهات".

ولهذا **توصي الدراسة** بزيادة البحوث المتعلقة بالأدلة الرقمية في الشريعة؛ لأجل أن الأدلة الرقمية يزداد نوعها يوماً بعد يوم؛ لأجل التطور التكنولوجي الذي تعيشه البشرية، وتزداد البحوث أهمية بكونها في قضايا الجرائم والجنايات، لما لذلك من الأهمية الكبيرة في حفظ حقوق الناس.

قائمة المراجع:

1) إبراهيم بن علي ابن فرحون. (1986). تبصرة الحكام في أصول الأقضية ومناهج الحكام (المجلد 1). القاهرة: مكتبة الكليات الأزهرية.

2) أحمد بن عبد الحليم ابن تيمية. (1995). مجموع الفتاوى (المجلد 1). (عبد الرحمن ابن قاسم، المحرر). السعودية: مجمع الملك فهد.

3) أحمد بن علي ابن حجر. (1957). فتح الباري شرح البخاري (المجلد 1). (فؤاد عبد الباقي، المحرر). القاهرة:: الدار السلفية.

4) أحمد بن علي الجصاص. (د.ت). أحكام القرآن. (محمد قمحاوي، المحرر) بيروت: دار إحياء التراث.

5) أمير فرج يوسف. (2006). الجرائم المعلوماتية على الأنترنيت. الاسكندرية: دار المطبوعات.

6) زين الدين بن إبراهيم ابن نجيم. (د.ت). البحر الرائق شرح كنز الحقائق (المجلد 2). بيروت: دار الكتاب الإسلامي.

7) صلاح الدين حسام. (2021). حجية الدليل الرقمي في النظام القضائي الإسلامي. مجلة الدراسات الفقهية، العدد 37.

8) عبد العزيز ابن عبد السلام. (1991). قواعد الأحكام (المجلد 1). بيروت: دار الكتب العلمية.

9) عبد الفتاح بيومي. (2008). الدليل الجنائي والتزوير في الجرائم الإلكترونية . القاهرة: دار الكتب.

10) عبد القادر عودة. ((د.ت)). التشريع الجنائي الإسلامي مقارنة بالقانون الوضعي. بيروت: دار الكتاب العربي.

11) عبد الله بن أحمد ابن قدامة. (1997). المغني شرح الخرقي. (عبد الله بن عبد المحسن التركي، المحرر) السعودية: دار عالم الكتب.

12) عبد المنعم بن عبد الرحيم ابن الفرس. (2006). أحكام القرآن (المجلد 1). بيروت: دار ابن حزم.

13) عوض عبد الله أبو بكر. (2002). نظام الإثبات في الفقه الإسلامي. مجلة المدينة النبوية، العدد 62.

14) فخري أبو صفية. (2009). مدى حجية وسائل الإثبات المعاصرة في القضاء. جامعى الأمير عبد القادر، المجلد 24، العدد1.

15) قطب الريسوني. (2014). صناعة الفتوى في القضايا المعاصرة (المجلد 1). بيروت: بن حزم.

16) محمد بن أحمد القرطبي. (1964). أحكام القرآن (المجلد 2). (احمد البردوني، و إبراهيم أطفيش، المحررون) القاهرة: دار الكتب العلمية.

17) محمد ابن المنذر. (2004). الإجماع. (فؤاد عبد المنعم، المحرر). الرياض: دار المسلم.

18) محمد ابن المنذر. (2004). الإشراف إلى مذاهب العلماء (المجلد 1). (صغير احمد الأنصاري، المحرر). الإمارات المتحدة: مكتبة مكة.

19) محمد الأمين الشنقيطي. (2019). اضواء البيان في تفسير القرآن بالقرآن (المجلد 5). الرياض: عطاءات العلم.

20) محمد الزحيلي. (1982). وسائل الإثبات في الشريعة الإسلامية (المجلد 1). سوريا: مكتبة الريان.

21) محمد الزحيلي. (1997). أصول المحاكمات الشرعية (المجلد 1). سوريا: دامعة دمشق.

22) محمد أمين ابن عابدين. (1966). الدر المحتار على الدر المختار (المجلد 2). مصر: مصطفى الحلبي.

23) محمد أمين ابن عابدين. (د.ت). حاشية على البحر الرائق شرح كنز الحقائق (المجلد 2). بيروت: دار الكتاب الإسلامي.

24) محمد بن أبي بكر ابن القيم. (د.ت). الطرق الحكمية. القاهرة: مكتبة الريان.

25) محمد بن أحمد ابن جزي. ((د.ت)). القوانين الفقهية (المجلد (د.ط)). (د.ن).

26) محمد بن أحمد الخطيب الشربيني. (1994). مغني المحتاج (المجلد 1). بيروت: دار الكتب العلمية.

27) محمد بن إسماعيل البخاري. (2002). الجامع الصحيح . (محمد الناصر، المحرر). بيروت: دار الطوق.

28) محمد بن علي ابن دقيق العيد. (د.ت). إحكام الإحكام شرح عمدة الأحكام. مصر: لمكتبة المحمدية.

29) محمد بن علي الشوكاني. (1993). نيل الأوطار شرح منتقى الأخبار(المجلد 1). (عصام الصباطي، المحرر) مصر: دار الحديث.

30) محمد شلتوت. (2001). الإسلام عقيدة وشريعة (المجلد 18). مصر: دار الشروق.

31) محمد عثمان شبير. (2014). التكييف الفقهي للوقائع المستجدة. دمشق: دار القلم.

32) مراد فلاك. (2019). آليات الحصول على الأدلة كوسائل إثبات في الجريمة الإلكترونية. مجلة الفكر القانوني والسياسي(م3، ع1).

33) مصطفى الزرقا. (2004). المدخل الفقهي العام (المجلد 2). سوريا: دار القلم.

34) وزارة الأوقاف الكويتية. (1427). الموسوعة الفقهية الكويتية (المجلد 2). الكويت: مطبعة وزارة الأوقاف الكويتية.

35) وهبة الزحيلي. ((د.ت)). الفقه الإسلامي وأدلته (المجلد 4). بيروت: دار الفكر.

الجريمة الإلكترونية كمظهر لأشكال الجرائم الحديثة وتصنيفاتها

Cybercrime as a manifestation of modern crime forms and their classifications

د.أمين مخفوظي/ جامعة المدية/الجزائر
Dr. Amine Mahfouzi/ Medea University/ Algeria

ملخص الدراسة:

إن الاهتمام بالطفل هدف من أعز الأهداف التي تسعى جميع الأقطار العربية إلى تحقيقها، فالاهتمام بمستقبل الطفل هو في الحقيقة ضمان مستقبل شعب بأسره، لأن الطفولة هي صانعة المستقبل، وإن أطفال اليوم هم رجال الغد فالطفل هو الثروة الحقيقية للوطن العربي ، وهو الأمل في الحاضر والمستقبل، فالأطفال يشكلون أهم نواة في المجتمع ولذلك نجد جميع العهود والمواثيق التي تتكلم عن الطفولة ببالغ من الأهمية حيث نجد إنعقاد عدة مؤتمرات عالمية ومنها القمة العالمية من أجل الطفل والذي عقد تحت رعاية هيئة الأمم المتحدة في سبتمبر 1990، وعلى المستوى الوطني نجد المجلس العربي للطفولة الذي يقدم خدماته للطفل في كافة الدول العربية ، كما أن هناك اتفاقيات عالمية حقوق الطفل، هذا الاهتمام المتزايد من طرف الدول على المستوى العالمي بالطفل جعل من الطفل محور حياة الإنسان الذي بطبيعة الحال ينطلق من الطفولة وصولا إلى الشيخوخة، لذلك كان من الضروري وضع الآليات المناسبة لحماية هذا الطفل ووقايته من كل أشكال الجريمة وخاصة التي المتعلقة بالجرائم الرقمية التي باتت تهدد البشرية جمعاء بما بالك بالطفل القاصر،

الكلمات المفتاحية: الحماية القانوني، الطفل، المجني عليه، المعرض للخطر، الجرائم الرقمية

Abstact :

Caring for the child is one of the dearest goals that all Arab countries seek to achieve. Caring for the future of the child is in fact ensuring the future of an entire people, because childhood is the maker of the future, and today's children are the men of tomorrow. The child is the real wealth of the Arab world, and it is the hope in the present and the future Children constitute the most important nucleus in society, and therefore we find all the covenants and charters that talk about childhood very important, as we find the convening of several international conferences, including the World Summit for Children, which was held under the auspices of the United Nations in September 1990, and at the national level we find the Arab Council for Childhood, which It provides its services to children in all Arab countries, and there are international agreements on the rights of the child. This increasing interest on the part of states at the global level in the child has made the child the center of human life, which naturally proceeds from childhood to old age, so it was necessary to put in place appropriate mechanisms to protect This child and his protection from all forms of crime, especially those related to digital crimes that threaten all of humanity, including what you think of the minor child.

Keywords : legal protection, child, victim, at risk, digital crimes

مقدمة:

يعد الطفل في عالمنا اليوم النموذج الأمثل للضحية لكثرة الجرائم التي يقع فريسة لها وذلك نظرا لما يمتاز به من صفات جسدية تكوينية ونفسية واجتماعية تجعل الجرائم المرتكبة ضده تختلف عن الجرائم المرتكبة ضد الأشخاص البالغين (سليمان، والعبيد،2010، ص.211)

وقد عنيت اتفاقية حقوق الطفل بتكريس حماية للطفل من جميع أشكال الإيذاء البدني والعقلي والاستغلال الجنسي وغيره ووجوب اتخاذ الإجراءات الكفيلة بمنع ذلك بما فيها تدخل القضاء (بولحية، 2010، ص. 65) وهو النهج الذي سار عليه المشرع الجزائري وذلك بتجريمه لأي فعل يمس الطفل ويهدد كيانه.

ويعتبر تعرض الطفل للعنف من قبل أسرته من أسوء أشكال الإساءة التي قد يتلقاها في حياته، والتي لها أثار سلبية على الصعيد البدني أو الذهني أو الاجتماعي ولذلك وضع المشرع الجزائري نصا دستوريا يحث الآباء على حماية الأبناء في المادة 65 منه تنص المادة 65 من الدستور "يجازى القانون الآباء على القيام بواجب تربية الأبناء و رعايتهم "، ويمنع العنف ضد الطفل الذي يجعله يعيش وضعا اجتماعيا صعبا يهدد بقائه ونمائه وهو ما يسمى بالطفولة المتواجدة في خطر ولي معالجة الجرائم التي يتعرض لها الطفل المجني عليه والموجود في خطر قسمنا هذا الفصل إلى مبحثين: في المبحث الأول: نتعرض فيه إلى الحماية الجزائية للطفل المجني عليه وذلك بتبيان اخطر الجرائم أما في المبحث الثاني: نتعرض فيه إلى الحماية القانونية للطفل المعرض للخطر.

المبحث الأول: الحماية الجزائية للطفل المجني عليه

لقد أيقن المشرع الجزائري بأن الطفل هو ذلك الإنسان الذي لم تتوفر لديه الملكات العقلية والجسمية الكافية وجاءت إرادته لتراعي هذه الحقيقة، وقد برهنت على هذا الاهتمام نصوص التشريع العقابي سواء قانون العقوبات أو القوانين المكملة له وذلك بإقراره حماية خاصة للأطفال من الاعتداءات التي يتعرضون لها حماية متميزة عن تلك التي أعدها للبالغين، علاوة عن ذلك ما فرضه من عقوبات جزائية على كل مساس بحق الطفل في العيش أو المساس بسلامة جسمه أو تعرضه للخطر وتحريضه على الانحراف.

إن المتصفح لقانون العقوبات وعلى غرار غيره من القوانين الأخرى نجده قد أولى أهمية كبيرة لهذه الفئة الضعيفة من المجتمع وجعل من صفة قصر الضحية كركن من أركانها وسبب في تشديد العقاب وهو الشيء الذي كرسه تعديل قانون العقوبات 14-01 المؤرخ 04 /2014/02، فالمشرع حاول الإلمام بكافة الجرائم التي طالت هذه البراءة، كما جاء قانون حماية الطفل 15-12 المؤرخ في 2015/07/15 ليعزز هذه الحماية إذ تنص المادة5 منه على أنه يقع على عاتق الوالدين مسؤولية حماية الطفل في حين تنص المادة 6 على أن الدولة تكفل حق الطفل في الحماية من كافة أشكال الضرر أو الإهمال أو العنف أو سوء المعاملة أو الاستغلال أو الإساءة البدنية أو المعنوية أو الجنسية وتتخذ من أجل ذلك كل التدابير اللازمة للوقاية وقد تم تقسيم الجرائم التي يتعرض لها الطفل تبعا للحق المعتدي عليه وهي على النحو التالي في المطلب الأول نتناول حماية حق الطفل في الحياة وسلامة جسمه أما في المطلب الثاني

نتعرض لحماية حق الطفل في صيانة عرضه وأخلاقه وأخيرا المطلب الثالث: حماية الطفل من جرائم المتعلقة بالوضعية الاجتماعية والعائلية .

المطلب الأول: حماية حق الطفل في الحياة وسلامة جسمه

لقد نصت المادة 6 من المرسوم الرئاسي رقم 92-461 والمؤرخ في 19ديسمبر 1992 والمتضمن المصادقة على التصريحات التفسيرية على اتفاقية حقوق الطفل التي وافقت عليها الجمعية العامة للأمم المتحدة والتي تعهدت الجزائر بأن تكفل لكل طفل حقا أصيلا في الحياة وأن تسير وظائفه الحيوية سيرا طبيعيا

كما أشارت المادة 19 من المرسوم السابق الذكر أن تتخذ الجزائر جميع التدابير التشريعية والإدارية والاجتماعية لحمايته من كافة أشكال العنف والضرر والإساءة البدنية والعقلية فما هي الجرائم التي نص عليها المشرع؟ وهل هي كافية بحماية هذه الحقوق؟

للإجابة على هذه الإشكالية سلطا الضوء على أكثر الجرائم التي يتعرض لها الطفل حاليا والتي تشكل أكثر القضايا المجدولة في محكمة الجنايات وأقسام الجنح وهي التي سنفصلها في الفروع الثلاثة الآتية:

الفرع الأول نتناول جريمة قتل الطفل أما في الفرع الثاني ندرس جرائم خطف القصر وأخيرا في الفرع الثالث نتعرض إلى جريمة بيع الأطفال والاتجار بهم.

الفرع الأول: جريمة قتل الطفل

لقد حرص المشرع على حماية حق الطفل في الحياة وشدد العقوبات على من يعتدي على هذا الحق وتظهر من خلال تجريم قتل الطفل حديث العهد بالولادة كتجريم خاص إذا كان الفاعل هي الأم وتطبق أحكام المادة 261فقرة أولى إذا كان الفاعل شخصا أخر.

أولا-قتل طفل حديث العهد بالولادة:

لم يعرف المشرع الجزائري ما هو المقصود بجريمة قتل الطفل بل اكتفى في المادة 259 من قانون العقوبات بالنص على أن قتل الطفل هو إزهاق روح طفل حديث العهد بالولادة

1 . أركان الجريمة: الركن المادي: تشترط هذه الجريمة شرطين:

الشرط الأول: يجب أن يقع القتل على مولود حديث العهد بالولادة أما عن تحديد وصف حداثة العهد بالولادة فهي متروكة للقاضي وقد حددها القانون الفرنسي بانقضاء اجل تسجيل المولود في سجلات الحالة المدنية وهو محدد بخمسة أيام في القانون الجزائري.

الشرط الثاني: يجب أن يكون القتل قد وقع من الأم وهو الأمر الذي حددته المادة 2/261 التي حددت الشخص الجاني بالأم وغير الأم مهما ربطته بالأم علاقته كالزوج والأخ والأب لا ينطبق عليه هذا السبب وتشدد المحكمة العليا

على أن يتضمن حكم الإدانة عنصر الجريمة لاسيما كون الطفل ولد حيا وكون الجانية أم المجني عليه (بوسقيعة، 2013، ص.38)

الركن المعنوي: هي منى الجرائم العمدية التي تتطلب توفر القصد الجنائي العام وانصرف إرادة الأم إلى ارتكابها مع علمها بكافة العناصر وقصد خاص وهو أن تتجه إرادة الأم إلى إزهاق روح الطفل.

العقوبة: هي عقوبة مخففة وهي السجن المؤقت من 10 إلى 20 سنة فهي عقوبة مقررة للأم فقط دون من ساهم أو شارك معها في ارتكابه

ثانيا: خضوع جريمة قتل الطفل للقواعد العامة: أن جريمة إزهاق روح الطفل من غير الأم تخضع للقواعد العامة وتطبق عليها أحكام المواد 254 و 1/26 من قانون العقوبات.

الركن المادي: يتمثل في السلوك الإجرامي وهو الفعل الموجه للقضاء على حياة الطفل وإزهاق روحه باعتباره إنسانا ولا عبرة بالوسيلة التي حقق الجاني بها فعل القتل والنتيجة: وهي إزهاق روح الطفل ولا يشترط تحقيق النتيجة مباشرة إثر نشاط الجاني إذ يمكن أن يكون هناك فاصل زمني بين الفعل والوفاة والرابطة السببية أن يكون سلوك الجاني هو المؤدي إلى تحقيق نتيجة الوفاة.

الركن المعنوي: يتكون من القصد العام وهو انصراف إرادة الجاني إلى تحقيق الجريمة مع علمه بعواقب فعله والقصد الخاص وهو نية إزهاق روح الطفل.

العقوبة: تطبق عليهم العقوبة المنصوص عليها في المادة 3/263 وهي السجن المؤبد ولكن هذه العقوبة لم تحقق الغرض ولم تحقق الردع المطلوب منها إذ تضاعفت جرائم قتل الأطفال أين تصدر الأب قائمة الفاعلين ولكن رغم ذلك فالمشرع الجزائري لم يحرك ساكنا فيما يخص هذه الأخيرة رغم قيامه بتعديل قانون العقوبات بتاريخ 2014/02/04 إلا انه لم يدخل أي تعديل على العقوبة المقررة في هذه الحالة بل سواها مع العقوبة المقررة في حالة كون المجني عليه بالغ ولكن الأمر ليس سواء فالطفل هو أحد ظروف التشديد وعليه ندعو المشرع إلى تعديل هذه المادة أو بالأحر سن مادة خاصة بالطفل وحده خاصة بعد صدور خاص بحمايته .

الفرع الثاني: جرائم خطف القصر

وهي من بين الجرائم التي تطرق إليها قانون العقوبات والتي أصبحت هاجسها يطارد كل طفل والتي راح ضحيتها العديد من الأبرياء نذكر منهم كل من: شيماء، مهدي، هارون وإبراهيم رحمة الله عليهم. (أنظر الحكم الجنائي الصادر عن محكمة الجنايات بمجلس قضاء قسنطينة بتاريخ 2013/07/21 تحت رقم فهرس 2013/208)

وتعرف أنها الاعتداء المتعمد الذي يقع على الحرية الفردية للشخص فيقيدها ويكون للاعتداء أسباب متعددة: الرغبة في الحصول على المال عن طريق الابتزاز والتهديد أو طلب فدية أو لأسباب سياسية ودون سند قانوني وخارج الحالات التي يسمح بها القانون وخطف الطفل هو انتزاعه من بيئته بقصد نقله إلى مكان أخر وإخفائه عن ذويه.

من اجل وضع حد للخطف وحماية للطفل المخطوف والتمكن من إيجاده بسرعة سمحت المادة 47 من قانون حماية الطفل لوكيل الجمهورية اتخاذ مجموعة من الإجراءات إذ تنص المادة على ما يلي: "يمكن لوكيل الجمهورية المختص، بناء على طلب أو موافقة الممثل الشرعي لطفل تم اختطافه، أن يطلب من أي عنوان أو لسان أو سند إعلامي نشر إشعارات و/أو أوصاف و/أو صور تخص الطفل، قصد تلقي معلومات أو شهادات من شأنها المساعدة في التحريات والأبحاث الجارية، وذلك مع مراعاة عدم المساس بكرامة الطفل و/او حياته الخاصة.

غير أنه يمكن لوكيل الجمهورية، إذا اقتضت مصلحة الطفل ذلك أن يأمر بهذا الإجراء دون القبول المسبق للمثل الشرعي للطفل "

وتجدر الإشارة إلى أن الخطف له نفس معنى الاختطاف فهما يشكلان جريمة واحدة، كما أن المشرع الجزائري لم يورد تعريفا مفردا لهذه الكلمة بل يلحق بها دائما مفردات أخرى: إبعاد، حجز، حبس، قبض.

أولا: صور جريمة خطف القصر: وتأخذ جريمة خطف القصر صورتين هما:

1.جريمة الخطف أو محاولة الخطف باستعمال العنف أو التهديد أو الاستدراج:

المنصوص عليها في المادة 293مكرر 1 التي استحدثت بموجب القانون رقم 14-01 مؤرخ في 2014/02/04 المتضمن تعديل قانون العقوبات على ما يلي : "يعاقب بالسجن المؤبد كل من يخطف أو يحاول خطف قاصر لم يكمل 18 سنة عن طريق العنف أو التهديد أو الاستدراج أو غيرهما من الوسائل، وتطبق على الفاعل العقوبة المنصوص عليها في الفقرة 1 من المادة 263 من هذا القانون (الإعدام) إذا تعرض القاصر المخطوف إلى تعذيب أو عنف جنسي أو إذا كان الدافع إلى الخطف هو تسديد فدية أو إذا ترتب عليه وفاة الضحية ولا يستفيد الجاني من ظروف التخفيف المنصوص عليها في هذا القانون مع مراعاة أحكام المادة 294 أدناه " الامر 66-156 المؤرخ في 1966/06/8 المتضمن قانون العقوبات جريدة رسمية عدد49 المؤرخة في 1966/06/11 المعدل و المتمم بالقانون 14-01 المؤرخ في 04-02-2014 جريدة رسمية عدد 07 المؤرخ في 2014/02/16 .

من خلال المادة نستنتج وصف الجريمة هي جناية وان أركانها تتمثل في ركن مادي يتوفر عن طريق النشاط الإرادي الذي يأتيه الفاعل ويتمثل في الخطف أو الحجز أو النقل وقد يجتمع أكثر من فعل واحد ويكون مصحوبا باستعمال أساليب العنف أو التهديد أو الاستدراج أو غيره من وسائل الغش والخداع والركن المعنوي الذي يتمثل في انصراف إرادة الجاني إلى ارتكاب جريمة خطف مع علمه بأنه يوجه فعله إلى طفل لم يكمل 18 سنة.

2. جريمة خطف أو إبعاد قاصر دون عنف آو تهديد أو تحايل: هي عبارة عن جنحة منصوص عليها بالمادة 326 من قانون العقوبات، وتقوم جريمة الخطف في هذه الصورة حتى وان رافق القاصر الجاني بمحض إرادته، ومن الجرائم الملحقة بهذه الصورة نجد:

أ) جريمة محاولة خطف آو إبعاد قاصر المادة 326 ق ع: "كل من خطف أو ابعد قاصرا لم يكمل الثامنة عشرة وذلك بغير عنف أو تهديد أو تحايل أو شرع في ذلك فيعاقب بالحبس لمدة سنة إلى خمس سنوات وبغرامة من 20.000 إلى 100.000 دينار.

وإذا تزوجت القاصر المخطوفة أو المبعدة من خاطفها فلا تتخذ إجراءات المتابعة الجزائية ضد الأخير إلا بناءا على شكوى الأشخاص الذين لهم صفة في طلب إبطال الزواج ولا يجوز الحكم عليه إلا بعد القضاء بإبطاله." وقد قضت المحكمة العليا بأن محاكمة متهم وإدانته من أجل جنحة إبعاد قاصر بغير عنف رغم معاينة واقعة الزواج وتنازل الطرف المدني مخالفتان للقانون (قرار المحكمة العليا رقم 313712 صادر بتاريخ 2006/04/26 ، مجلة المحكمة العليا عدد 1 ، ص.579).

ب)– **جريمة إخفاء قاصر كان قد خطف أو ابعد أو هربه من البحث عنه المادة 329 ق ع:** " كل من تعمد إخفاء قاصر كان قد خطف أو أبعد أو هربه من البحث عنه وكل من أخفاه عن السلطة التي يخضع لها قانونا، يعاقب بالحبس من سنة إلى خمس سنوات وبغرامة من 20.000 إلى 100.000 دينار أو بإحدى هاتين العقوبتين، وذلك فينا عدا الحالة التي يكون فيها الفعل جريمة اشتراك معاقب عليها . وتأخذ هذه الجنحة ثلاثة صور وهي:

1. إخفاء قاصر كان قد خطف
2. تهريب القاصر من البحث عنه بعد خطفه أو إبعاده
3. إخفاء الطفل عن السلطة التي يخضع لها قانونا: وتتطلب هذه الصورة ما يلي:

- ✓ أن يكون القاصر محل أحد التدابير الحماية والتهذيب المنصوص عليها في المادة 444 ق إ ج.
- ✓ أن يكون قرار الوضع أو التسليم صادر عن قاضي الأحداث.
- ✓ أن يكون القاصر قد فر من تلك المؤسسة.

3. العقوبة المقررة لجرائم الخطف:

. **جريمة خطف أو محاولة خطف قاصر دون عنف او تهديد أو تحايل:** تنص المادة 326 انه تكون العقوبة الحبس من سنة إلى خمس سنوات وغرامة من 20.000الى 100.000 دج علاوة على العقوبة التكميلية الاختيارية المقررة للجنح في المادة 9 من قانون العقوبات.

- **جريمة إخفاء قاصر كان قد خطف أو ابعد أو هرب من البحث عنه:** هي جنحة تعاقب عليها المادة 329 كما يلي هي جنحة عقوبتها الحبس من سنة إلى خمس سنوات وغرامة من 20.000 إلى 100.000 دج أو بإحدى هاتين العقوبتين فيما عدا الحالة التي يكون فيها الفعل جريمة اشتراك معاقب عليها.
- **جريمة الخطف أو محاولة الخطف باستعمال العنف أو التهديد أو الاستدراج:** تنص عليه المادة 293مكرر1 أن العقوبة المقررة هي المؤبد، وفي حالة تعرض المخطوف إلى التعذيب أو عنف جنسي أو كان الدافع إلى الخطف هو تسديد فدية أو إذا ترتبت عليه وفاة الضحية تكون العقوبة هي الإعدام وهي العقوبة المنصوص عليها في المادة 263.

ملاحظة: نلاحظ أن المشرع شدد العقوبة المتعلقة بجريمة خطف القاصر مقارنة بالعقوبة المقررة لجريمة خطف شخص بالغ المعاقب عليها بموجب المادة 293 مكرر وهي السجن المؤقت من 10الى 20 سنة وذلك بموجب تعديل قانون العقوبات بقانون 14-01 وقد كان قبل ذلك يخضع لنفس العقوبة وذلك حماية منه للقاصر الذي يسهل تنفيذ هذه الجريمة عليه بسبب ضعفه وعدم قدرته على المقاومة.

كما نصت المادة 293 مكرر 1 انه لاستفيد الجاني من ظروف التخفيف، مع مراعاة أحكام المادة 294 التي تنص على أعذار مخففة يستفيد منها الجني إذا وضع فورا حدا للحبس أو الحجز أو الخطف حسب مفهوم المادة 52 من قانون العقوبات وذلك على النحو التالي:

يستفيد الجاني من الأعذار المخففة حسب مفهوم المادة 52 إذا وضع فورا حدا للحبس أو الحجز أو الخطف.

إذا انتهى الحبس أو الحجز بعد اقل من عشر 10 أيام كاملة من يوم الاختطاف أو القبض أو الحبس أو الحجز وقبل اتخاذ أية إجراءات تخفض العقوبة إلى الحبس من سنتين إلى خمس سنوات في الحالة المنصوص عليهما في المادة 293 وإلى الحبس من ستة أشهر إلى سنتين في الحالتين المنصوص عليهما في المادتين 291 و292.

وإذا انتهى الحبس أو الحجز بعد أكثر من عشرة أيام كاملة من يوم الاختطاف أو القبض أو الحبس أو الحجز بعد أكثر من عشرة أيام كاملة من يوم الاختطاف أو القبض أو الحبس أو الحجز وقبل الشروع في عملية التتبع فتخفض العقوبة إلى الحبس من خمس إلى عشر سنوات في الحالة المنصوص عليها في المادة 293 والى الحبس من سنتين إلى خمس سنوات في جميع الحالات الأخرى.

تخفض العقوبة إلى السجن المؤقت من خمس إلى عشر سنوات في الحالة المنصوص عليها في الفقرة الأولى من المادة 293 مكرر، والى السجن المؤقت من عشر إلى عشرين سنة في الحالات الواردة في الفقرتين 2و 3 من نفس المادة.

ملاحظة: المشرع لم يذكر المادة 293 مكرر 1 ضمن حالات الاستفادة من الأعذار المخففة المنصوص عليها 294 ولكن استقراء نص المادة نجدها تحمل عبارة «مع مراعاة أحكام المادة 294 أدناه " وهو ما يؤكد على سهوه ولكن نظر لعدم جواز القياس ومبدأ التفسير الضيق للنص التشريعي يتعين النص عليها في فحوى المادة مادامت تخدم مصلحة القاصر وتدفع الجاني إلى التراجع.

***جريمة إخفاء قاصر بعد خطفه أو إبعاده**: عقوبة الفعل منصوص عليها في المادة 329 وهي الحبس من سنة إلى خمس سنوات وغرامة من 20.000 إلى 100.000 دج أو إحدى هاتين العقوبتين، علاوة على العقوبات التكميلية الاختيارية المقررة للجنح.

الفرع الثالث: جريمة بيع الأطفال والاتجار بهم:

وهي الجريمة المنصوص والمعاقب عليها بنص المادة 319 مكرر من قانون العقوبات ، ولم يكن المشرع الجزائري يعاقب على جريمة المتاجرة بالأطفال بصورة مستقلة ، بل ادخلها ضمن جرائم الاتجار بالأشخاص المنصوص عليها في

المادة 303 مكرر 4 فقرة 2 من قانون العقوبات التي اعتبرت ضعف الضحية الناتج عن سنها ظرفا مشدد عند معاقبة مرتكبي هذه الجرائم وكذلك المادة 303 مكرر 20 التي تعاقب على الاتجار بالأشخاص بعقوبة مشددة عندما تكون الضحية قاصرا أو شخصا مصابا بإعاقة ذهنية ، بالإضافة إلى جرائم تهريب المهاجرين المنصوص في المادة 303 مكرر 30 وتم النص على عقوبات مشددة لمرتكبي هذه الجرائم في الحالات الواردة في المادة 303 مكرر3 ومن ضمن حالات التشديد العقوبة عندما يكون من بين الأشخاص المهربين قاصر.

وبموجب القانون 14-01 المعدل والمتمم لقانون العقوبات استحدث المشرع نص المادة 319 مكرر الذي يعاقب على جريمة بيع وشراء الأطفال وفعل التحريض أو التوسط في عملية بيع الطفل أو محاولة ذلك مع تشديد العقاب إذا ارتكبت الجريمة جماعة إجرامية منظمة.

ونلاحظ أن المشرع استعمل عبارة بيع وشراء الأطفال وليس عبارة المتاجرة ما يفيد أن المشرع يعاقب على الفعل ولو ارتكب مرة واحدة ولا يشترط تكرار هذه العملية لتصبح متاجرة حتى تقع تحت طائلة القانون.

وقد صدر المرسوم الرئاسي رقم 14-251 مؤرخ في 2014/09/08 الذي يتضمن التصديق على الاتفاقية العربية لمكافحة الجريمة المنظمة المحررة بالقاهرة بتاريخ 2010/10/21 وتنص المادة 11 منها في الفقرة 2 على مايلي :"يعتبر استخدام طفل أو نقله أو إيوائه أو استقباله لغرض الاستغلال اتجارا بالأشخاص حتى إذا لم ينطو على استعمال أي من الوسائل المبينة في الفقرة 1 من هذه المادة وفي جميع الأحوال لا يعتد برضائه " (المرسوم الرئاسي رقم 14-251 مؤرخ في 2014/09/08 الذي يتضمن التصديق على الاتفاقية العربية لمكافحة الجريمة المنظمة المحررة بالقاهرة بتاريخ 2010/10/21 الجريدة الرسمية عدد 56 المؤرخة في 2014/10/25).

والوسائل المذكورة في الفقرة 1 من هذه المادة هي كل تهديد بالقوة أو استعمالها أو غير ذلك من أشكال القسر أو الاختطاف أو الاحتيال أو الخداع أو إساءة استعمال السلطة أو استغلال حالة الضعف وذلك من اجل استخدام أو نقل أو إيواء أو استقبال أشخاص لغرض استغلالهم بشكل غير مشروع.

أولا-تعريف الجريمة:

بيع الطفل هو مبادلة الطفل أو أي جزء منه بمال أو منفعة أو بأي شكل من أشكال التعويض، (سلمان، والعيدي، 1013، ص.243) وقد عرفها البروتوكول الاختياري الثاني الملحق باتفاقية حقوق الطفل والخاص ببيع واستغلال الأطفال في البغاء والمواد الإباحية في المادة الثانية منه كما يلي: أي فعل أو تعامل يتم بمقتضاه نقل طفل من جانب أي شخص أو مجموعة إلى شخص أخر لقاء مكافأة أو أي شكل أخر من أشكال العوض.

كما أن هناك غرض أخر لبيع الأطفال والاتجار بهم وهو التبني غير المشروع للأطفال عبر الدول كما يمكن أن يكون بيع الطفل أو شراءه أو عرضه للبيع أو تسليمه وتسلمه أو نقله أو استغلاله اقتصاديا أو جنسيا أو تجاريا أو في التجارب العلمية أو غير ذلك من الأغراض غير مشروعة وقد أصبحت هذه الجريمة تأخذ صورة الجريمة المنظمة العابرة للحدود.

ثانيا: أركان الجريمة: الركن المادي: يشتمل على مجموعة من الأفعال حددتها المادة 319 مكرر وهي:

1.فعل بيع أو شراء الطفل نظير مقابل مالي أو أي منفعة أخرى وبأي شكل من الأشكال ولأي غرض فالمشرع لم يحدد إن كان الغرض من البيع والشراء هو تحقيق الربح والمنفعة المالية أو غير ذلك.

2.التحريض على بيع الطفل أو شرائه والمحرض يعتبر فاعل أصلي.

3.التوسط في عملية بيع الطفل.

4. النشاط ضمن جماعة إجرامية منظمة أو ذات طابع عابر للحدود الوطنية وتكون العقوبة مشددة.

5-الشروع في ارتكاب الفعل المادي المتمثل في بيع الطفل.

الركن المعنوي: هي جريمة مادية تتحقق بمجرد توافر العناصر المكونة لركنها المادي وذلك لكون المشرع لا يعتد بالغرض الذي من اجله قام الفاعل ببيع الطفل ولا بالشكل الذي حدثت تحت غطائه عملية البيع.

صفة المجني عليه: أن يكون طفلا دون الثامنة عشر إذ يختلف الغرض من البيع والشكل الذي يستغل به القاصر حسب عمره.

العقوبة: منصوص عليها في المادتين 319 مكرر و320 مكرر

- يشكل الفعل جنحة معاقب عليها بنص المادة 319 مكرر بالحبس من 5 سنوات إلى 15 سنة وبغرامة من 500.000 دج إلى 1.500.000 دج ويأخذ الوسيط والمحرض في عملية البيع نفس العقوبة.

- ويأخذ الفعل وصف جناية عندما يرتكب من طرف جماعة إجرامية منظمة أو ذات طابع عبر للحدود الوطنية وتكون العقوبة المقررة السجن من 10 سنوات إلى 20سنة وغرامة مالية من 1.000.000 دج إلى 2.000.000 دج.

ويعاقب على الشروع في هذه الجريمة بنفس عقوبة الجريمة التامة: كما تنص المادة 320 مكرر على تطبيق نظام الفترة الأمنية بخصوص الجرائم المنصوص عليها في مجمعة من المواد من ضمنها المادة 319 مكرر.

المطلب الثاني: حماية حق الطفل في صيانة عرضه وأخلاقه

حرصا منه على حماية حق الطفل في صيانة عرضه وأخلاقه جعل المشرع الصغير المجني عليه ظرفا مشددا للعقوبة في بعض جرائم الاعتداء على العرض والأخلاق وركنا جوهريا في جرائم أخرى من نفس الطائفة وقد انطوى قانون14-01 المعدل لقانون العقوبات على حماية أكثر للطفل من خلال تجريمه لأفعال الاستغلال الجنسي للأطفال ونشر الصور الإباحية التي تخص القصر أو المساهمة في انجازها أو ترويجها بأي طريقة كانت بالإضافة إلى تجريمه لفعل التسول بقاصر دون أي إعفاء من العقاب ولو كان المتسول بالقاصر هي أمه.

أن هذه الجرائم تؤثر سلبا على أخلاق القاصر وعرضه إذ تترك أثار نفسية عميقة إلى درجة انه لاستطيع حتى التعبير عما حدث له بسبب الخوف الكبير كما يجد حرجا في الإبلاغ على هذه الجرائم ونظرا لتشعب هذه الأخيرة فضلنا التطرق إلى البعض منها في الفروع الأربعة الآتية: في الفرع الأول ندرس جريمة الفعل المخل بالحياء على قاصر أما في الفرع الثاني: تحريض القصر على الفسق وفساد الأخلاق وفي الفرع الثالث: جريمة اغتصاب قاصر والفرع الرابع: جريمة استغلال القصر في مواد إباحية.

الفرع الأول: جريمة الفعل المخل بالحياء على قاصر: (بوسقيعة، 2010، ص. 114و 115)

ومفهوم الفعل المخل بالحياء المنصوص عليه في المادة 335 من قانون العقوبات، هو كل فعل يمارس على جسم الطفل سواء كان ذكر أو أنثى، ومن شأنه أن يشكل إخلال بالآداب سواء كان ذلك علنا أو في الخفاء، وقد ميز المشرع من حيث الجزاء بين الفعل المخل بالحياء المرتكب بعنف والفعل المرتكب دون عنف

أولا: الفعل المخل بالحياء المرتكب بالعنف: تنص المادة 2/335 من قانون العقوبات على" وإذا وقعت الجريمة على قاصر لم يكمل السادسة عشرة يعاقب الجاني بالسجن المؤقت من عشر سنوات إلى عشرين سنة "

ثانيا: الفعل المخل بالحياء المرتكب بالعنف: يجرم المشرع الجزائري الفعل المخل بالحياء الوقع على القاصر ولو كان بدون عنف ويميز من حيث الجزاء بين حالتين حسب سن المجني عليه:

1. **إذا كان المجني عليه قاصرا بلغ سن التميز (13 سنة) ولم يتجاوز 16 سنة:** يعد هذا الفعل جنحة تعاقب عليها المادة 334 بالحبس من 5 إلى 10 سنوات، وترفع العقوبة إلى السجن المؤقت ن 10الى 20 سنة حال توافر أحد الظروف الآتية:

. إذا كان الجاني من الأصول أو من الفئة التي لها سلطة على الضحية

. إذا استعان الفاعل بشخص أو أكثر (المادة 337).

2. **إذا كان المجني عليه قاصر تجاوز سنه 16 سنة ولم يبلغ سن الرشد وكان الجاني من الأصول:** يعد الفعل جناية تعاقب عليها الفقرة الثانية من المادة 344 بالسجن من 5 إلى 10 سنوات إلى جانب تطبيق الفترة الأمنية والعقوبات التكميلية عليه.

الفرع الثاني: تحريض القصر على الفسق وفساد الأخلاق:

تنص على هذه الجريمة المادة 342 من قانون العقوبات وهي حث أو دفع طفل لم يكمل التاسعة عشر من عمره ذكرا كان أو أنثى على الفسق أو فساد الأخلاق أو القيام بتشجيعهم أو تسهيله لهم، وتأخذ الجريمة وصفين وهما:

. صورة الجريمة العرضية إذا كان الطفل قاصرا لم يكمل 16 سنة.

. صورة الجريمة الاعتيادية إذا كان الطفل قاصرا أكمل 16 سنة ولم يبلغ 18 سنة.

الركن المادي: ويتمثل في حث الطفل على أعمال الفسق وفساد الأخلاق أو تشجيعه أو مساعدته على ذلك، سواء بالقول أو بغيره، بغض النظر عن الوسيلة المستعملة من طرف المحرض ليمهد له طريقا للفسق أو يزين له ذلك بالهدايا.

لم يحدد المشرع الجزائري ما المقصود بفساد الأخلاق، ولا يقتصر مفهومه على الجانب الجنسي بل اعتبر القضاء الجزائري مجالسة الرجال في أماكن شرب الخمر تحريضا على فساد الأخلاق.

الركن المعنوي: القصد العام وهو المستخلص من علم المتهم بأن ما يقوم به من تحريض يؤدي بالطفل إلى الدخول في دائرة الفسق وفساد الأخلاق.

الجزاء: حددت العقوبة من خمسة سنوات إلى عشر سنوات وبغرامة مالية من 20.000 إلى 100.000 دج.

الفرع الثالث: جريمة اغتصاب قاصر

لقد نص المشرع الجزائري على هذه الجريمة في المادة 336 من قانون العقوبات ضمن جرائم انتهاك الآداب، وقد كان يسميها جريمة هتك عرض قاصر وتغيرت التسمية بموجب تعديل 14-01 إلى جريمة اغتصاب والى جانب تخليه على التسمية عدلت المادة فيما يخص سن القاصر الذي تم رفعه إلى 18 سنة بعدما كان 16 سنة كما حذ حذو المشرع الفرنسي في التوسيع من مجال هذه الجريمة ليشمل اغتصاب القاصر سواء كان الضحية ذكرا أم أنثى بنصه في الفقرة الثانية من المادة 336 "إذا وقع اغتصاب على قاصر لم يبلغ 18 سنة ...."

ويعرف الاغتصاب انه كل إيلاج جنسي جرى ارتكابه على شخص الغير ذكرا كان أم أنثى بدون رضاه منها نستنتج أن أركان الجريمة تتمثل في:

الركن المادي: الذي ينقسم إلى عنصرين:

1/الاعتداء الجنسي: ويتحقق بالعملية الجنسية بين المعتدي والقاصر ويتم بالإيلاج الجنسي الطبيعي.

2/ انعدام رضا المجني عليه: ويكون باستعمال العنف أو التهديد أو الإكراه ماديا كان أم معنويا أو قد يكون باستعمال العنف ولكن عندما يتعلق الأمر بالقاصر فإن انعدام الرضا مفترض عند القاصر دون سن التمييز وسن التميز وفق للمادة 42 من القانون المدني هو 13 سنة فلا يكون لرضاه قيمة قانونية لنفي الجريمة.

أما الركن المفترض: فهو صغر الضحية والذي لا يتجاوز 18 سنة سواء كان ذكر أو أنثى.

أما عن العقوبة المقررة: كون الاغتصاب هو ظرف مشددا إذا وقع على قاصر فتكون العقوبة هي السجن المؤقت من 10 إلى 20 سنة عملا بنص المادة 336.

وإذا كان الجاني من الأصول أو من الفئة التي عليها سلطة على الضحية ترفع العقوبة في هذه الحالة إلى السجن المؤبد طبقا للمادة 337 من قانون العقوبات.

بالإضافة إلى العقوبات التكميلية الإلزامية والعقوبات الاختيارية، فعند الحكم بجناية يكون إلزاما الحرمان من ممارسة حق أو أكثر من الحقوق الوطنية والمدنية والعائلية المنصوص عليه في المادة 9 مكرر 1 وذلك أثناء تنفيذ العقوبة الأصلية، كما تنص المادة 341 على تطبيق الفترة الأمنية المنصوص عليها في المادة 60مكرر على المحكوم عليه عند الإدانة بجريمة الاغتصاب المنصوص والمعاقب عليها في المادتين 336 و337 من قانون العقوبات.

الفرع الرابع: جريمة استغلال القصر في مواد إباحية

لقد استحدث المشرع الجزائري هذه الجريمة بموجب تعديل قانون العقوبات بالقانون14-01 في المادة 333 مكرر 1 وذلك تماشيا مع البرتوكول الاختياري لاتفاقية حقوق الطفل بشأن بيع واستغلال الأطفال في البغاء والأعمال الإباحية وتنص المادة " يعاقب بالحبس من خمس (5) سنوات إلى عشر (10) سنوات وبغرامة من 500.000 دج إلى 1.000.000 دج، كل من صور قاصرا لم يكمل 18 سنة بأي وسيلة كانت وهو يمارس أنشطة جنسية بصفة مبينة، حقيقية أو غير حقيقية، أو صور الأعضاء الجنسية للقاصر لأغراض جنسية أساسا، أو قام بإنتاج أو توزيع أو نشر أو ترويج أو استيراد أو تصدير أو عرض أو بيع أو حيازة مواد إباحية متعلقة بالقصر " .

بالرجوع إلى نص المادة نستنتج ما يلي:

أولا: يقصد باستغلال الأطفال في مواد إباحية هو تصوير أي طفل بأي وسيلة كان يمارس ممارسة حقيقية أو بالمحاكاة أنشطة جنسية صريحة أو أي تصوير للأعضاء الجنسية للطفل لإشباع الرغبة الجنسية أساسا وهي ظاهرة جد خطيرة انتشرت في السنوات الأخيرة بين الأشخاص اللذين يعانون انحراف في التفضيل الجنسي للأطفال لممارسة الجنس معهم أو مشاهدة صور خليعة أو أفلام إباحية.

ـ كما يتم استخدام الطفل لإنتاج أعمال أو أداء عروض إباحية لجني الأموال من وراء ذلك وقد يكون استغلال الطفل من طرف الغير أو حتى من طرف ذويه فالأسرة ليست دائما المقر الأمن لحماية الطفل فالآباء قد لا يمتنعون فقط عن الاعتداء بالأبناء بل قد يعرضونهم إلى الخطر كما يؤدي فقدان أحد الوالدين أو انفصالهما إلى عواقب وخيمة يكون ضحيتها الطفل القاصر تستدعي إسقاط الولاية الأبوية لمدة قد تطول أو تقصر.

ثانيا: بالرجوع إلى نص المادة نجد أن الركن المادي للجريمة يتمثل في:

1) التصوير: ويشتمل على

- ✓ تصوير قاصر بأي وسيلة كانت وهو بصدد ممارسة أنشطة جنسية سواء كان ذلك حقيقة أو عن طريق الخدع التصويرية.
- ✓ تصوير الأعضاء الجنسية للقصر لأغراض جنسية فإذا كان التصوير لأغراض عملية أو طبية لا يندرج ضمن هذه الجريمة

2) **الإنتاج والتوزيع والنشر والترويج:** وذلك مهما كانت الوسيلة المستعملة سواء السمعية، البصرية، الانترنيت والأنظمة المعلوماتية، فكل من أنتج أو أرسل أو نشر عن طريق نظام معلومات أو الشبكة المعلوماتية أو كل ما هو مسموع أو مقروء أو مرئي يتضمن أعمالا إباحية وجنسية يشارك فيها القصر وتتعلق بالاستغلال الجنسي لهؤلاء الذين لم يتجاوز سنهم 18 سنة.

3) الاستيراد والتصدير أو البيع والحيازة: كل هذه الأفعال تفيد تداول هذه المنتوجات التي موضوعها أعمال إباحية وجنسية تتعلق بالقصر سواء بالاستيراد أو التصدير أو البيع أو حتى الحيازة، وهنا نلاحظ أن المشرع ذهب في المادة 333 مكرر1 إلى ابعد مما جاء في البروتوكول الاختياري بتجريمه لفعل حيازة هذه المواد.

ثالثا: ما الركن المعنوي فيتمثل في علم الجاني بان ما ينتجه أو ما يتداوله ويروجه أو ينشره أو ما يحوزه يتعلق بمواد إباحية موضوعها قصر لم يبلغوا 18 سنة من العمر.

رابعا: العقوبة: تعاقب المادة 333 مكرر 1 الفاعل بالحبس من 5 سنوات إلى 10سنوات وغرامة مالية من 500.000دج إلى 1.000.000 دج، مع مصادرة الوسائل المستعملة لارتكاب الجريمة والأموال المتحصل عليها بصفة غير مشروعة مع مراعاة حقوق الغير حسن النية.

ملاحظة: تنص المادة 10 من قانون حماية الطفل أنه "يمنع، تحت طائلة المتابعات الجزائية، استعمال الطفل في ومضات إشهارية أو الأفلام أو صور أو تسجيلات مهما كان شكلها إلا بترخيص من ممثله الشرعي خارج فترات التمدرس وذلك طبقا للتشريع والتنظيم المعمول بهما "وهو ما يشكل وجه أخر للحماية للطفل.

المطلب الثالث: حماية الطفل من جرائم المتعلقة بالوضعية الاجتماعية والعائلية:

تعد الأسرة الجو الملائم للطفل الذي يجد فيه توازنه الفكري والجسدي ويعد المجتمع المكان الذي يطور فيه الطفل ملاكاته باحتكاكه بالغير وتفتحه على الوسط الذي يعيش فيه فيغدوا إنسانا كاملا وصالحا، إلا أن الواقع عكس ذلك لأن الأماكن التي كانت من المفروض أن تكون مصدر للدفء والأمان للطفل أصبحت كالثعبان تلسعه كلما اقترب منها فالعائلة اليوم أصبحت المنتهكة الأولى لحقوق هذا العبد الضعيف، فيضطر للخروج منها ليقع في مخالب المجتمع الذي يجرده مما بقي له منها فلهذه الأسباب جرم المشرع الكثير من الأفعال حماية منه للقاصر سواء على مستوى عائلته أو المجتمع ككل، وهو ما سنفصله في الفرعين الآتيين:

الفرع الأول: الجرائم المؤثرة على الوضعية العائلية للطفل:

تستند رعاية الطفل في شكلها الطبيعي على رعايته في أحضان أبويه اللذين يرتبط بهما طبيعيا، عاطفيا واجتماعيا ويعتمد عليهما بشكل تلقائي في إشباع حاجياته، فهو وديعة على عاتقهما يقع عليهما التزم قانوني برعيته والاعتناء به وعدم إهماله، ولكن بتصفح قانون العقوبات نجده يعج بالجرام التي يتعرض لها الطفل التي يرتكبها الآباء ونظر لكثرتها حاولنا التطرق إلى الأخطر منها في نظرنا وهي كالاتي بيانها:

أولا: جريمة عدم الإبلاغ عن ميلاد الطفل:

تنص المادة 07 من اتفاقية حقوق الطفل لسنة 1989 " يسجل الطفل بعد ولادته فورا ويكون له الحق في اكتساب جنسية وفي معرفة والديه وتلقي رعايتهما "(اتفاقية حقوق الطفل، صادقت عليها الجمعية العامة للأمم المتحدة بتاريخ 20 نوفمبر 1989 والتي دخلت حيز التنفيذ في 02 /1990/09 والمصادق عليها مع تصريحات التفسيرية بموجب المرسوم الرئاسي رقم 92-461 المؤرخ في 13-12-1992 الجريدة الرسمية عدد91 المؤرخة في 23 ديسمبر 1992.)

لقد كان المشرع الجزائري السباق إلى إقرار هذا الحق في الحالة المدنية منذ صدور الأمر المتعلق بها سنة 1970 والذي لم يعدل إلا مؤخرا بموجب القانون 14-08 المؤرخ في 2014/08/09 والذي رسم قواعد إلزام المواطنين باحترامها وإلا تعرضوا إلى عقوبات مخالفتها خاصة تلك المتعلقة بالطفل وتأخذ هذه الجريمة صورتين هما

1) **صورة عدم التصريح بالميلاد:** تنص المادة 61 من أمر 20/70 المعدل بقانون 14-08 بمايلي " يصرح بالمواليد خلال 5 أيام من الولادة إلى ضابط الحالة المدنية للمكان وإلا فرضت العقوبات المنصوص عليها في المادة 442ف 3 من قانون العقوبات وتحدد المدة المذكورة في الفقرة الأولى أعلاه بعشرين يوم لولايات الجنوب .... ولا يحسب يوم الولادة في الأجل المحدد في الفقرة السابقة عندما يصادف أخر يوم من هذه الآجال يوم عطلة، ويحدد هذا الأجل إلى أول يوم عمل يلي يوم العطلة " وتنص المادة 62 من نفس الأمر "يصرح بولادة الطفل الأب أو الأم وإلا الأطباء والقابلات أو أي شخص أخر حضر الولادة وعندما تكون الأم ولدت خارج مسكنها فالشخص الذي ولدت عنده الأم، تحرر شهادة الميلاد فورا "

وبالرجوع إلى قانون العقوبات نجده في المادة 442 ف 3 منه يعاقب كل من حضر ولادة طفل ولم يقدم الإقرار المنصوص عليه قانونا في المواعيد المحددة بالحبس من 10 أيام إلى شهرين وبغرامة من 8000الى 16000دج أو إحدى هاتين العقوبتين.

إذن نستنتج من نص المادة 62 لكي يلزم الشخص بالتصريح بولادة طفل إلى ضابط الحالة المدنية يجب أن يكون الأب أو الأم أو الطبيب أو القابلة أو أي شخص كان قد حضر فعلا الوضع وان يكون التصريح في المدة المحددة في المادة 61 وإذا امتنعوا عن ذلك يكون قد ارتكبوا جريمة ويتعرضون للعقاب المنصوص عليه في المادة 442ف 3 من قانون العقوبات.

1) صورة عدم تسليم طفل حديث العهد بالولادة : تنص المادة 67فقرة 1 من الأمر 20/70المعدل بالقانون رقم 14-08 على انه "يتعين على كل شخص وجد مولود حديثا أن يصرح به إلى ضابط الحالة المدنية التابع لمكان العثور عليه إذا لم تكن له رغبة في التكفل بالطفل يجب عليه تسليمه إلى ضابط الحالة المدنية مع الألبسة والأمتعة الأخرى الموجودة معه "أما المادة 442 فقرة 3 تنص" يعاقب بالحبس من 10 أيام على الأقل إلى شهرين على الأكثر و بغرامة من 8000الى 16000 دج أو بإحدى هاتين العقوبتين فقط ،كل من حضر ولادة طفل ولم يقدم عنه الإقرار المنصوص عليه في القانون في المواعيد المحددة وكل من وجد طفلا حديث العهد بالولادة ولم يسلمه إلى ضابط الحالة المدنية كما يوجب ذلك القانون ما لم يوافق على أن يتكفل به و يقر بذلك أمام جهة البلدية التي عثر على الطفل في دائرتها .

ثانيا: جريمة الإهمال المعنوي للأولاد

لقد نص المشرع على هذه الجريمة في القسم الخامس المعنون ترك الأسرة في المادة 330 فقرة 3 إلى جانب كل من جريمة ترك الأسرة والتخلي عن الزوجة الحامل وقد فضل التفصيل في هذه الجريمة نظرا لما لها من أثار سلبية على الطفل

إذ تنص المادة 330ف 3 " أحد الوالدين الذي يعرض صحة أولاده أو أحد أو أكثر منهم أو يعرض أمنهم أو خلقهم لخطر جسيم بان يسيء معاملتهم أو يكون مثلا سيئا لهم للاعتياد على السكر أو سوء السلوك أو يمهل رعايتهم أو لا يقوم بالإشراف الضروري عليهم، وذلك سواء كان قد قضى بإسقاط سلطته الأبوية عليهم أو لم يقض بإسقاطها "

يتشكل الركن المادي لهذه الجريمة من ثلاثة عناصر وهي:

1- **صفة الأب أو الأم**: يقصد بهما الأبوين الشرعيين.

2 -**الأعمال المبينة في المادة 3/330:** ويمكن تقسيمها إلى نوعين:

. أعمال ذات طابع مادي: سوء المعاملة وانعدام الرعاية الصحية مثل ضرب الطفل، الذهاب إلى العمل وترك الطفل بمفرده في البيت أو الشارع، عدم عرض الطفل على الطبيب في حالة مرضه.

. أعمال ذات طابع أدبي: المثل الشيء مثل تعاطي المخدرات والإدمان على السكر، القيام بالأعمال المنافية للأخلاق وعدم رعاية الأطفال.

3 . **النتيجة المترتبة عن الإهمال**: يجب أن تعرض سلوكات الأب والأم صحة الأولاد وأمنهم لخطر جسيم وتقدير مدى جسامة الخطر تخضع للسلطة التقديرية للقاضي.

العقوبة: الحبس من شهرين إلى سنة وبغرامة من 25.000دج إلى 100.000 دج

ملاحظة : فيما يخص إجراءات المتابعة فعلى غرار جريمة ترك الأسرة التي علق المشرع فيها المتابعة على شكوى المضرور فان هذا الإجراء غير واردة في جريمة الإهمال المعنوي لسبب واحد لكون المضرور هنا طفل أو أولاد لم يكتمل بعد نضجهم الجسمي والعقلي ويتعذر عليهم تقديم شكوى فلم يخض إجراءات المتابعة لأي قيد وبالتالي يمكن للنيابة العامة تحريك الدعوى العمومية دو انتظار الشكوى، كما لم يجعل الصفح سببا لوضع حد للمتابعة الجزائية مثلما فعل في جريمة ترك الأسرة و الامتناع عن دفع النفقة (خرباش، 2009، ص. 79) ولكن رغم مراعاة المشرع للطرف المضرور إلا أن هذه الجرائم كثرا ما ترتكب ويفلت الوالدين من العقاب لكونها تتم داخل الأسرة ويتعذر وصولها لعلم النيابة إلا إذا تقدم القاصر بشكوى أو قدم أحد الجيران بلاغ .

الفرع الثاني: الجرائم المؤثرة على الوضعية الاجتماعية

سنتناول في هذا الفرع جريمتين أساسيتين وهما جريمة تقديم طفل إلى ملجأ أو مؤسسة خيرية وجريمة عدم تسليم طفل تحت رعاية الغير.

أولا: جريمة تقديم طفل إلى ملجأ أو مؤسسة خيرية:

تنص المادة 3/442 من قانون العقوبات "يعاقب بالحبس من عشرة أيام على الأقل إلى شهرين على الأكثروبغرامة من 8.000 دج إلى 16.000 دج كل من قدم طفلا تقل سنه عن سبع سنوات كاملة إلى ملجأ أو إلى مؤسسة خيرية متى كان قد سلم إليه لرعاية أو لأي سبب أخر ما لم يكن غير مكلف أو غير ملزم بتوفير الطعام له مجانا وبرعايته ولم يوفر له أحد ذلك "

إذن: من خلال النص نستنتج أن الأمر يتعلق بطفل لم يتجاوز السابعة وقصر الضحية هو ركن في هده الجريمة أما الشرط الثاني يجب أن يكون الجاني شخصا مكلفا أو ملزما بتوفير الطعام للطفل مجانا وبرعايته وقد يجد هذا الإلزام مصدره في علاقة الرحم كالجد والجدة والأخ والأخت والعم والعمة والخال والخالة او في عقد شرعي كما في الكفالة طبقا للمادة 116 من قانون الأسرة أما الآباء و الأمهات فلا تقوم الجريمة في حقهم إذ لا يمكن الحديث بشأنهم عن استلام طفل لرعايته، كما لا تقوم في حق من هو مكلف أو غير ملزم برعاية الطفل ومن ثم لا يمكن مساءلة من وجد طفلا فقدمه إلى ملجأ أو مؤسسة خيرية (بوسقيعة، 2013، ص. 182)

ثانيا: جريمة عدم تسليم طفل موضوع تحت رعاية الغير:

تنص عليها المادة 327 من قانون العقوبات التي جاء نصها كالاتي: "كل من لم يسلم طفلا موضوعا تحت رعايته إلى الأشخاص الذين لهم الحق في المطالبة به يعاقب بالحبس من سنتين إلى خمس سنوات "

من خلال النص نستنتج ما يلي:

الركن المادي: يتطلب لقيام الجريمة توفر شرطين هما:

- ✓ أن يكون الطفل قد وكل إلى الغير كان يوكل إلى مربية أو مرضعة والى مدرسة داخلية أو حضانة أو روضة أطفال ومن ثمة لا تقوم الجريمة في حق الوالدين حتى وان كانت الرابطة الزوجية منحلة والأصل هوان لا يتجاوز الطفل 7 سنوات قياسا على نص المادة 3/442.
- ✓ أن يطالب به من له الحق في ذلك أي الشخص الذي يتمتع بالحضانة (الأب، الأم أو الوصي) بغض النظرعما إذا كان الطفل قد وكل إلى المتهم بطريقة غير مباشرة
- ✓ يجب قيام عدم تسليم سواء امتنع من أوكل له عن رده أو امتنع عن تعيين مكان تواجده.

الركن المعنوي: تقتضي هذه الجريمة توفر نية إجرامية لدى المجني ولا تقوم الجريمة إلا إذا تعمد من كان الطفل تحت رعايته رفض تسليمه إلى من له الحق في المطالبة به أو امتنع عن الإفصاح عن مكان الذي يوجد فيه الطفل

أما عن العقوبة: فقد صنفها المشرع جنحة وذلك من خلال العقوبة المقررة لمرتكبيها والتي هي الحبس من سنتين إلى خمس سنوات إضافة إلى إمكانية الحكم بالعقوبات التكميلية المقررة في الجنح كل ذلك ما هو إلا تكريسا للحماية التي قررها المشرع للطفل وحمل كل من تولى رعايته مسؤولية الحفاظ عليه ورده إلى أهله متى طلب منه ذلك.

ثالثا: جريمة استغلال القصر في التسول:

هي جريمة تم استحداثها بموجب تعديل قانون العقوبات بموجب القانون رقم 01/14 وذلك بإضافة نص المادة 195 مكرر والتي تنص على أنه يعاقب بالحبس من 06 أشهر إلى سنتين كل من يتسول بقاصر لم يكمل 18 سنة أو يعرضه للتسول وتضاعف العقوبة عندما يكون الفاعل أحد أصول القاصر أو أي شخص له سلطة عليه.

وقد أحسن المشرع في إدراج هذه المادة لان ظاهرة التسول بالأطفال انتشرت بالكثرة وهو ما يشكل خطر عليهم.

المبحث الثاني: الحماية القانونية للطفل المعرض لخطر:

سعيا من المشرع لتكريس مبدأ المصلحة الفضلى للطفل جاء قانون 15-12 المؤرخ في 15 جويلية 2015 المتعلق بحماية الطفل ليكرس وجه أخر للحماية وهي حماية الطفل في خطر، (قانون 15-12 المتعلق بحماية الطفل المؤرخ في 15-07-2015 جريدة رسمية عدد 39 المؤرخة في 19 جويلة 2015) رغم أن الأمر 72-3 المؤرخ في 10 فبراير 1972 المتعلق بحماية الطفولة والمراهقة الملغى أشار إلى هذا النوع من الحماية إلا أن هذا القانون وسع في مفهوم وحالات الخطر كما حدد وسائل الحماية وقسمها إلى حماية اجتماعية وقضائية ولإبراز هذه الحماية قسمنا المبحث إلى المطالب الثلاثة الآتية: في المطلب الأول نتناول مفهوم وحالات تعرض الطفل للخطر أما في المطلب الثاني نتطرق الحماية الاجتماعية للطفل والمطلب الثالث خصصناه للحماية القضائية للطفل .

المطلب الأول: مفهوم وحالات تعرض الطفل للخطر

يشكل وجود الطفل في خطر أحد المخاطر التي تهدد وجوده وكيانه وقد حرص المشرع إلى إدراج هذه الوضعية في التشريع واعتبرها من بين الحالات التي يكون فيها الطفل في مركز الضحية وبصدور قانون حماية الطفل نلاحظ أنه وسع من مفهوم وحيزها وهو ما سنبينه أدناه في الفرعين الآتيين:

الفرع الأول: تعريف الطفل في خطر:

تعرف المادة 02 من قانون 15-12 المتعلق بحماية الطفل أن الطفل المعرض للخطر هو ذلك "الطفل الذي تكون صحته آو أخلاقة أو تربيته أو أمنه في خطر أو عرضة له أو تكون ظروفه المعيشية آو سلوكه من شأنهما أن يعرضاه للخطر المحتمل أو المضر بمستقبله أو يكون في بيئة تعرض سلامته البدنية أو النفسية أو التربوية للخطر"، من خلال التعريف نلاحظ أن المشرع يحمي الطفل حتى من الخطر المحتمل الشيء الذي لم تنص عليه المادة 01 من الأمر 72-03 المتعلق بحماية الطفولة والمراهقة وهو دليل على حرصه الشديد على حماية الطفل هو ما جسده في تحديده لحالات تعرضه للخطر.

الفرع الثاني: حالات تعرض الطفل لخطر:

لقد حدد المشرع الحالات التي يعد فيها الطفل في خطر في المادة 02 والتي جاءت على النحو التالي:

" تعتبر من بين الحالات التي تعرض الطفل للخطر: فقدان الطفل لوالديه وبقائه دون سند عائلي، تعرض الطفل للإهمال أو التشرد، المساس بحقه في التعليم، التسول بالطفل أو تعريضه للتسول، عجز الأبوين أو من يقوم برعاية الطفل عن التحكم في تصروفاته التي من شانها أن تؤثر على سلامته البدنية أو النفسية أو التربوية.

التقصير البين والمتواصل في التربية والرعاية، سوء معاملة الطفل لاسيما بتعريضه للتعذيب ولاعتداء على سلامته البدنية أو احتجازه أو منع الطعام عنه أو إتيان أي عمل ينطوي على القساوة من شانه التأثير على توازن الطفل العاطفي آو النفسي، إذا كان الطفل ضحية جريمة من ممثله الشرعي، إذا كان الطفل ضحية جريمة من أي شخص أخر إذا اقتضت مصلحة الطفل حمايته ، الاستغلال الجنسي للطفل بمختلف أشكاله، من خلال استغلاله لاسيما في المواد الإباحية وفي البغاء وإشراكه في عروض جنسية، الاستغلال الاقتصادي للطفل لا سيما بتشغيله أو تكليفه بعمل يحرمه من متابعة دراسته أو يكون ضارا بصحته آو بسلامته البدنية أو المعنوية،
وقوع الطفل ضحية نزاعات مسلحة وغيرها من حالات الاضطراب وعدم الاستقرار، الطفل اللاجئ.

إن المشرع عند تعداده لحالات تعرض الطفل للخطر نجده قد شمل كافة الميادين التي لها علاقة بالطفل وأكثر من ذلك حمى الطفل للاجئ الذي يجتاز الحدود طالبا الحماية ومن اجل تحقيق هذه الحماية جند وسائل الاجتماعية والقضائية الآتية:

المطلب الثاني: الحماية الاجتماعية للطفل

قبل صدور قانون الطفل 15-12 كانت مهمة تأمين حماية الطفولة والمراهقة موكلة إلى كل من المؤسسات والمصالح التالية: المركز المتخصصة لإعادة التربية، المراكز التخصصية للحماية، مصالح الملاحظة والتربية في الوسط المفتوح، والمراكز المتعددة الخدمات لوقاية الشبيبة وذلك بموجب الأمر 75-64 المؤرخ في 26 سبتمبر سنة 1975 الذي يتضمن إحداث المؤسسات والمصالح المكلفة بحماية الطفولة والمراهقة ولكن بموجب 149 تم إلغاء هذا الأمر وعهدت هذه الحماية إلى مؤسسات أخرى ستنشأ على المستويين الوطني والمحلي ففيما تتمثل هذه الأخير وما هو مصير المصالح التي حملها هذا الأمر بعد إلغاءه؟.

الفرع الأول: الحماية على المستوى الوطني:

لقد تناولت المواد من 11 إلى 20 من قانون 15-12 الحماية الاجتماعية للطفل على المستوى الوطني والتي أوكلت فيها المهمة إلى الهيئة الوطنية لحماية وترقية الطفولة والى المفوض الوطني.

أولا: الهيئة الوطنية لحماية وترقية الطفولة:

تنص المادة 11 على انه" تحدث لدى الوزير الأول هيئة وطنية لحماية وترقية الطفولة يرأسها المفوض الوطني لحماية الطفولة، تكلف بالسهر على حماية وترقية حقوق الطفل، تتمتع بالشخصية المعنوية والاستقلال المالي، تضع الدولة تحت تصرف الهيئة الوطنية لحماية وترقية الطفولة، كل الوسائل البشرية والمادية اللازمة للقيام بمهامها "

إنه بالرجوع إلى الأمر رقم 75-64 المؤرخ في 26ستمبر 1975 الذي يتضمن إحداث المؤسسات والمصالح المكلفة بحماية الطفولة والمراهقة نجد أن المهمة كانت موكلة إلى وزير الشبيبة والرياضة في حين أن القانون الجديد أوكل المهمة إلى الوزير الأول وهو ما يعد أحد أوجه تكريس مبدأ المصلحة الفضلى للطفل.

أما فيما يخص شروط وكيفيات تنظيم الهيئة الوطنية وسيرها فقد أرجعها المشرع صدور تنظيم والذي لم يصدر بعد.

ثانيا: المفوض الوطني لحماية الطفولة:

من هو: تنص المادة 12 على أنه يعين المفوض بموجب مرسوم رئاسي من بين الشخصيات الوطنية ذات الخبرة والمعروفة بالاهتمام بالطفولة.

مهامه: لقد حددت المواد 13،14، 19 و 20 المهام المسندة للمفوض الوطني نذكر منها:

1. وضع برامج وطنية ومحلية لحماية وترقية حقوق الطفل بالتنسيق مع مختلف الإدارات والمؤسسات والهيئات العمومية والأشخاص المكلفين برعاية الطفولة وتقيمها الدوري.
2. متابعة الأعمال المباشرة ميدانيا في مجال حماية الطفل والتنسيق بين مختلف المتدخلين
3. أبداء الرأي في التشريع الوطني الساري المفعول المتعلق بحقوق الطفل.
4. زيارة المصالح المكلفة بحماية الطفولة وتقديم أي اقتراح كفيل بتحسين سيرها وتنظيمها.
5. المساهمة في إعداد التقارير المتعلقة بحقوق الطفل التي تقدمها الدولة إلى الهيئات الدولية والجهوية المختصة.
6. إعداد تقرير سنوي عن حالة حقوق الطفل ومدى تنفيذ اتفاقية حقوق الطفل، ويرفعه إلى رئيس الجمهورية ويتم نشره وتعميمه خلال الثلاثة أشهر الموالية لهذا التبليغ.

.كيفية إخطاره والإجراءات التي يتخذها: تنص المواد 15، 16،17 و18 من القانون 15-12 على ذلك، إذ يتم إخطار المفوض الوطني بوجود مساس بحقوق الطفل سواء من الطفل ذاته أو ممثله الشرعي أو من كل شخص طبيعي أو معنوي ثم يقوم هو باتخاذ الإجراءات الآتية:

- ✓ يقوم بتحويل الإخطارات إلى مصلحة الوسط المفتوح المختصة إقليميا للتحقيق فيها واتخاذ الإجراءات المناسبة.
- ✓ . يقوم بتحويل الإخطارات التي يحتمل أن تتضمن وصفا جزائيا إلى وزير العدل الذي يخطر النائب العام المختص قصد تحريك الدعوى العمومية.

ملاحظة: أنه من خلال استقراء المواد المنظمة لدور ومهام المفوض الوطني نستنتج أنه يشكل أحد العناصر الهامة والفعالة في تجسيد وحماية حقوق الطفولة خاصة وأنه وضعت تحت تصرفه كل الوسائل ولا يمكن الاعتداد في مواجهته بالسر المهني فهو همزة وصل بين الهيئات المركزية والمحلية.

الفرع الثاني: الحماية الاجتماعية على المستوى المحلي:

لقد تطرقت المواد من 21 إلى 31 إلى الحماية الاجتماعية على المستوى المحلي أين أسندت المهمة إلى الوسط المفتوح بالتنسيق مع مختلف الهيئات والمؤسسات العمومية والأشخاص المكلفين برعاية الطفولة.

. **ما هو الوسط المفتوح**؟ تنص المادة 21 على انه تنشأ مصالح الوسط المفتوح بواقع مصلحة واحدة بكل ولاية مع إمكانية إنشاء أكثر من مصلحة في الولايات ذات الكثافة السكانية يتشكل من موظفين مختصين لاسيما: مربين ومساعدين اجتماعين وأخصائيين نفسانيين وأخصائيين اجتماعيين وحقوقيين وضعت الدولة تحت تصرفه كل الوسائل المادية والبشرية اللازمة للقيام بمهامه. وسيحدد التنظيم شروط تطبيق هذه المادة لاحقا.

مهامه: أسندت للوسط المفتوح المهام الآتية:

- ✓ متابعة وضعية الأطفال في خطر ومساعدة أسرهم.
- ✓ إعلام قاضي الأحداث دوريا بالأطفال المتكفل بهم وبالتدابير المتخذة بشأنهم.
- ✓ إعلام المفوض الوطني بمآل الإخطارات التي وجهها إليه مع موافاته بتقرير مفصل كل ثلاثة أشهر.

. **كيفية إخطار الوسط المفتوح والإجراءات المتخذة:**

كيفية الإخطار:

تنص المادة 22 على انه يتم إخطار مصالح الوسط المفتوح إما من قبل الطفل أو ممثله الشرعي أو الشرطة القضائية أو الوالي أو رئيس المجلس الشعبي البلدي أو كل جمعية أو هيئة عموميه أو خاصة تنشط في مجال حماية الطفل أو المساعدين الاجتماعيين أو المربين أو المعلمين أو الأطباء أو كل شخص طبيعي أو معنوي أخر

بكل ما من شأنه أن يشكل خطر على الطفل أو على صحته أو سلامته البدنية أو المعنوية كما يمكنه التدخل تلقائيا لا يمكن للوسط المفتوح رفض التكفل بطفل يقيم خارج اختصاصه الإقليمي ولكن يمكنه في هذه الحالة أن يطلب المساعدة من مصلحة مكان إقامة أو سكنه أو تحويله إليه.

الإجراءات المتخذة:

تنص المادة 23 على انه بعد تأكد الوسط المفتوح من الوجود الفعلي لحالة الخطر من خلال القيام بالأبحاث الاجتماعية والانتقال إلى مكان تواجد الطفل والاستماع إليه والى ممثله الشرعي من اجل اتخاذ التدابير المناسبة له أو طلب تدخل النيابة أو قاضي الأحداث إذا تطلب الأمر ذلك أحد الإجراءات الآتية:

الإجراء الأول: إذا تأكد الوسط من عدم وجود خطر يقوم بإعلام الطفل وممثله الشرعي بذلك.

الإجراء الثاني: إذا تأكد من وجود الخطر يقوم الوسط المفتوح بما يلي:

- ✓ الاتصال بالممثل الشرعي للطفل من اجل الوصول إلى الاتفاق بخصوص التدبير الأكثر ملائمة لاحتياجات الطفل ووضعيته.
- ✓ إذا كان الطفل يبلغ من العمر ثلاثة عشر سنة على الأقل يقوم بإشراكه في التدبير الذي سيتخذ بشأنه

- ✓ يحرر الاتفاق في محضر يوقع عليه جميع الأطراف بعد تلاوته عليهم مع إعلام الطفل وممثله الشرعي بحقهما في رفض الاتفاق.
- ✓ يقوم الوسط المفتوح بإبقاء الطفل في أسرته مع اقتراح أحد التدابير الاتفاقية الآتية:

1. إلزام الأسرة باتخاذ التدابير الضرورية المتفق عليها لإبعاد الخطر على الطفل في الآجال التي تحددها مصالح الوسط المفتوح لحماية الاجتماعية
2. تقديم المساعدة الضرورية للأسرة وذلك بالتنسيق مع الهيئات المكلفة بالحماية الاجتماعية.
3. إخطار الوالي أو رئيس المجلس الشعبي البلدي المختص أو أية هيئة اجتماعية من اجل التكفل الاجتماعي بالطفل.
4. اتخاذ الاحتياطات الضرورية لمنع اتصال الطفل مع أي شخص يمكن أن يهدد صحته أو سلامته البدنية أو المعنوية.

1. يمكن لمصالح الوسط المفتوح تلقائيا أو بناء على طلب الطفل أو ممثله الشرعي، مراجعة التدبير المتفق عليه كليا أو جزئيا.

الإجراء الثالث: رفع الأمر إلى قاضي الأحداث المختص تنص على هذا الإجراء المادة 28 التي تنص "يجب أن ترفع مصالح الوسط المفتوح الأمر فورا إلى قاضي الأحداث المختص في حالات الخطر الحال أو في الحالات التي يستحيل معها إبقاء الطفل في أسرته لاسيما إذا كان صحية جريمة ارتكبها ممثله الشرعي وهنا يتم الانتقال إلى الحماية القضائية للطفل.

ملاحظة: من خلال تدريبنا الميداني في كل من ولاية ورقلة ، مسيلة والقالة لحظنا أن قضاة الأحداث يستنجدون بمراكز ومصالح موجودة خارج اختصاصهم لوضع الطفل الموجود في خطر فيها فمثلا ولاية المسيلة يستعينون بالمراكز الموجودة على مستوى ولاية سطيف في حين نجد قاضي الأحداث بمحكمة القالة يستعين بمركز إعادة التربية للإناث بقسنطينة وان نص المشرع على إنشاء مصلحة في كل ولاية يخدم الطفل في الدرجة الأولى لأنه سيبقى في محيطه كما يخدم قاضي الأحداث في الدرجة الثانية لان الطفل يكون تحت مراقبته المستمرة وتسهل عليه الإجراءات

المطلب الثالث: الحماية القضائية للطفل: إلى جانب الحماية الاجتماعية المقررة للطفل على المستويين الوطني والمحلي قرر المشرع حماية قضائية والتي خص بها قاضي الأحداث على مستوى المحكمة فقد حدد القانون 15-12 المتعلق بحقوق الطفل اختصاصه وكيفية إخطاره كما رسم له التدابير الواجب اتخاذها لمساعدة الطفل في خطر وهو ما سنبينه في الفرعين الآتيين:

الفرع الأول: كيفية إخطار قاض الأحداث:

تنص المادة 32 على ما يلي "يختص قاضي الأحداث لمحل إقامة الطفل المعرض للخطر أو مسكنه أو محل إقامة أو مسكن ممثله، وكذلك قاضي الأحداث للمكان الذي وجد به الطفل في حالة عدم وجود هؤلاء بالنظر في العريضة التي ترفع إليه من الطفل أو ممثله الشرعي أو وكيل الجمهورية أو الوالي أو رئيس المجلس الشعبي البلدي لمكان إقامة الطفل أو مصالح الوسط المفتوح أو الجمعيات الهيئات العمومية المهتمة بشؤون الطفولة.

كما يجوز لقاضي الأحداث أن يتدخل تلقائيا ويمكن تلقي الإخطار المقدم من الطفل شفاهه "

إنه باستقراء نص المادة الحالية ومقارنتها بنص المادة 2 من الأمر 72 -03 المتعلق بحماية الطفولة والمراهقة الملغى والتي تنص "يختص قاضي الأحداث لمحل إقامة القاصر أو مسكنه أو محل إقامة أو مسكن والدية أو الولي عليه وكذلك قاضي الأحداث للمكان الذي وجد فيه القاصر في حالة عدم وجود هؤلاء بالنظر في العريضة التي ترفع إليه من والد القاصر أو والدته أو الشخص الذي يسند إليه حق الحضانة على القاصر نفسه، وكذلك العريضة التي ترفع إليه من الولي أو وكيل الدولة او رئيس المجلس الشعبي البلدي لمكان إقامة القاصر أو المندوبين المختصين بالإفراج المراقب، كما يجوز لقاضي الأحداث كذلك، أن ينظر في القضايا المتعلقة بالإحداث بصفة تلقائية "

نستنتج ما يلي:

أولا: نلاحظ أن المشرع احتفظ بالجهات التي يجوز لها إخطار قاضي الأحداث بوجد الطفل في خطر مع تعديل في مصطلحات التي جاء شاملة كما خول حق الإخطار لأشخاص آخرين لم يتم إدراجهم من قبل وقد حددت كالتالي:

1. **الطفل**: نلاحظ أن المشرع قد تدارك السهو الذي وقع فيه وذلك بتكريسه لحق الطفل الموجود في خطر برفع عريضة إلى قاضي الأحداث وقد ذهب إلى أكثر من ذلك فقد اعتبر الإخطار الشفهي المقدم من الطفل أحد وسائل تدخله وذلك ترسيخا منه لمبدأ المصلحة الفضلى للطفل.

ممثله الشرعي: وهو مصطلح واسع بالمقارنة عما كان عليه في المادة 2 الملغاة التي حصرته والد القاصر، والدته والشخص الذي يسند إليه حق الحضانة، إذ يمكن إدراج تحت مصطلح الممثل الشرعي كل من الوالي، والوصي والمقدم والكفيل.

وكيل الجمهوري: والذي كان يسمى في ضل المادة 02 بوكيل الدولة.

الوالي؛ رئيس المجلس الشعبي البلدي لمكان إقامة الطفل؛ مصالح الوسط المفتوح الهيئات العمومية المهتمة بشؤون الطفل

ثانيا: نلاحظ أن المشرع احتفظ بإجراء الإخطار الذي يكون بتقديم عريضة مكتوبة من قبل الجهات المخول لها الحق في ذلك كما اعتبر التصريح الشفوي المقدم من الطفل وسيلة إخطار أخذا بعين الاعتبار صغر المبلغ وان المصلحة المحمية تستدعي التدخل الفوري بعيدا عن الإجراءات الشكلية خاصة إذا كان المستغيث هو الطفل.

ثالثا: نلاحظ أن المشرع في القانون الجديد تخلى عن معيار إقامة الحدث في تحديد اختصاص قاضي الأحداث إذ وسع في نطاق اختصاصه ليشمل محل إقامته، أو مسكنه أو محل إقامة أو مسكن ممثله الشرعي ومكان تواجد الطفل كل ذلك حماية لمصلحة الطفل.

حالة تطبيقية:

1. الطلب الموجه من السيدة (ع ل) الموجه إلى السيد قاضي الأحداث بالقالة أين تلتمس فيه إيداع ابنها في دار طفولة المسعفة لأنها تعيش في ظروف صعبة وإنها لاستطيع تربية ابنها وعليه تلتمس إيواءه لكي لا يضيع نسخة من طلب مرفقة (نسخة من طلب الموجه إلى قاضي الأحداث من طرف ممثله الشرعي (الأم) مرفقة كملحق)

2. العريضة الموجه من السيد وكيل الجمهورية لدى محكمة القالة إلى قاضي الأحداث يلتمس فيها أصدر أمر بوضع الطفلة (ج ك) المعرضة لخطر معنوي بمركز مخصص في حماية الأطفال عملا بنص المادة 32و 41 من القانون رقم 12/15 المتعلق بحماية الطفل (نسخة من العريضة المقدمة من السيد وكيل الجمهورية مرفقة كملحق.)

3.الطلب الموجه من الكفيل إلى السيد قاضي الأحداث بمسيلة بواسطة محاميه أين يلتمس فيه إيداع الطفل المكفول لعدم قدرته على رعايته بعد أن توفيت زوجته. (نسخة من الطلب الكفيل مرفقة كملحق)

الفرع الثاني: التدابير المتخذة لحماية الطفل

تنص المواد من 33 إلى 45 على التدابير الواجب على قاضي الأحداث اتخذها عند تلقيه للعريضة أو التصريح الشفوي من الطفل الموجود في خطر وهي كالأتي:

أولا: أثناء التحقيق: يقوم قاضي الأحداث باتخاذ التدابير الآتية:

1. استدعاء على الفور الطفل ووليه الشرعي وسماع أقوالهم وتلقى أراءهم بالنسبة لوضعية الطفل ومستقبلة مع جواز استعانة الطفل بمحامي أين يتم سماع على محضر يسمى محضر سماع أقوال المسؤول المدني عن الحدث في خطر معنوي (نسخة من محضر سماع المسؤول المدني مرفق كملحق)
2. يجوز لقاضي الأحداث القيام بدراسة شخصية الطفل بواسطة البحث الاجتماعي والفحوص الطبية والعقلية والنفسانية ومراقبة سلوكه إذا اقتضى الآمر ذلك فمثلا توجيه أمر إلى طبيب من اجل معاينة طفل موجود في خطر معنوي لكي يقدم له تقرير حول حالته الصحية (نسخة من الأمر الموجه لطبيب مرفق كملحق)
3. كما يجوز له تلقي كل المعلومات والتقارير المتعلقة بوضعية الطفل من أي شخص يرى فائدة من سماعه وله الاستعانة بالوسط المفتوح
4. يجوز له أثناء التحقيق أن يتخذ بشأن الطفل وبموجب أمر بالحراسة المؤقتة أحد التدابير الآتية:
   - ✓ إبقاء الطفل في أسرته
   - ✓ تسليم الطفل إلى شخص أو عائلة جديرين بالثقة
   - ✓ أو تكليف الوسط المفتوح بملاحظة الطفل في وسطه الأسري أو المدرسي أو المهني.
5. يمكن لقاضي الأحداث أن يأمر بوضع الطفل بصفة مؤقتة في: (نسخة من الأمر مرفقة كملحق)
   - ✓ مركز متخصص في حماية الأطفال في خطر
   - ✓ مصلحة مكلفة بمساعدة الطفولة

- ✓ مركز أو مؤسسة استشفائية، إذا كان الطفل في حاجة إلى تكفل صحي أو نفسي.

6 . لا يمكن أن تتجاوز مدة التدابير المؤقتة المتخذة أثناء التحقيق ستة 06 أشهر مع وجوب إعلام الطفل وممثله الشرعي خلال 48 ساعة من صدورها بأية وسيلة كانت.

حالة تطبيقية: الأمر الصادر عن قاضي الأحداث بمسلة المتضمن وضع الحدث (ي ع) مؤقتا في مركز الطفولة المسعفة بسطيف لمدة ستة أشهر إلى غاية الفصل النهائي في قضيته.

ثانيا: بعد الانتهاء من التحقيق: بعد الانتهاء من التحقيق يقوم قاضي الأحداث بما يلي:

1. إرسال الملف إلى وكيل الجمهورية للاطلاع عليه ويكون ذلك بموجب أمر بالإبلاغ. (نسخة من الأمر بالإبلاغ مرفق كملحق)
2. استدعاء الطفل وممثله الشرعي والمحامي عند الاقتضاء بموجب رسالة موصى عليها مع العلم بالوصول قبل ثمانية أيام على الأقل من النظر في القضية.
3. يسمع قاضي الأحداث بمكتبه الأطراف وكل شخص يرى فائدة من سماعه كما يجوز له إعفاء الطفل من المثول أمامه آو الآمر بانسحابه أثناء المناقشات أو بعضها إذا اقتضت مصلحته ذلك.
4. يتخذ قاضي الأحداث بموجب أمر أحد التدابير التي نصت عليها المادة 40 على النحو الأتي:

- ✓ إبقاء الطفل في أسرته (نسخة من الأمر ابقاء الطفل في اسرته مرفق كملحق)
- ✓ تسليم الطفل لوالده أو لوالدته الذي يمارس حق الحصانة، ما لم تكن قد سقطت عنه.
- ✓ تسليم الطفل إلى أحد أقاربه.
- ✓ تسليم الطفل إلى شخص أو عائلة جديرين بالثقة: ولكن المشرع لم يحدد الشروط الواجب توفرها في الأشخاص والعائلات الجديرة بالثقة عن طريق التنظيم وهي تبقى سلطة تقديرية للقاضي (نسخة من أمر وضع الحدث لدى الغير مرفق كملحق)
- ✓ يجوز له أن يكلف مصالح الوسط المفتوح بمتابعة وملاحظة الطفل وتقديم الحماية له من خلال توفير المساعدة الضرورية لتربيته وتكوينه ورعايته مع وجوب تقديمه لتقرير دوري حول تطور وضعيته. (نسخة من طلب موجه من قاضي الأحداث إلى مدربة مركز الطفولة مسعفة اين يلتمس فيها تقرير حول وضعية حدث مرفق كملحق)

5. يجوز لقاضي الأحداث أن يأمر بوضع الطفل إما في: مركز متخصص في حماية الأطفال في خطر أو بمصلحة مكلفة بمساعدة الطفولة. (نسخة من الأمر الوضع بمركز حماية الأحداث مرفق كملحق)

6 . **مدة التدبير ونهايتها**: تنص المادة 42 من قانون حماية الطفل أنه: يجب أن تكون التدابير المقررة في المادتين 40و 41 لمدة سنتين 02 قابلة للتجديد ولا يمكن أن تتجاوز في كل الأحوال تاريخ بلوغ الطفل سن الرشد الجزائي.

. يمكن لقاضي الأحداث عند الضرورة أن يمدد الحماية إلى إحدى وعشرون سنة بناء على طلب من سلم إليه الطفل أو من قبل المعني (الطفل) أو من تلقاء نفسه.

. تنتهي مدة الحماية بنهاية الوقت المحدد لها، كما يمكن لقاضي الأحداث أن ينهي الحماية بموجب أمر بناء على طلب المعني بمجرد أن يصبح قادرا على التكفل بنفسه.

7. **الطعن في التدبير ومراجعته:**

تنص المادة 43 على أن " تبلغ الأوامر المنصوص عليها في المادتين 40 و4 من هذا القانون بأية وسيلة إلى الطفل وممثله الشرعي خلال 48 ساعة من صدورها

لا تكون هذه الأوامر قابلة لأي طريق من طرق الطعن " إذن من خلال نص المادة نستنتج أن كافة الأوامر التي تصدر عن قاضي الأحداث والتي يتخذ بشأنها أحد التدابير المنصوص عليها في المادتين 40و 41 لا تكون قابلة لأي طعن وهو ما يخدم مصلحة الطفل وذلك بالتصدي لوضعية الخطر التي هو فيه.

. ولكن سمحت المادة 45 لقاضي الأحداث أن يعدل ما أمر به أو العدول عنه بناءا على طلب الطفل أو ممثله الشرعي أو وكيل الجمهورية أو من تلقاء نفسه على أن يبت في طلب المراجعة خلال مدة لا تتجاوز شهر من تقديمه له .[1]

قائمة المراجع:

1) اتفاقية حقوق الطفل، صادقت عليها الجمعية العامة للأمم المتحدة بتاريخ 20 نوفمبر 1989 والتي دخلت حيز التنفيذ في 02 /1990/09 والمصادق عليها مع تصريحات التفسيرية بموجب المرسوم الرئاسي رقم 92-461 المؤرخ في 13-12-1992 الجريدة الرسمية عدد91 المؤرخة في 23 دسمبر 1992.

2) بوسقيعة، أحسن. (2013). الوجيز في القانون الجزائي الخاص الجزء الأول الطبعة الخامسة عشر

3) بولحية، شهيرة. (2010). حقوق الطفل بين المواثيق الدولية وقانون العقوبات الجزائري. الإسكندرية: دار الجامعة الجديد الازاريطة

4) خرباش، عقيلة. (2009). حماية الأولاد من الإهمال المعنوي. مجلة دراسات قانونية، مركز البصيرة للبحوث، 12

5) سليمان، بشرى، والعبيدي، حسين. (2010). الانتهاكات الجنائية الدولية لحقوق الطفل، منشورات الحلبي الحقوقية، الطبعة الأولى

6) قانون 15-12 المتعلق بحماية الطفل المؤرخ في 15-07-2015 جريدة رسمية عدد 39 المؤرخة في 19 جويلة 2015

[1] :نسخة من أمر القاضي بمراجعة التدبير مرفق كملحق.

جريمة التنمر الالكتروني

The crime of cyberbullying

أ. منى رجب الشاعري/ الاكاديمية الليبية للدراسات العليا، بنغازي/ليبيا
Prof.Mona Rajab Al shari/ Libyan Academy of Higher Studies, Benghazi/Libya

ملخص الدراسة:

تعد جريمة التنمر الالكتروني من الجرائم التي ساعد على انتشارها، سرعة التطور التكنولوجي بفعل الانترنت الذي ساهم بشكل مباشر في انتشار العديد من الجرائم الالكترونية والتي من بينها، جريمة التنمر الالكتروني.

حيث إن القصد منها الاضرار بالآخرين ومضايقتهم بشتى السبل والوسائل، وذلك من خلال الإساءة لهم، وانتهاك خصوصياتهم والتلاعب بأسرارهم الشخصية، ونشرها على أوسع نطاق، وتشويه سمعتهم واستعمال الفاظ نابية عبر وسائل التواصل الاجتماعي من القذف والسب.

ولقد تنبهت الكثير من الدول الى جريمة التنمر الالكتروني، باعتبارها مشكلة خطيرة اضرت بالمجتمعات فقامت بالعديد من الجهود من أجل مكافحتها للحد من انتشارها، ولقد تناولت في هذه المداخلة جريمة التنمر الالكتروني بمقدمة، ولقد تناولت تعريف لها في المطلب الأول، وتطرقت الى وسائل هذه الجريمة في المطلب الثاني، ثم السبل والآليات التي استخدمتها الدول لمكافحتها والحد منها في المطلب الثالث، ثم الخاتمة التي جاءت بجملة من التوصيات والنتائج.

الكلمات المفتاحية: التنمر الإلكتروني، وسائلها، طرق مكافحتها والوقاية منها.

Abstract:

The crime of cyberbullying is one of the crimes that helped its spread, the speed of technological development due to the Internet, which directly contributed to the spread of many electronic crimes, including the crime of cyberbullying.

As it is intended to harm and harass others in various ways and means, by abusing them, violating their privacy, manipulating them on the widest scale, distorting their reputation and using profanity through social media, including slander and slander.

Many countries have become aware of the crime of cyber-bullying, as a serious problem that has harmed societies, So they made many efforts to combat it to limit its spread.

In this intervention, I dealt with the crime of cyber-bullying with an introduction, and I dealt with a definition of it in the first requirement, and I discussed the means of this crime in The second requirement, then the ways and mechanisms that countries used to combat and limit them in the third requirement, then the ways and mechanisms that countries used to combat and limit them in the third requirement, then the conclusion that came with a set of recommendations and results.

Keywords : Cyberbullying, its means, Methods of combating and preventing it.

مقدمة:

لقد ساعد التقدم التكنولوجي وانتشار الانترنت في العالم، على تنوع الجرائم الإلكترونية، وظهور العيد من صور الانحراف السلوكي القديم في حلة جديدة، تختلف باختلاف تطور وتقدم العلم والتقنية وتغير أفكار الشعوب ومعتقداتهم، فظهرت العديد من الممارسات العنيفة والغير سلوكية سواء من فئة الأطفال أو الشباب عبر وسائل التواصل الاجتماعي والتي أثرت على الكثير من الناس في العالم، وشكلت سلوكاً يعاقب عليه قانوناً ومن أشكال وأنواع هذه السلوكيات والتي أصبحت من الجرائم الالكترونية المعاقب عليها، هي جريمة التنمر الإلكتروني.

أولاً: أهمية الدراسة:

تظهر الأهمية في دراسة هذا النوع من الجرائم الإلكترونية تحديداً، هو انتشارها بشكل واسع في مختلف العالم، وتضرر العديد منه، خاصة وان الدراسات القانونية وغيرها شحيحة وبالكاد نجد من يتحدث عن هذا النوع من الجرائم في مؤلفات موسعة، كما أن المشرعين في مختلف الدول لم يسلطوا الضوء على تشريع قانون خاص بجرائم التنمر الالكتروني، ومنها من لا يعده جريمة ويستخف به.

ثانياً: أهداف الدراسة:

نسعى من خلال دراستنا الى التعريف بمضمون جريمة التنمر الإلكتروني، وإلى الوسائل التي تمكن الجناة من ارتكابها والدافع إليها، كما تهدف دراستنا إلى معرفة الأسباب والوسائل التي سعت إليها الدول لمعرفة أسباب انتشارها وتوسعها، والطرق التي لجأت اليها من أجل القضاء عليها ومحاربتها باعتبارها آفة فوق انها جريمة معاقب عليها.

ثالثاً: إشكالية الدراسة:

إن تطور وسائل الاتصال الالكتروني الحديث، ساهمت بدرجة كبيرة الى تصاعد وتيرة الاعتداءات والتهديدات الالكترونية بين الافراد، فقد دفعت الشباب والمراهقين والأطفال الى الدخول عبر منصات التواصل المتعددة، إلى استخدام وممارسة العنف والتحرش، واستعمال وسائل السب والقذف، وهو ما يطلق عليه التنمر الإلكتروني، وهو ما يسمى في كثير من الأحيان بالتحرش الإلكتروني عبر الانترنت.

رابعاً: منهجية الدراسة:

لقد اعتمدت في دراستي على المنهج التحليلي والذي من خلال يمكننا من دراسة هذه الجريمة الإلكترونية، وتحليل جوانبها للوصول إلى علاج يقضي أو يخفف من حدتها، كما لجأنا في الدراسة إلى استخدام المنهج المقارن، والذي يمكننا من دراسة الجريمة وذلك بمقارنتها بعدة دول.

خامساً: دراسات سابقة:

ظهرت العديد من الاحصائيات والدراسات التي لا تكاد تجمع في تقييمها على إحصائية يمكن الاعتماد عليها حول جريمة التنمر الإلكتروني، إذ أشارت دراسة روبن وسوزان في 2007م إلى أن نسبة 42% من الافراد قد تم التنمر عليهم خلال تواجدهم على الأنترنت، ثم زادت هذه النسبة في عام 2008م لتتعدى النسبة السابقة إلى 72% من التنمر الإلكتروني الذي يحدث عبر الأنترنت في دراسة اجراها كلاً من (gross & Juvonen).

فضلاً على أن مرصد حقوق الأنترنت أظهر استطلاع أجراه أن 34.3% من الشباب هم من ضحايا التنمر عبر الأنترنت، وزعم أن 21.2% يتعرضون للمضايقات.

سادساً: هيكلية الدراسة:

لقد قسمت الدراسة في هذا البحث من أجل الإلمام بالموضوع الى ثلاث مطالب حيث تناولت في المطلب الأول: مفهوم التنمر الإلكتروني، تلاه في المطلب الثاني: إلى وسائل الجريمة الإلكترونية، وفى المطلب الثالث: الآيات التي اتبعتها الدول لمكافحة جريمة التنمر الإلكتروني، وانتهيت بخاتمة تضمنت النتائج والتوصيات.

المطلب الأول: الإطار المفاهيمي لجريمة التنمر الالكتروني:

تعتبر جريمة التنمر من الجرائم الالكترونية، التي لازالت كثير من الدول في غفلة عنها، رغم اتساعها بشكل متزايد مع تزايد استعمال وسائل الاتصال والتكنولوجيا، خاصة وان أصبحت اكثير من فئات الشباب والأطفال يتعرضون للتنمر الالكتروني، فكان من الأهمية بمكان تسليط الضوء على هذه الجريمة، لذلك سنتناول مفهومها من عدة زوايا على النحو الاتي:

الفرع الأول: مفهوم التنمر لغة:

تشتق كلمة التنمر لغوياً من اللفظ نمر بمعنى غضب وساء خلقه، وأصبح يشبه انمر الغاضب (قاموس،2022) ويعرف التنمر بأنه شكل من أشكال الايذاء والمضايقة المتعمدة من فرد أو مجموعة لشخص ما باستخدام الكلمات اللفظية البذيئة، بشكل متكرر.

كما ورد في لسان العرب لابن منظور في المجلد الخامس، يقال للرجل السيء الخلق قد تنمر ونمر وجهه، أي غيره وعبسه، وتنمر له أي تغير وتنكر وأوعده، لان النمر لا تلقاه أبداً إلا متنكراً غضباناً، قال ابن بري معنى تنمروا تنكروا لعدوهم، وأصله من النمر لأنه من أمكن السباع وأخبته (ابن منظور،1956م، ص.200).

وتأتي كلمة تنمر في المعجم الوسيط تنمر تشبه بالنمر في لونه أو طبعه، ويقال تنمر لفلان تنكر له وأوعده، وتنمر مدد في صوته عند الوعيد، وفى حديث أبي أيوب: أنه أتى بداية سرجها نمور فنزع الصفة، يعنى الميثرة، فقيل الجديات نمور يعنى البداد، فقال إنما ينهي عن الصفة.

وقال ثعلب من قال نمر رده إلى أنمر، ونمار عنده جمع نمر كذئب وذئاب، وكذلك نمور عنده جمع نمر، وذهب الأصمعي في قوله: تنمر له أي تنكر وتغير وأوعده لان النمر لا تلقاه أبداً إلا متنكراً غضبان، وفى حديث الحد يبيه: قد لبسوا لك جلود النمور، كونها كناية عن شدة الحقد والغضب وتشبيهاً بأخلاق النمر وشراسته (قاموس اللغة،2022).

الفرع الثاني: مفهوم التنمر اصطلاحاً:

التنمر وبالإنجليزية (Bullying) وهي ظاهرة تتسم بالعدوانية الغير مرغوبة، حيث يقوم الشخص المتنمر بتصرفات عدائية، مثل مهاجمة الاخرين جسدياً أو لفظياً أو تهديدهم، أو نشر اشاعات سيئة عنهم، وقد يكون هذا التصرف متكرر مع مرور الزمن، واذي يعود على كلا الشخصين المتنمر والمتنمر عليه بوقوعهم بمشاكل فعلية وطويلة الأمد.

وغالباً ما يكون الشخص المتنمر أقوى من المتنمر عليه، حيث يكون موازين اقوى بهذه الحالة غير متوازنة، فيستخدم الشخص المتنمر قواه، سواء أكانت هذه القوى جسدية أو معرفته لبعض المعلومات المحرجة عن الشخص المتنمر عليه، وذلك بهدف التحكم به أو إلحاق الأذى به (الإلكتروني،2022).

كما تناوله البعض حول مفهوم الصعلكة mobbing حيث شاع استخدامه في البلدان الاسكندنافية، ويقصد به قيام تلميذ أو أكثر بمضايقة وإيذاء تلميذ آخر إيذاءاً متكرر عن طريق ممارسة بعض السلوكيات السلبية عليه.

وقد عرف الباحث النرويجي " دان أولويس" التنمر بأنه " تعرض شخص بشكل متكرر وعلى مدار الوقت، إلى أفعال سلبية من جانب واحد أو أكثر من الأشخاص الآخرين " كما عرف اعمل السلبي بأنه " تعمد شخص إصابة أو ازعاج راحة شخص آخر، من خلال الاتصال الجسدي، أو من خلال الكلمات، أو بطرائق أخرى"، وقدم أولويس عام 1978م تعريفاً يعد من أول وأهم التعريفات التي تناولت مفهوم التنمر حيث عرفه بأنه: "تعرض الطالب وبشكل متكرر خلال فترة من الوقت الى سلوكيات سلبية من جانب طال آخر أو أكثر"(حاسي، مليكة2020، ص.67).

كما يعرف التنمر كذلك بأنه:" إساءة استخدام القوة الحقيقية أو المدركة بين التلاميذ داخل المدرسة، ويحدث ذلك بصورة مستمرة ومتكررة، بغرض السيطرة على الآخرين، فالتنمر إذاً سلوك سلبي ناتج عن سوء استخدام القوى بين الأخرى
(شطبي، ص.75).أما سميث وشارب فقد عرفا التنمر بأنه:" هو نهج يتم فيه استغلال التفاوت في القوة على نحو سلبي " وفي هذا الصدد أكد كل من جوفاتن، جراهام، شيستر، على أن التنمر هو: "سلوك يحصل في وجود عدم التوازن بين طرفين، يسمى الأول المتنمر، ويسمى الآخر الضحية، وهو يتضمن الإيذاء الجسدي والإيذاء اللفظي والإذلال بشكل عام "(عيناب،2017، 14).

في حين عرف (Barto) التنمر وفقاً لثلاثة معايير ، الأول : أنه عام ومتعمد، وقد يكون مادياً او لفظياً او جسدياً أو إلكترونيا، الثاني: التنمر يكشف عن ضحايا لعدوان متكرر عبر فترة ممتدة من الزمن، أما المعيار الثالث: التنمر يحدث اختلال بالغ في العلاقات الشخصية (القضاة، الصبحين، 2013، ص.14).

في حين يرى علماء النفس أن سلوك التنمر قد يتحول الى سلوك منحرف والذي يتحول وفقاً لمنظورهم " السلوك المضاد للمجتمع «وعندها تصطدم شخصية المتنمر بالقوانين الجزائية أو الأعراف العامة أو عدم التوافق مع الاخرين، وهو ما يوصف بالشخصية السيكوباتية، التي تمارس أفعالاً مضادة للمجتمع ومنها السلوك التنمري(سايحي، 88).

ومن وجهة نظري كباحثة أكاديمية أرى أن التنمر هو: " ذلك الفعل أو السلوك السيء الذي يلحق الضرر بالآخرين فرداً أو مجموعة، بعدة أساليب ووسائل قد تكون جسدية أو نفسية أو مادية أو اجتماعية وقد تكون إلكترونية، ويكون من سبب الضرر هو المتنمر".

الفرع الثالث: مفهوم التنمر الالكتروني:

يعتبر التنمر الإلكتروني أحد التبعات السلبية اتى خلفها التطور التكنولوجي، ورغم إن التنمر سلوك سلبي قديم من زمن إلا إن ظهوره في العالم الافتراضي زاد من خطورته، وذلك لتوسع حرية مقترفيه للمساحة التي يمنحها الانترنت في العالم الافتراضي، فضلاً على تفاقم آثاره على ضحاياه، وفى ذلك أشار كل من "بفي" و "ديان" أن التنمر الالكتروني يتضمن مضايقات وتحرشات عن بعد باستخدام وسائل التواصل الالكتروني، من طرف متنمر لإحداث جو نفسي للضحية يتسم بالتهديد والقلق.

كما أكد كل "تروبي" و "هائل" و "شيلدز" إن هذا السلوك يتضمن استخدام وسائل الاتصال الالكتروني في إيقاع أذى مقصود بطرف آخر دون الاتصال الجسدي المباشر(حبيب، 1). وقد فصل "توكيوناجا" في تحديد معنى التنمر الإلكتروني بأنه سلوك يتم عبر الانترنت أو وسائل الإعلام الإلكترونية أو الرقمية، والذي يقوم به فرد أو جماعة من خلال الاتصال المتكرر الذي يتضمن رسالة عدوانية، والتي تهدف الى إلحاق الأذى بالآخرين، وقد تكون هوية المتنمر مجهولة أو معروفة لضحية (المكانين وآخرون،2018، ص.57).

وقد عرف (Belsey) في 2006م التنمر الالكتروني بأنه: " استخدام تكنولوجيا المعلومات والاتصالات مثل ابريد الالكتروني وGMS والرسائل النصية والرسائل الفورية وصفحات الويب الشخصية لتبنى موقف عدائي متعمد ومتكرر تجاه فرد أو مجموعة، مع نية التسبب في ضرر للآخرين .

كما تشير الدراسات أن خمسة من الخصائص المميزة للتكنولوجيا تسمح للأفراد استخدام الانترنت بشكل مسيئ كما هو الحال في التنمر الإلكتروني وهى استخدام المجهولية، أو إخفاء الهوية، مع إمكانية إنشاء حسابات إلكترونية مؤقتة أو بأسماء مستعارة أو مزورة، كما إن غياب الاتصال المباشر بين المتنمر والضحية، مع صعوبة تخلي بعض المراهقين والشباب من الاستخدام الدائم للاتصال الالكتروني الذي جعل الاتصال عبر الانترنت من الالتزامات الاجتماعية مما زاد الامر تعقيداً(مقراني، 2018، ص.30).

كما يمكن تعريف التنمر الالكتروني بأنه: "شكل من أشكال العدوان يعتمد على استخدام وسائل الاتصال الحديثة وتطبيقات الانترنت من الهواتف الذكية، والحواسيب المحمولة، والألواح، وكاميرات الفيديو، الحساب البريدي، وصفحات الواب في نشر منشورات" بوست "أو تعليقات تسبب النكد للضحية أو الترويج لإخبار كاذبة، أو إرسال رسائل إلكترونية للتحرش بالضحية بهدف ارباكه وإصابته بحالة من النكد المعنوي والمادي"

كما يعرف التنمر الالكتروني على أنه: "سلوك يتم القيام به عبر الميديا الالكترونية، أو الرقمية بقصد إيقاع الضرر بالآخرين، وعدم راحتهم والتنمر الإلكتروني ما هو إلا امتداد للتنمر التقليدي " (المكانين وآخرون، ص.87).

ويعرف أيضاً: هو ذلك الايذاء المتعمد يتم بنشاط عن طريق الأجهزة الرقمية كالهواتف المحمولة وذلك بإرسال رسائل عبر وسائل التواصل الاجتماعي أو عبر الألعاب والتطبيقات من خلال شبكة الأنترنت ويشمل عدة أمور تسبب ضرر للشخص المتنمر عليه وتشمل مشاركة معلومات شخصية محرجة لغرض إزعاج وبث الخوف في نفس الشخص المتنمر عليه (حاسي، 69).

كما ذكر موقع ويكيبيديا أن التنمر هو استخدام الانترنت والتقنيات المتعلقة به، بهدف إلحاق الضرر بالآخرين بطرق متعمدة متكررة وعدائية، كما ذكرت الجمعية النسائية البحرينية-التنمية الإنسانية أن التنمر الالكتروني هو العمل على إيقاع الأذى على الطرف الاخر وذلك باستخدام الأجهزة الالكترونية المرتبطة بالأنترنت مثل الأجهزة اللوحية.

كما يعرفه آخرون بأنه فعل عدائي يقوم به المتنمر إلكترونياً، باستخدام التقنية الحديثة ضد طرف آخر، بغرض إلحاق الضرر به مادياً، معنوياً، اجتماعياً ونفسياً، وتظهر الخطورة في جريمة التنمر الإلكتروني في أن المتنمر مجهول الهوية في أغلب الأحيان، بالإضافة إلى أن مادة المتنمر متوفرة على الشبكة المعلوماتية (الأنترنت) بصورة دائمة إذا لم يتم التدخل من الجهات ذات العلاقة لإزالتها، وهذا يعنى أن التنمر قد يطول زمنه على الضحية مما يتسبب في أضرار مختلفة العافية،2022).

وعليه من خلال جميع التعريفات السالفة الذكر يمكن أن نخلص كباحث أكاديمي إلى أن جريمة التنمر الإلكتروني، هي ذلك السلوك العدواني المتعمد من المتنمر باستخدام وسائل التقنية وشبكة الانترنت والتكنولوجيا، لإحداث الضرر بالآخرين سواء معنوي أو مادي غرض التنمر في إحداث الحصول على نفع من الشخص المتنمر عليه قد يكون مادياً أو معنوياً.

المطلب الثاني: وسائل جريمة التنمر الإلكتروني:

بفعل التطور السريع لاستخدام التكنولوجيا وانتشارها في كل بيت وجهة عمل، إحداث ذلك العديد من الجرائم الإلكترونية ومنها جريمة التنمر الالكتروني التي يستخدم فيها المتنمر العديد من الوسائل ويستحدث غيرها، بقصد الاضرار ، وذكر الهاجري أن شبكة الأنترنت استخدمت في بدايتها بشكل رئيسي في تبادل المعلومات والبيانات، أما الان فقد اتسع وتنوع استخدامه حيث أصبح من الصعب حصرها، وهذا القول مع مطلع التسعينات ، حيث ظهور ما يسمى بشبكة النسيج العالمية world wide web بسبب التطور الهائل في تقنية المعلومات والاتصالات 17 . وفى هذا المطلب نسلط الضوء على تلك الوسائل المستخدمة على النحو الاتي:

1) المكالمات الهاتفية:

تتمثل في المكالمات الصوتية عبر الهواتف الذكية، أو مواقع الويب التي يستهدف فاعلها ترويع الضحية عبر السب ، القذف، التهديد، أو استلاء التنمر على بيانات خصوصية بالضحية والتهديد بنشرها واطلاع الغير عليها..

2) الصور ومقاطع الفيديو:

تتمثل هذه الوسيلة باستيلاء المتنمر على صور ومقاطع فيديو شخصية تعود للضحية، قام بتداولها بين أصدقائه، وقيام المتنمر بإعادة تداولها كما هي أو قد يجرى عليها التغير والتغيير بالإضافة، والتحوير عليها ببرامج معالجات الصور والفيديو، إذ يجعلها وسيلة لصنع المعطيات المخلة بالأخلاق والآداب العامة، التي تشمل الصور والكتابات والاصوات، فإذا توافرت الصور ومقاطع الفيديو الواضحة المعنية بطريق الإنتاج، انتقل الفاعل الى مظاهر جريمة الاستغلال الجنسي للضحية عبر الأنترنت (الشيخي، 2022).

3) الرسائل النصية:

تتضمن الرسائل عبارات التهديد بإفشاء الاسرار أو بث الشائعات، أو ابتزازه مادياً أو جنسياً مقابل عدم تكرار التهديد.

4) البريد الالكتروني:

تتمثل بإرسال الفاعل رسالة الى بريد الضحية تتضمن فيروساً يستهدف منه الاستيلاء على بريده الالكتروني، والاطلاع على رسائله بمجرد فتح رسالة المتنمر، وهذا يتيح للفاعل إمكانية ارسال رسائل مخلة للحياء لأصدقائه، أو رسائل تهديدية للغير على أنها مرسلة باسم الضحية، واتى قد توقع الضحية في الحرج والمشكلات الاجتماعية، فضلاً على قيام المتنمر بإرسال مواقع إلكترونية مخادعة لافتة للانتباه، بمجرد دخول الضحية إليها يتمكن المتنمر من نشر أخبار وصور زائفة وغير لائقة على صفحة الضحية(الهاجري،2004، ص.30).

5) غرف المحاورة:

بالنظر إلى إقبال الأشخاص على هذه المواقع استغل المتنمرين ضحاياهم عن طريق استدراجهم في محادثات تتطور لتكون ذات طبيعة جنسية، وتأخذ عمقاً كبيراً لانعدام الرقابة الاجتماعية بين المتحادثين، فضلاً عن محاولة المتنمر إلحاق الأذى بالضحية عن طريق الاستيلاء وقرصنة البيانات الشخصية للضحية عبر او صور منافية للأخلاق والآداب العامة (مجيد، 2019، ص.134).

بالإضافة الى وجود العديد من الوسائل الأخرى التي يقوم فيها المتنمر باصطياد فريسته منها نذكرها على سبيل المثال هي مواقع شبكات التواصل الاجتماعي، لوحات الحوار والتي تستخدم للتعليق في موضوع معين، بالإضافة الى ألعاب الانترنت.

وبعد التعرف على الوسائل المستخدمة من جانب المتنمر لضحيته والتي تتعدد بتطور التقنية، واستحداث كل ما هو جديد عبر التطبيقات المستخدمة عبر الانترنت، إذاً فما هي الوسائل الكفيلة للوقاية من جريمة التنمر الالكتروني، وما هي الوسائل والسبل الكفيلة للقضاء عليها، سوف نتعرف على كل هذه الأمور في المطلب الثالث، وذلك على النحو الاتي:

المطلب الثالث: الوسائل والاليات الكفيلة للقضاء على جريمة التنمر الالكتروني:

لقد تنوعت الأساليب والسبل التي قامت بها الدول لحماية مواطنيها والقاطنين فيها من التنمر الالكتروني، فمنها من نص على تشريعات قانونية صارمة ومنها من اكتفى بدور العقوبة المخففة، والتي لاقت الأخيرة نقداً واسع المجال، ومنها مؤسسات المجتمع الدولي والمدني التي بذلت من الجهود للحد منها أو التخفيف من سرعة انتشارها، لمحاولة القضاء عليها، عليه سوف نبين ذلك في عدة فروع وذلك على النحو الآتي:

الفرع الأول: وسائل القضاء على جريمة التنمر الالكتروني على المستوى الدولي:

لقد سعت الولايات المتحدة الامريكية الى محاولة القضاء على هذه الجريمة الالكترونية، والتي ازداد تفشيها وخاصة بعد سرعة التقدم والتكنولوجيا، واستعمال الأنترنت بشكل سهل وميسر لكل فرد، خاصة وأنها من الجريمة التي يصعب اكتشافها وضبط فاعلها ومعاقبته، لاستخدامه الأسماء الوهمية والمستعارة.

ففي أمريكا على المستوى الفيدرالي لا يوجد قانون اتحادي يعالج مباشرة جريمة التنمر، لكن في بعض الحالات يتداخل التنمر المبني على أساس الأصل القومي، العرقي، اللون، الجنس، الدين، الإعاقة، مع جريمة المضايقة التمييزية التي تغطيها قوانين الحقوق المدنية الفيدرالية اتى تطبقها وزارة التعليم الامريكية، ووزارة العدل الامريكية، فتكون المدارس ملزمة قانوناً بمعالجتها بصرف النظر عن مسمى السلوك (تنمر، مضايقة، إغاضة الخ) (الليثي، درويش، 2017، ص.204).

وتعالج وزارة التعليم الامريكية التنمر المبني على أساس عرق الطالب أو لونه أو أصله القومي أو جنسه أو إعاقته دون التنمر الديني بموجب البند السادس من قانون الحقوق المدنية لعام 1964م، إلا إن وزارة العدل الامريكية لها اختصاص على الدين بموجب الباب الرابع من قانون الحقوق المدنية لعام 1964م فتعالج التنمر المبنى على أساس الدين.

والمدارس التي تفشل في الاستجابة بشكل مناسب على سلوكيات التنمر المتداخلة مع جريمة المضايقة التمييزية ستنتهك فصل أو أكثر من قوانين الحقوق المدنية لعام 1964م التي تنفذها كلاً من وزارة التعليم ووزارة العدل بما في ذلك الباب الرابع والسادس من القانون سالف الذكر.

أما على مستوى الولايات المتحدة الامريكية بصفة عامة، قد أقرت تشريعات تدين التنمر، وكانت ولاية جورجيا أول ولاية سنت تشريعاً ضد التنمر المدرسي في عام 1999م، في حين تعد ولاية مونتانا آخر وأحدث ولاية سنت تشريعاً ضد التنمر المدرسي في عام 2015م.

فلقد اتخذ المشرعون في مختلف الولايات إجراءات لمنع التنمر وحماية الأطفال في كل ولاية، بما في ذلك جميع الولايات الخمسين ومقاطعة كولومبيا والاقاليم الخاضعة للولاية الامريكية، إذ قام البعض منها بتشريع قوانين ووضع سياسات وأنظمة تتعلق بالتنمر ، في حين طور آخرون سياساتها ولوائحها من المقاطعات الامريكية والمدارس تنفيذ سياسات وإجراءات معينة، في التحقيق في سلوكيات التنمر والرد عليها عند حدوثها، بينما اتجه قسم من الولايات الى وضع برامج وقائية للتنمر وإدراجها ضمن معايير التعليم الصحي أو التطوير المهني للمعلم، في حين لا تنص قوانين هذه الولايات عموماً على عقوبات محددة للأطفال اذين يمارسون سلوك التنمر، وقليل منهم يصنف التنمر على أنه جريمة جنائية (النجار، 2020، ص.144).

وفى بعض الأحوال نجد بعض الولايات تتناول التنمر التقليدي أو التنمر عبر الانترنت والسلوكيات ذات الصلة في قانون واحد، أو عبر قوانين متعددة (التحرش، المضايقة، المطاردة إلخ) وفى بعض الحالات يعاقب جنائياً الحدث المتنمر ضمن القوانين الخاصة بفئة الاحداث (الأمريكية، 2022).

ونتيجة لانتشار التنمر بشكل متسارع في القرن العشرين، وظهرت الكثير من الحالات لاسيما في المدارس، من الانتحار وإطلاق النار وغيرها، دفعت بالولايات الى سن تشريعات خاصة بالتنمر الالكتروني، وجعلها جريمة يعاقب عليها القانون، ولكن في الغالب ما تكون المسؤولية مدنية وليست جنائية، تكتفى بالتعويض وتترك في أيدى مسؤولي المدارس ، وغالباً ما يستخدم المدعون العامين قوانين المضايقة الجنائية والمطاردة الإلكترونية في الدعاوى في حالات الانتحار من جراء التنمر (النجار ،2020، ص.152).

فقد تتضمن عن فعل التنمر عقوبات جنائية كما في السابق، فتطبق قوانين الاعتداء إذا نجم على التنمر إيذاء بدني، وتطبق قوانين المضايقة والمطاردة الالكترونية إذا نجم على الفعل ارتكابه عبر الوسائل الالكترونية ، على سبيل المثال حدث في ولاية الألباما يسأل المتنمر ضمن قانون المضايقة أو التحرش كعقوبة جنحة إذا ارتكب الفاعل الازعاج والتحرش عن طريق شخص آخر سواء بفعل ركلات أو لمس أو اخضاعه لاتصال جسدي أو استخدام لغة مسيئة أو فاحشة وتشمل المضايقة التهديد الذي قد يكون لفظي أو غير لفظي وأن يكون القصد منه التهديد (الأمريكية، 2022).

الفرع الثاني: وسائل مكافحة التنمر الالكتروني على المستوى الإقليمي:

نبدأها في ليبيا فلقد طالب تقرير أعدته منظمة محامون من أجل العدالة في ليبيا الدولة الليبية بضرورة الاعتراف العلني بانتشار ممارسات العنف ضد المرأة ، بما في ذلك العنف الممارس على شبكات الأنترنت للتحقيق فيه ومعاقبة الجناة ، وفى ذلك قدم مجموعة من المحامون والقضاة الليبيين ونشطاء مدافعين عن حقوق الانسان، دراسة لمشروع قانون مكافحة العنف ضد المرأة لتجريم جميع أشكال العنف ضدها، وخاصة العنف الإلكتروني ، كما طالبت بضرورة سن تشريعات تتصل بالجرائم الإلكترونية والرقمية، مما يستوجب سن هذه التشريعات لردع المسيئين والجناة.

على الرغم من وجود استخدام للمواد المنصوص عليها في قانون العقوبات والمتصلة بجرائم السب والتشهير والتهديد في المواد (230،433،430) من قانون العقوبات الليبي، ولكن يشير الباحثين إن عدم إقدام المجنى عليهم على الشكوى من الجرائم الإلكترونية، هو عدم وجود قانون خاص يصرح تلك الجرائم، وبالتالي ضياع حقوق من تم الاعتداء عليهم (الإلكتروني، 2022).

ثم ما لبث أن قام مجلس النواب بتاريخ:26/أكتوبر/2021م بالمصادقة على قانون مكافحة الجرائم الإلكترونية، حيث نص في المادة الرابعة منه على "أن استخدام الانترنت ووسائل التقنية الحديثة يعد مشروعاً شريطة احترام النظام العام والآداب العامة "ونص في المادة 37 منه على العقوبة التي تصل إلى السجن لمدة 15 عاماً، وغرامة مالية لا تقل عن 10.000 عشرة آلاف دينار ليبي، لكل من بث إشاعة أو نشر معلومات أو بيانات تهدد الأمن أو السلامة العامة في الدولة، أو أي دولة أخرى "

كما نصت المادة 21 من القانون السالف الذكر على عقوبة بالحبس مدة لا تقل عن سنة: " كل من مزج أو ركب بغير تصريح مكتوب أو الكتروني من صاحب الشأن، صوتاً أو صورة لاحد الأشخاص باستخدام شبكة المعلومات الدولية أو بأي وسيلة إلكترونية أخرى، بقصد الاضرار بالآخرين".

وحيث إن هذا القانون تعرض لكثير من الانتقادات والعيوب وذلك لأنه غير صالح لتطبيق، وناشدت منظمات حقوقية بضرورة سحب هذا القانون أو إلغائه لأنه يتعارض مع المعايير الدولية لحقوق الانسان والالتزامات الدولية، من ذلك مان صت عليه المادتين (13،47) المتعلقتين بالاعتراض والتعرض، والتنصت غير المشروع، إن ذلك قد يحتم استخدام إجراءات كتبرير لحجب المعلومات على الصحفيين ، أو منع تواصلهم مع المبلغين بقصد مشاركة معلومات مع الجمهور ، وهذا يتنافى مع المادة 19 من العهد الدولي اخاص بالحقوق المدنية والسياسية التي تنص في الفقرة الثانية على انه : " لكل انسان الحق في حرية التعبير ويشمل هذا الحق حريته في التماس مختلف ضروب المعلومات والأفكار

وتلقيها ونقلها، إلى آخرين دونما اعتبار للحدود سواء في شكل مكتوب أو مطبوع أو في قالب فني، أو بأي وسيلة أخرى يختارها" (الجار، 2020، ص.153).

بالإضافة إلى الانتقادات الأخرى التي تعرض لها بحيث ينادوا الحقوقيون الى ضرورة الاجتماع مع مؤسسات المجتمع المدني، والمنظمات التي تتصل بحقوق الانسان وحرياته لكي يتلاءم القانون مع الحقوق والحريات وحقوق النشر واعمال الصحفيين والإعلاميين.

أما في العراق، فلقد سعت ابتداًء من دستورها الى حماية الحقوق والحريات ومنعت كل صور وأشكال الاعتداء عليها، وفرضت الجزاء القانوني على مرتكبها، ومن خلال تعريف جريمة التنمر نجد أن المتنمر يقحم نفسه في خصوصيات الضحية وينتهك حرمة حياته الخاصة، وعلى الرغم من خلو القوانين الجزائية في العراق من النص على تجريم جريمة التنمر الإلكتروني، إلا إن هذا لا يعني إفلات الجناة من الجريمة كون فعل التنمر الالكتروني يتداخل مع نصوص تجريمية في قانون العقوبات العراقي.

وبذلك يكون بإمكان المجنى عليه المطابة بالتعويض المدني والجزاء الجنائي معاً، ومن المواد التي يعاقب على مخالفتها المتنمر وفقاً لقانون العقوبات العراقي رقم 111 لسنة 1969م عندما تناول جريمة التهديد في الباب الثالث من الفصل الثالث في المادتين(430-432) إذ قد يعمد المتنمر الالكتروني الى تهديد الضحية قولاً أو فعلاً أو بالإشارة أو غيرها، حيث نص في المادة(1/430) على انه : " يعاقب بالسجن مدة لا تزيد على سبع سنوات أو بالحبس كل من هدد آخر بارتكاب جناية ضد نفسه أو ماله ،أو ضد نفس أو مال غيره بإسناد أمور مخدشة بالشرف أو إفشائها وكان ذلك مصحوباً بطلب أو بتكليف أمر، أو الامتناع عن فعل أو مقصوداً به ذلك" وفي الفقرة الثانية منه نصت على أن تكون العقوبة ذاتها إذا كان التهديد في خطاب خالي من اسم مرسله، أو كان منسوب صدوره الى جماعة سرية، موجودة أو مزعومة (الفلاح، 2022).

ومن الاحكام القضائية التي شهدتها العراق، حكم محكمة استئناف بغداد الرصافة الاتحادية بصفتها التمييزية بالرقم (98/جزاء /2014م والتي قضت فيه المحكمة بالإدانة وفق المادة 433 من قانون العقوبات العراقي، والتي عدت أن مواقع التواصل الاجتماعي مثل الفيس بوك، من وسائل العلانية، وإن نشر عبارات القذف عن طريقه يمثل نشراً بإحدى وسائل العلانية مما يوجب تشديد العقوبة على الجاني بقولها موقع التواصل تندرج عليه القوانين التي تنظم وسائل الاعلام الأخرى (الإلكتروني،2022).

وهذا جزء ما اتجهت اليه العراق بشأن التنمر وما استخدمته من وسائل لتجريم التنمر ومعاقبة مرتكبها، أما في الامارات العربية المتحدة فلقد شهدت إصدار تشريع في 20 سبتمبر 2021 سيكون سارياً ومعمول به ابتداءامن شهر يناير 2022م وهو ما يسمى قانون مكافحة الشائعات والجرائم الالكترونية، رقم 34 لسنة 2021م حيث استند القانون على مجموعة كبيرة من القوانين منها قانون الإجراءات الجنائية، قانون العقوبات وتعديلاته، وقانون مكافحة جرائم تقنية المعلومات بتعديلاته، قانون تنظيم قطاع الاتصالات، وعدة قوانين أخرى (العراقي، 1989م).

أما في مصر فلقد تصدت المحاكم المصرية لهذا النوع من الجرائم العصرية، ورغم أن المشرع لم يرصد مواد من قانون العقوبات، إلا أن العقوبة التي تطبق على المتنمر الجاني هي المادة الخاصة بالتهديد كتابة أو شفاهة أو وتعتبر جناية مادامت مصحوبة بأمر أو سداد مبالغ مالية.

ويؤكد أحد المحاميين في مصر بأنه إذا تقدم المجنى عليه بشكوى الى مراكز الشرطة ، فتتولى ملاحقة الجاني وتعقبه إلكترونياً ومحاكمته جنائياً ويواجه عقوبة لا تقل على ثلاث سنوات، على كل جاني متنمر يهدد بعض الأشخاص بنشرهم صوراً أو فيديوهات فاضحة، أو مخلة بالشرف ويطالب مقابل عدم نشرها تنفيذ أمور معينة قد تكون غير أخلاقية، أو سداد مبالغ مالية ضخمة، وأضاف أيضاً أن المشرع وضع قانوناً خاصاً لتطبيق مواده على من يرتكب هذه الحالات في القانون رقم 157 لسنة 2021م للتعدي على القيم والمبادئ الأسرية، كتشويه صورة أو إساءة بالقول أو نشر صور ساخرة أو مسيئة للأشخاص، وعقوبتها الحبس التي تتراوح من ستة شهور إلى ثلاث سنوات وغامة تتعدى 100 ألف جنيه، كما تقع عقوبة الابتزاز بالقياس على المادة 267 من قانون العقوبات مثل جريمة التهديد كتابة(يزيدي، 2015)..

ونلاحظ مما سبق أن الجهود المبذولة من الدول للحد من الجريمة الالكترونية، ومحاربة التنمر ومعاقبة مرتكبيه منها ما كان موفق، ومنها ما تعرض للانتقادات من خلال التشريعات الليبية الصادرة، منها قانون مكافحة الجرائم الالكترونية والذي تعرض لكثير من الانتقادات، وطالبوا بضرورة إلغائه وعدم تطبيقه، وكذلك في مصر والذي طالب فيه المحامون بضرورة سن تشريع خاص بالجرائم الإلكترونية.

الفرع الثالث: دور المنظمات الدولية في مكافحة التنمر الالكتروني:

قامت العديد من المنظمات الناشطة لمحاربة التنمر الالكتروني بأشكالها المختلفة، التي أصبحت تعرف بالجريمة القاتلة، من هذه المنظمات الشبكة الدولية للحقوق والتنمية " فهي من المنظمات التي تتولى حماية حقوق الطفل فقام مكتب المنظمة في اسبانيا باعتمادي مشروع ايراسموس لمدة ستة أشهر حظي بقبول الاتحاد الأوربي، وشاركت فيه خمس منظمات دولية، لمكافحة التنمر بجميع أشكاله.

فقامت منظمة " دعم تنمية الشباب" في رومانيا ومنظمة "IFALL" في السويد، ومنظمة " اسير معاً " في بلغاريا، وجمعية المستقبل الرقمي في إيطاليا، ومنظمة" الاخوة المغامرين" في استونيا، بالتعاون مع الشبكة الدولية للحقوق والتنمية في تنظيم ورش عمل تفاعلية مختلفة من أجل رفع مستوى الوعي، بين مجموعة مختارة من قادة الشباب الأوروبي بخصوص التنمر وآثاره، وسيحمل المشروع اسم " ماذا يمكنني فعله؟ أوقفوا التنمر واتخذوا الإجراءات اللازمة «(الإمارات، 2021).

الفرع الرابع: مسؤولية الاسرة لوقاية أبنائها من الجريمة القاتلة:

تقع على الاسرة في الدرجة الأولى مسؤولية في مواجهة التنمر الإلكتروني، التي قد يتعرض له أبنائهم وهذا يكون من خلال متابعتهم ومراقبة المواقع الإلكترونية التي يتصفحها الأولاد والمحتويات التي يتعرضون لها، وماهية المادة التي تقدمها تلك المواقع، مع تعزيز الحوار والثقة والاحترام مع الأبناء، وذلك من أجل تبليغ اسرتهم بكل المضايقات التي

تصلهم، مع ضرورة اتخاذ الإجراءات اللازمة لحمايتهم وتخليصهم من الابتزاز، كما يمكن وضع قوانين أسرية يمكن لها الحد من حدوث التنمر الإلكتروني، مصل عدم الحديث مع أشخاص مجهولين، عدم فتح أية رسالة من جهة مجهولة.

مع أهمية إبلاغ أحد الوالدين في حال حدوث حالات التنمر الالكتروني مهما كانت، وتحديد أوقات لاستخدام الأجهزة الالكترونية وبرامج التواصل الاجتماعي ولا يكون الأمر مفتوحاً على مصراعيه للأبناء، مع ضرورة إيجاد قناة للتواصل مستمرة مع إدارة المدرسة في هذا الشأن 33.

الفرع الخامس: مسؤولية وسائل الاعلام والمجتمع المدني:

للإعلام والمجتمعات المدنية دور كبير في التوعية، والتثقيف وإقامة المحاضرات والندوات، لتوعية الافراد من خطورة التنمر الالكتروني، كتعزيز الثقة بالنفس لدى الطفل، وتأمين برامج توعوية للحد من خطورة التنمر الالكتروني.

والعمل على نشر المادة التوعوية من التنمر الإلكتروني على مختلف وسائل الأجهزة، المرئية منها والمسموعة وكذلك المقروءة، ولا يمنع من وضع مقررات دراسية في المناهج للأطفال حول أضرار التنمر الالكتروني والتعريف به.

كما إن وسائل الاعلام تعد من الوسائل الفعالة والمؤثرة للتحذير من التنمر، للتخفيف منه سعياً الى القضاء عليه، وخاصة إذا قامت بتلك الاعمال التوعوية والتثقيفية شخصيات محبوبة لدى الأطفال، أو المراهقين والشباب، فتستطيع بذلك التأثير عليهم وتحذيرهم من مخاطر التنمر الالكتروني، وما يسببه للآخرين من اضرار مادية أو معنوية وقد تكون قاتلة.

وكذلك الاجتماعات والندوات والمحاضرات التي تقوم بها تلك الفئات المثقفة والواعية في المجتمع المدني، من خلال نشر رسائل وصور تحذيرية توضح ضرر اتنمر الالكتروني، وعقوبة المتنمر جنائياً ومدنياً للحد منه.

خاتمة:

بعد أن استعرضنا في بحثنا دراسة كاملة للتنمر الإلكتروني، من حيث تعريفه والوقوف على الوسائل المستخدمة في أفعال التنمر الإلكتروني، والطرق والسبل التي تسعى إليها الجهود الدولية والإقليمية لمكافحة الجريمة الالكترونية ومنها جريمة التنمر، وفي نهاية بحثنا نصل إلى جملة من النتائج والتوصيات:

أولاً: النتائج:

- ✓ الانترنت وتقنية الاتصالات أحدث تسارعاً كبيراً أدى الى إحداث العديد من الجرائم التي تكون تارة بالإلكترونية، وتارة أخرى بالمعلوماتية.
- ✓ التنمر هو كل سلوك عدواني يحدث ضرراً بالآخرين، القصد منه الحصول على منفعة مادية أو معنوية.
- ✓ تعتبر جريمة التنمر الالكتروني من الجرائم الإلكترونية، المستحدثة والتي تسمى بالقاتلة.
- ✓ تعددت وتنوعت وسائل التنمر الإلكتروني، منها المكالمات الهاتفية، الصور، ومقاطع الفيديو، مع تعدد أنواعه.
- ✓ هناك العديد من الدول التي خلت تشريعاتها من قانون خاص بالجرائم الإلكترونية مثل مصر، مع وجود بعض التشريعات مثل ليبيا الذي أصدرت قانون خاص بالجرائم الإلكترونية يشوبه النقد والكثير من المثالب.

- ✓ يظهر خطورة التنمر الالكتروني في جسامة الأثر الذي يخلفه على الشخص المتنمر عليه، المجنى عليه، التي قد تصل إلى حد الانتحار.

ثانياً: التوصيات:

- ✓ نطالب مجلس النواب الليبي من خلال هذا المنبر العلمي، بضرورة سحب وإلغاء القانون الخاص بالجرائم الالكترونية الصادر في 6 سبتمبر 2021م.
- ✓ نأمل من الجهة التشريعية في ليبيا عند اصدار قانون خاص بالجرائم الالكترونية ضرورة مناقشته من قبل جهات الاختصاص، خاصة الجُلة من المثقفين والمحاميين والمنظمات الحقوقية ومنظمات المجتمع المدني، ليظهره في صورته الصحيحة التي يمكن تطبيقها على ارض الواقع.
- ✓ ضرورة أن يقوم أولياء الأمور، وإدارة المدرسة بالمراقبة المستمرة للأطفال والمراهقين، ومحاولة تنبيههم إلى سلوك التنمر العدواني والذي يعود عليهم وللآخرين بالضرر المباشر والغير مباشر.
- ✓ كما يقع على وسائل الاعلام ومنظمات المجتمع المدني المسؤولية في ضرورة توعية وتثقيف مختلف شرائح المجتمع، بالتنمر الإلكتروني، من خلال الدورات والمحاضرات المكثفة والداعية الى نبذ سلوك التنمر المسيء.
- ✓ تشجيع الأطفال والأحداث على ضرورة التكلم في حال وقوع تنمر من الغير، وتوجيههم الى السلوك الصحيح، في حال كونهم متنمرين.

قائمة المراجع:

1) ابن منظور. (1956). لسان العرب، بيروت : دار صادر

2) أبو العافية، فاتنة. ما هو التنمر الالكتروني، عبر الرابط الالكتروني: www.mawdoo3.com ، اخر زيارة للموقع، الأربعاء:2022/01/26م، الساعة 10:30 مساءاً.

3) الإمارات. (2021). بمرسوم قانون اتحادي رقم 34 في شأن مكافحة الشائعات والجرائم الالكترونية لدولة الامارات العربية المتحدة.

4) انظر الموقع الالكتروني www.http//classic.austlii.au/au/journals/UniSAStuLawRW/2015/5pdf آخر زيارة للموقع:2022/01/28م، الساعة الثامنة.

5) التنمر الإلكتروني، انتفاضة ضد الجريمة الرقمية بالدول العربية، على الموقع الالكتروني: www.almashhadalaraby.com/news آخر زيارة للموقع:2022/01/28م، الساعة العاشرة..

6) حاسي، مليكة، وشرارة، حياة. (2020). بحث بعنوان: التنمر الالكتروني، دراسة نظرية في الابعاد والممارسات ،جامعة الشهيد حمه الأخضر الوادي، مجلة الاعلام والمجتمع، المجلد 4، العدد 1، 67.

7) حبيب، أمل عبد المنعم محمد عمر. (د.ت.). فاعلية برنامج قائم على الاثراء النفسي في تحسين الكفاءة الاجتماعية وخفض سلوك التنمر المدرسي لدى المتنمرين ذوي صعوبات التعلم بالمرحلة الابتدائية، دراسة أجريت في كلية التربية، جامعة بنها، 1.

8) درويش، عمرو محمد محمد،والليثي، محمد أحمد حسن. (2017). بحث بعنوان: فاعلية بيئة تعلم معرفي /سلوكي قائمة على المفضلات الاجتماعية في تنمية استراتيجيات مواجهة التنمر الالكتروني لطلاب المرحلة الثانوية، مجلة العلوم التربوية، العدد الرابع، ج1، أكتوبر، 204.

9) سايحي، سليمة. (د.ت،). بحث بعنوان: التنمر المدرسي، مفهومه، أسبابه، طرق علاجه. مجلة التغيير الاجتماعي، جامعة بسكرة، الجزائر، العد 6، 88.

10) شطبي، فاطمة الزهراء. (د.ت.). بحث بعنوان: واقع التنمر في المدرسة الجزائرية، مرحلة التعليم المتوسط" دراسة ميدانية". مجلة دراسات نفسية، العدد 11، 74.

11) الشيخي، موسى محمد. ما هو التنمر الالكتروني، وسائلة وأساليب علاجه. متاح على الرابط التالي: www.net-educ.com، آخر تاريخ لزيارة الموقع:2022/01/27م، الساعة: الثامنة مساءاً.

12) الصبحين، على موسى، والقضاة، محمد فرحان. (2013). سلوك التنمر عند الأطفال والمراهقين، جامعة نايف العربية للعلوم الأمنية، الرياض، 14.

13) العراقي، المادة 19 /ثالثاً من قانون العقوبات، وينظر: يزيدي، فائق، خبير قانوني " القذف على الفيسبوك جريمة يعاقب عليها القانون " في 02/11/ 2015، انظر الموقع الالكتروني: www.pukmedia.com/AR Direje.aspx?jimara=57147 ، وينظر القاضي أياد محسن ضمد، القذف والسب عبر مواقع التواصل الاجتماعي الفيس بوك، مجلس القضاء الأعلى، 2016/06/30م، آخر زيارة للموقع، 2022/01/28م، الساعة 9:30 مساءاً، الموقع الالكتروني: www.hjc.iq/view.3371/

14) العراقي، قانون العقوبات، رقم 111 لسنة 1989.م.

15) عيناب لوك وآخرون، 2017م، تنمية المسؤولية الشخصية والاجتماعية ومواجهة ظاهرة التنمر، وزارة التربية والتعليم، وحدة تطوير مناخ الامن ومنع العنف، القدس، 14.

16) الفلاح، خلود، مقال بعنوان: العنف الالكتروني في ليبيا، كراهية ضد النساء، انظر الموقع الالكتروني: www.hunalibya.com/dammawashadda/gbv آخر زيارة للموقع:2022/01/28م، الساعة :10:30.

17) قاموس اللغة العربية المعاصر، الموقع الالكتروني: www:almaany.com، اخر زيارة للموقع، 2022/01/24، الساعة: التاسعة مساءاً.

18) مجيد، سحر فؤاد. (2019). الجرائم المستحدثة، دراسة معمقة ومقارنة في عدة جرائم، المركز العربي لنشر والتوزيع، القاهرة ،134.

19) مقراني، مباركة. (2018). التنمر الالكتروني وعلاقته بالقلق الاجتماعي، جامعة قاصدي مرباح ورقلة، 30.

20) المكانين، عبد الفتاح، وآخرون. (2018). تقرير عن: التنمر الالكتروني لدى عينة من الطلبة المضطربين سلوكياً وانفعالياً في مدينة الزرقاء، جامعة الهاشمية، الأردن،57

21) الموقع الالكتروني: https://ifex.org/ar/libya-cybercrime-law-threatens-to-restrict-free-expression ، آخر زيارة للموقع:2022/01/28م، الساعة: العاشرة والنصف

22) الموقع الالكتروني: www.almaany.com، المصدر السابق، اخر زيارة للموقع: 2022/01/24م، الساعة 9:30 مساءاً.

23) الموقع الالكتروني: www.new-educ.com آخر موعد لزيارة الموقع: 2022/01/30م، الساعة السابعة مساءاً.

24) الموقع الالكتروني:www.joacademy.com ، حول ما هو التنمر الالكتروني. اخر زيارة لموقع:2022/01/24م، الساعة: 10 مساءاً.

25) الموقع الرسمي للحكومة الأمريكية: www.stopbullying.gov/resources/laws . آخر زيارة للموقع:2022/01/28م، الساعة السابعة مساءاً.

26) النجار، سحر فؤاد مجيد. (2020). بحث بعنوان: جريمة التنمر الالكتروني دراسة في القانون الأمريكي والعراقي، المجلة الاكاديمية للبحث القانوني، المجلد 11، العدد4، 144.

27) النجار، سحر فؤاد مجيد، بحث بعنوان: جريمة التنمر الالكتروني دراسة في القانون الأمريكي والعراقي، المرجع السابق، ص152.

28) النجار، سحر فؤاد مجيد، بحث بعنوان: جريمة التنمر الالكتروني دراسة في القانون الأمريكي والعراقي، المرجع السابق،153.

29) الهاجري، إياس بن سمير. (2004). تاريخ الانترنت في المملكة العربية السعودية، 30.

إجراءات التحري الخاصة في الحد من الجرائم الإلكترونية في القانون الجزائري

د.يمينة زريكي/ جامعة سيدي بلعباس/الجزائر
Dr. Yamina Zeriki/ University of Sidi Bel Abbes/ Algeria

ملخص الدراسة:

نتيجة لانتشار وسائل التكنولوجية الحديثة واستخدامها في شتى الميادين، ظهرت سلوكيات وتصرفات ضارة عرفت في الفقه القانوني بالجريمة الإلكترونية، وبالتالي لا يمكن مواجهتها والتصدي لها بالقواعد التقليدية.

وعلى هذا الأساس حاول المشرع الجزائري تدارك هذا الفراغ القانوني من خلال توفير حماية موضوعية إلا أنها غير كافية وإنما يجب تعزيزها بقواعد إجرائية خاصة تضمن توفير حماية فعالة من الناحية العملية وهو ما تضمنه في قانون الإجراءات الجزائية رقم: 22/06؛ فقد خول للضبطية القضائية في مرحلة البحث والتحري إجراءات مستحدثة تساهم في الكشف عن مرتكبي الإجرام الإلكتروني.

الكلمات المفتاحية: الإجـــرام الإلكتروني، الضبطية القضائية، قـــانون الإجراءات الجزائية.

résumé:

En raison de la diffusion de la technologie moderne et de son utilisation dans divers domaines, des comportements préjudiciables et des comportements connus dans la jurisprudence sous le nom de cybercriminalité sont apparus et ne peuvent donc pas être confrontés et traités par les règles traditionnelles.

Sur cette base, le législateur algérien a tenté de combler ce vide juridique en assurant une protection objective, mais celle-ci n'est pas suffisante. Elle doit plutôt être renforcée par des règles procédurales particulières garantissant une protection effective dans la pratique, ce qui est inscrit dans le code de procédure pénale. n° 22/06 ; Au stade de la recherche et de l'enquête, la police judiciaire a été autorisée à mettre en place de nouvelles procédures contribuant à la détection des cybercriminels.

Mots clés : cybercriminalité - saisie judiciaire - droit de procédure pénale.

مقدمة:

تكمن طبيعة الجرائم المعلوماتية على أنّها ظاهرة مستحدثة، وكان لزاماً على المشرّع تماشياً مع تطوّرها استحداث نصوص قانونية تجرّم وتعاقب على الأفعال التي تدخل ضمن إطار الجريمة المعلوماتية، وكذا صنع قواعد قانونية إجرائية تسهّل عمل أجهزة البحث والتحرّي في الممارسة العملية؛ أي الاهتمام الدولي والوطني المبكّر لهاته الظاهرة.

لقد تفطّن المشرع الجزائري الثغرة القانونية التي كانت تسود قانون العقوبات من خلال تعديله بموجب القانون رقم: 15/04 باستحداث القسم السابع مكرر ضمن الفصل الثالث من الباب الثاني من الكتاب الثالث عنوانه "المساس بأنظمة المعالجة الآلية للمعطيات"، ويشمل المواد من (394 مكرر) إلى (394 مكرر7) **(15-04، 2004م)**، وكذلك تقررت عقوبات للاعتداء على أنظمة المعلومات في قانون حماية

حقوق المؤلف رقم : 05/03 **(03-05، 2003)**، كما استوجبت في فحواها إقرار عقوبات للاعتداء على أنظمة المعلومات في إطار نفس القانونين (أمحمدي بوزينة، 2017م)، كذلك إضافة إلى الإجراءات المتبعة في التحري في مجال الجرائم المعلوماتية؛ تم استحدث إجراءات تحري خاصة بموجب المادة 65 مكرر 5 من قانون الإجراءات الجزائية الجزائري وما تلاها من مواد؛ وكرّس المشرع الجزائري من خلال القانون رقم: 04/09 قواعد تحري وحجز وتحقيق خاصة للوقاية من جرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها (09-04، 2009م).

وترجع أهمية الدراسة إلى الانتشار الواسع لهذا النوع من الجرائم سواء على المستوى الوطني أو الدولي، وما أصبح يشكّل تهديداً على الأمن المعلوماتي سواء للأفراد أو الدولة في حد ذاتها، أمّا أهداف البحث فتتلخص في معرفة خصوصية الإجراءات المتّبعة من الضبطية القضائية في القضاء على الجريمة الإلكترونية ومدى نجاعتها في توفير حماية فعالية من الناحية العملية.

ومن هنا الإشكالية المطروحة:

كيف ساهمت القواعد الإجرائية في الحد من الجرائم الإلكترونية؟ وما مدى فعاليتها؟

وللإجابة تم تقسيم هذه الدراسة إلى محورين:

- المحور الأول: المراقبة الإلكترونية كإجراء من إجراءات التحري
- المحور الثاني: تقنية التسرب في كشف الجرائم الإلكترونية.

المحور الأوّل: المراقبة الإلكترونية كإجراء من إجراءات التحرّي.

يعتبر نظام المراقبة الإلكترونية نظام تقني حديث ومبتكر (مديحة بن زكري بن علو، ونصيرة شيبان، 2019، ص. 387)، أحدث تطوّراً في السياسة الجنائية المعاصرة، واعتماد القضاء على الكثير من وسائل التكنولوجيا في مرحلة التحقيق القضائي من أجل الفصل في القضايا التي تحتاج وسائل متطورة للوصول إلى الحقيقة (حوبة ، 2020م، ص. 13).

فقد نظّم المشرّع الجزائري في قانون الإجراءات الجزائية الذي يسعى إلى الكشف عن حقيقة الجريمة ومرتكبيها بوصول المحققين ورجال القضاء إلى المعلومات المتعلّقة بالوقائع الجرمية وأدلّتها والأشخاص المنتمين إليها (روابح، 2020م، ص. 02)، وكذا قانون مكافحة الجرائم تكنولوجيا الإعلام والاتّصال إجراء مراقبة المراسلات والاتّصالات الإلكترونية عبر شبكات الإنترنت ووسائل الاتّصال عبر الأقمار الصناعية كأسلوب للتحرّي والتحقيق في بعض الجرائم الخطيرة، على سبيل المثال : جريمة الإرهاب؛ والجريمة المنظمة؛ والمخدّرات؛ والفساد؛ وتبييض الأموال، وكذا الجرائم المعلوماتية التي تتّخذ المنظومة المعلوماتية وشبكات التواصل وسيلة إجرامية أو هدفاً إجرامياً (روابح، 2020، ص. 01). في القانون رقم: 06-22 المؤرخ في: 2006/12/20م المعدّل والمتمّم لقانون الإجراءات الجزائية استخدام آليات

وأساليب جديدة للبحث والتحرّي عن هذه الجرائم (القانون رقم: 06-22، 2006م) وحددّ المشرع في تطبيقها جملة من الشروط والإجراءات القانونية التنظيمية (زوزو، 2019، ص. 403).

وتجدر الإشارة هنا إلى دراسة المراقبة الإلكترونية كإجراء من إجراءات التحرّي، من خلال استعراض تقنية التحرّي كآلية الكلاسيكية في كشف الجريمة المعلوماتية وهذا في المطلب الأوّل؛ والوسائل المناط استخدامها في أداء التحرّي وجمع الأدلّة في المطلب الثاني.

المطلب الأوّل: تقنية التحرّي كآلية الكلاسيكية في كشف الجريمة المعلوماتية

وضع المشرّع الجزائري أساليب أو وسائل التحرّي العامّة والخاصة في التعديلات من قانون الإجراءات الجزائية رقم: 15-02؛ فالأساليب العامّة هي الأساليب التقليدية للبحث والتحرّي من المعاينة؛ والضبط؛ والتفتيش؛ والمراقبة؛ والخبرة، وأمّا الأساليب الخاصة؛ فيمكن تصنيفها إلى ثلاث أشكال، هي: المراقبة؛ اعتراض المراسلات والأصوات والتقاط الصور (خرشي، وعمارة ، 2020م، ص 802) التسرّب (غزالي، 2020م، ص.974).

عند الشروع في تحقيق في جريمة ما؛ فإنّه يستلزم على المحقق تقيّد بقوانين وتشريعات ولوائح مفسّرة وقواعد فنّية تحقق الشرعية، وسهولة الوصول إلى الجاني أو المشتبه به، وللجرائم المعلوماتية طابعها الخاص المميّز لها (عثماني، 2018م، ص. 54).

فمراقبة الإلكترونية تعتبر من أهمّ مصادر التحرّي التي غالباً ما يستعان بها في البحث والتقصّي الحقائق عن الجرائم المرتكبة سواءاً كانت تقليدية أو مستحدثة كـ: "جرائم الإنترنت"؛ فهي همزة وصل بينها وبين أعمال رجال البحث والتحرّي، وتعتبر أسرع درب في كشف الجرائم المعلوماتية، لهذا تسمّى بـ : " المراقبة الإلكترونية ". فعملية المراقبة هي عمل أمني أساسي له نظام معلومات، يقوم به المراقب بمراقبة المراقب بالوسائل لتحقيق غرض محدّد وتحرير تقارير بالنتيجة (مرنيز ، 2016م، ص ص. 103 و106).

ويكمن عمل مأمور الضبط القضائي في إلزاميته بالقيام بالبحث عن الجرائم ومرتكبيها عبر شبكة الإنترنت، حسب ما يقرّه القانون، أو ما يثني عليه القانون بأساليب التحرّي الخاصة، والتي هي جملة من الإجراءات التي يقوم بها المتحرّي عبر شبكة الإنترنت بواسطة التغطية الإلكترونية الرقمية، وعلى أجهزة الحاسب الآلي، وذلك للحصول على بيانات ومعلومات تعريفية أو توضيحية عن الأشخاص أو الأماكن أو الأشياء حسب طبيعتها لضبط جرائم الإنترنت؛ فهي وسيلة لجمع المعلومات والأدلّة (مرنيز، 2016، ص. 103)

وعلى هذا الأساس، وفي مجال المكافحة الإجرائية للجريمة المعلوماتية، ينبغي التطرّق إلى الدور الذي تلعبه الشرطة القضائية كأداة رئيسية لصيانة أمن المجتمع وحمايته من الجرائم بصفةٍ عامّة والجريمة المعلوماتية بصفة خاصة، وهنا يترتّب إبراز الإجراءات الممكنة على النحو التالي:

أوّلاً: معاينة مسرح جريمة الماسّة بأنظمة المعالجة الآلية للمعطيات.

لمكافحة الجريمة الإلكترونية إجرائياً، يتأتّى دراسة تعريفية لمقصود " المعاينة "، والمقصود منها رؤية العين لمكان أو شخص أو شيء لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة ومعاينة مسرح الجرائم المعلوماتية (فلاح، وآيت عبد المالك ، 2019م، ص. 1697) ويتطلّب هذا الأمر انتقال مأمور الضبط القضائي إلى مكان ما لمباشرتها في إثبات حالته وحالة ما قد يوجد فيه من أشخاص أو أشياء تفيد في إظهار الحقيقة للكشف عن الجريمة محل الإجراء.

ثانياً: تفتيش وضبط النظم المعلوماتية

والغرض من التفتيش هو البحث أو ضبط الأدلة المادية للكشف عن حقيقة الجريمة؛ فكل ما يضبطّه مأمور الضبط القضائي جرّاء عملية التفتيش من أشياء متعلّقة بالجريمة (فلاح، وآيت عبد المالك، 2019، ص. 1697) هو الأثر المباشر للتفتيش؛ فالتفتيش والضبط يعدّ من إجراءات التحقيق في الجريمة المعلوماتية (أمحمدي بوزينة، 2017).

وهذا ما استهدفته المادة 04 من القانون رقم: 04/09 المؤرخ في: 5 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، التي قررت الفقرة الثانية منها أنه: " في حالة توافر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني" (المادة 04 فقرة 02 من قانون رقم: 09-04، المرجع السابق، ص. 06).

المطلب الثاني: الوسائل المناط استخدامها في آداء التحرّي وجمع الأدلة.

فالتحقيق في هذا المجال يستحّق فيها معرفة تامّة وإدراك لوسائل وقوع الجريمة، وفي الأخير فك شيفرة، والوصول المباشر إلى الجاني، وعلى هذه الأساس يتّم هذا الأمر باعتماد المحقّق على مجموعة من الإمكانيات من بينها:

أوّلاً: الوسائل المادية:

وهي الإمكانيات التي تستخدم في قاعدية نظم المعلومات، تستخدم في تنفيذ إجراءات وأساليب التحقيق والتحرّي والتي تثبت وقوع الجريمة وتساعد على تحديد شخصية مرتكبها ومن أهمّها:

- ✓ برامج المحادثة؛ والبريد الإلكتروني، عناوين IP.
- ✓ البروكسي: برنامج يعمل كوسيط بين الشبكة ومستخدميها، بحيث تضمن الشركات الكبرى المقدّمة لخدمة الاتّصال بالشبكات قدرها لإدارة الشبكة وضمان الأمن وتوفير خدمات الذاكرة الجاهزة.
- ✓ برامج التتبّع: حيث تقوم هذه البرامج بالتعرّف على محاولات الاختراق التي تتّم مع تقديم بيان شامل بها إلى المستخدم الذي تمّ اختراق جهازه، ويحتوي هذا البيان على اسم الحدث وتاريخ حدوثه وعنوان IP.

- ✓ نظام كشف الاختراق ويرمز له بـ: "IDS". وهو برنامج يتولّى مراقبة بعض العمليات التي يجري حدوثها على أجهزة الحاسبة الإلكترونية أو الشبكة مع تحليلها بحثاً عن أيّة إشارة قد تدّل على وجود مشكلة قد تهدّد أمن الحاسبة الإلكترونية أو الشبكة.
- ✓ أدوات تدقيق ومراجعة العمليات الحاسوبية، وأدوات فحص ومراقبة الشبكات (عثماني، 2018، ص. 55).

ثانياً: الوسائل الإجرائية.

وهي إجراءات بمجرّد استعمالها يتّم تنفيذ طرق التحقيق الثابتة والمحدّدة والمتغيّرة والغير محدّدة التي تثبت وقوع الجريمة وتحدّد شخصية مرتكبها ومن بينها:

- ✓ اقتفاء الأثر: ويتّم عن طريق تتبّع أثر الجهاز الذي تمّ استخدامه للقيام بعملية الاختراق.
- ✓ الاستعانة بالذكاء الاصطناعي، واطّلاع على عمليات النظام المعلوماتي وأسلوب حمايته، ومراقبة الاتّصالات الإلكترونية (عثماني، 2018، ص.55).
- ✓ تقنية برنامج كارنيوز: تقنية طوّرتها إدارة المعلومات التابعة لمكتب التحقيقات الفيدرالي F.B.I.
- ✓ تقنية تعقّب المواقع الإباحية أو ما يسمّى ببرنامج " نويد شرطة الإنترنت": ويقصد به برنامج يبحث عن الصور الجنسية المخلّة على أنظمة الكمبيوتر التي تعمل ببرامج تشغيل "ويندوز" هدفها تطهير الشبكة من المواقع الإباحية والجنسية (مرنيز ، 2016 ص. 109).

المحور الثاني: تقنية التسرّب في كشف الجرائم الإلكترونية.

يعرّف تقنية التسرّب في إطار جريمة المعلوماتية بأنّه " التسرّب الرقمي" الذي يتم عن طريقه الدخول والولوج (بن عودة ، ونوار ، 2020م، ص. 328) إلى الأنظمة المعلوماتية بصورة متخفّية مستخدماً أسماء وأوصاف مستعارة أو وهمية يندس عن طريقها في المجموعات لرصد الأشخاص المشتبه فيهم لارتكابهم أو شروعهم في ارتكاب جرائم والتقاط البيانات الخاصة بهم (حليم، 2021، ص. 233). ويقصد به أيضاً تسلّل معلوماتي يسمح بالدخول بطريقة احتيالية مخادعة في منتدى حوار أو على المواقع (روابح، 2020، ص. 13).

وعلى ضوء هذا المحور، سوف نتطرّق إلى دراسة تقنية التسرّب كآلية مستحدثة في استخلاص الجريمة المعلوماتية في ظلّ التشريع الجزائري وهذا في المطلب الأوّل؛ الإمكانيات الرامية إلى استخدام تقنية التسرّب في المطلب الثاني.

المطلب الأوّل: التسرّب كآلية مستحدثة في استخلاص الجريمة المعلوماتية.

يعتبر التسّرب إجراء نصّ عليه قانون الإجراءات الجزائية بموجب المواد 65 مكرر 11؛ 65 مكرر 12؛ 65 مكرر 13؛ 65 مكرر 14؛ 65 مكرر 15؛ 65 مكرر 16؛ 65 مكرر 17؛ 65 مكرر 18.

وتتمّ عملية التسرّب بقيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلّف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جنحة أو جناية وإيهامهم بأنّه فاعل معهم أو شريك، كما يسمح لعون أو ضابط الشرطة القضائية أن يستعمل لهذه العملية هوّية مستعارة ويرتكب عند الضرورة الأفعال الناصة في المادة 65 مكرر 14 بقولها : " يسمح القانون طبقاً لأحكام المادة 65 مكرر 14 لضابط أو لعون الشرطة القضائية أن يستعمل لهذا الغرض هوّية مستعارة، وأن يرتكب عند الضرورة الأعمال التالية : اقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتوجات أو وثائق أو معلومات متحّصل عليها من ارتكاب الجرائم أو المستعملة في ارتكابها، واستعمال أو وضع تحت تصرّف مرتكبي الجرائم الوسائل ذات الطابع القانوني أو المالي، وكذا وسائل النقل والتخزين أو الإيداع أو الحفظ أو الاتّصال" (حليم، 2021، ص. 233).

ويتّم اللجوء إلى هذه الكيفية عندما يتوجّب الأمر في التحرّي والتحقيق في الجرائم المنصوص عليها حصراً في نص المادة 65 مكرر 05 من قانون الإجراءات الجزائية على أنّه:" إذا اقتضت ضرورات التحرّي في الجريمة المتلبّس بها أو التحقيق الابتدائي في جرائم المخدّرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسّة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلّقة بالتشريع الخاص بالصرف، وكذا جرائم الفساد، يجوز لوكيل الجمهورية المختّص أن يأذن بما يأتي:

- ✓ اعتراض المراسلات (بوضياف ، 2018م، ص. 361) التي تتّم عن طريق وسائل الاتّصال السلكية واللاسلكية؛
- ✓ وضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط وتثبيت وبثّ وتسجيل الكلام المتفوّه به بصفةٍ خاصة أو سرّية من طرف شخص أو عدّة أشخاص في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدّة أشخاص يتواجدون في مكان خاص؛
- ✓ يسمح الإذن المسلم بغرض وضع الترتيبات التقنية بالدخول إلى المحلات السكنية أو غيرها ولو خارج المواعيد المحدّدة في المادة 47 من هذا القانون وبغير علم أو رضا الأشخاص الذين لهم حق على تلك الأماكن؛
- ✓ تنفّذ العمليات المأذون بها على هذا الأساس تحت المراقبة المباشرة لوكيل الجمهورية المختّص؛
- ✓ في حالة فتح تحقيق قضائي، تتّم العمليات المذكورة بناء على إذن من قاضي التحقيق (زوزو، 2019، ص. 412) وتحت مراقبته المباشرة " (القانون رقم: 06-22، 2007م، ص 30).

المطلب الثاني: الإمكانيات الرامية إلى استخدام تقنية التسرّب.

يعتبر التسرّب بمثابة إجراء جديد وحديث للبحث والتحرّي عن الجرائم الخطيرة، وقد استحدثه المشرّع الجزائري بعد تعديله لقانون الإجراءات الجزائية سنة 2006م و2007م، وهو اختصاص يمنحه

المشرّع لأعوان وضبّاط الشرطة القضائية بشأن جرائم محدّدة في القانون لتسهيل عملية البحث والتحرّي فيها (برابح، وبوبعاية، 2021، ص. 248).

وطرح المشرّع الجزائري هذه التقنية بجملة مهمّة من الشروط التي فرض مراعاتها والتقيّد بها لإضفاء صفة المشروعية على هذا الإجراء، ومنها ما يتعلّق بالجانب الشكلي والآخر بالجانب الموضوعي.

أوّلاً: الشروط الشكلية لإجراء تقنية التسرّب.

وتتجلّى الشروط الشكلية لإجراء تقنية التسرّب في تقرير محرّر من طرف ضابط الشرطة القضائية؛ وصدور إذن قضائي بمباشرة العملية.

تحرير تقرير مسبق من طرف ضباط الشرطة القضائية:

يقوم أعوان وضباط الشرطة القضائية قبل مباشرة في إجراء تقنية التسرّب بكتابة تقرير إلى وكيل الجمهورية المنصوص عليه في المادة 18 من قانون الإجراءات الجزائية المعدّل والمتمّم.

إذ تنص المادة 65 مكرر 13 على أنّه: " يحرّر ضابط الشرطة القضائية المكلّف بتنسيق عملية التسرّب تقريراً يتضمّن العناصر الضرورية لمعاينة الجرائم غير تلك التي تعرض للخطر أمن الضابط أو العون المتسرّب، وكذا الأشخاص المسخرين طبقاً للمادة 65 مكرر 14" (شيخ، 2018، ص ص. 04 و05).

أ. صدور إذن قضائي بمباشرة العملية:

تقتضي المادة 65 مكرر 11 من قانون الإجراءات الجزائية على أنّه : "عندما تقتضي ضرورة التحرّي أو التحقيق في إحدى الجرائم المذكورة في المادة 65 مكرر 05، يجوز لوكيل الجمهورية، أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرّب ضمن الشروط المبيّنة في المواد"، ويكون صدور الإذن من قبل وكيل الجمهورية أو قاضي التحقيق في مرحلة التحقيق القضائي(قادري، 2021م، ص. 649)؛ حسب استقراء المادة 65 مكرر 11 (برابح، وبوبعاية، 2021، ص. 247)، والبيانات الواجب توافرها في الإذن، وهذا ما تعكسه المادة 65 مكرر 15 بقولها : " يجب أن يكون عملية التسرّب مكتوباً، تطبيقاً للمادة 65 مكرر 11 ، مكتوباً ..." (شيخ ، 2018، ص ص. 06 و07).

ثانياً: الشروط الموضوعية لإجراء عملية التسرّب.

أضاف المشرّع على الشروط الشكلية، ضرورة توافر شروط الموضوعية عند ممارسة هذه التقنية، المتمثّلة في وجود دوافع اللّجوء إلى تقنية التسرّب؛ أي الإشارة إلى دواعي العملية، وسرية عملية التسرّب.

أ. دواعي اللجوء إلى تقنية التسرّب:

يتمّ التطرّق إلى تقنية إجرائية للتسرّب بمجرّد وقوع إحدى الجرائم المحدّدة في التقنين لتبرير العملية، وهذا ما أقرّته المادة 65 مكرر 11 في حكمها: "عندما تقتضي ضرورات التحرّي أو التحقيق ".

ب. سرية عملية التسرّب:

سرية عملية التسرّب يتوقف في السير الحسن لها، وهو اتّخاذ لعون أو ضابط الشرطة القضائية في استعمال هويّة مستعارة، وهذا وفقاً للمادة 65 مكرر 16 من قانون الإجراءات الجزائية، كما أضاف

بموجب المادة 65 مكرر 18 أنّه: " يجوز سماع ضابط الشرطة القضائية الذي تجري عملية التسرّب تحت مسؤوليته دون سواه، بوصفه شاهداً عن العملية " (شيخ، 2018، ص ص. 09 و10).

ج. **الجرائم الإلكترونية المقصودة بعملية التسرّب:**

وجرّمها المشرّع الجزائري بموجب المادة 65 مكرر 05 من القانون رقم: 06-22 المعدّل والمتمّم لقانون الإجراءات الجزائية، والتي حصرها في سبع (07) جرائم، هي (يامة، 2019م، ص. 151):

- ✓ جرائم الإرهاب (مقلاتي، ومشري، 2021م، ص. 505)؛
- ✓ جرائم المخدّرات؛
- ✓ جرائم تبييض الأموال؛
- ✓ جرائم الفساد؛
- ✓ جرائم الماسّة بأنظمة المعالجة الآلية للمعطيات؛
- ✓ جرائم المتعلّقة بالتشريع الخاص بالصرف (عنتر، 2017م، ص. 75)
- ✓ جرائم المنظمة العابرة للحدود الدولية (بوضياف، 2018، ص. 355) والوطنية (شيخ، 2018، ص ص. 11 و12).

ووفقاً لنص المادة 65 مكرر 15 فقرة الثالثة، لا يمكن أن تتجاوز مدّة عملية التسرّب أربعة (04) أشهر، ويمكن أن تتجدّد العملية حسب مقتضيات التحرّي والتحقيق ضمن الشروط الشكلية، بترخيص من القاضي (يامة، 2019، ص. 152).

كما لا نستغني عن آليات البحث والتحرّي عن الجرائم الإلكترونية في بلد الجزائر، التي تعتبر آلية مهمّة متمثّلة في الضبطية القضائية؛ أي صاحبة الاختصاص الأصيل في كل أشكال الجرائم بما فيها الجرائم الإلكترونية، ويندرج اختصاصها على مستوى أجهزة مكلّفة بالبحث والتحرّي عن الجرائم الإلكترونية، من بينها:

- **جهاز الشرطة {المديرية العامة للأمن الوطني}:** مخبر مركزي بمركز الشرطة بـ : "شاطوناف" بالجزائر العاصمة، وفروع جهوية بكل من : قسنطينة؛ ووهران؛ وبشار؛ وورقلة؛ وتمنراست مهمتهم التحقيق والكشف على جرائم الإنترنت، وتعميم هذا النشاط على كافة تراب الوطني.
- **جهاز الدرك الوطني:** يرتقي دور جهاز الدرك الوطني على مكافحة الجريمة الإلكترونية بواسطة المعهد الوطني للأدلّة الجنائية وعلم الإجرام الكائن مقرّه بـ: بوشاوي التابع لقيادة الدرك الوطني العامّة، قسم الإعلام والإلكترونيك الذي يختّص بالتحقيق والكشف عن الجرائم الإلكترونية (فلاح، وآيت عبد المالك، 2019، ص ص. 1695 و1696).

خاتمة:

إنّ سرعة الرهيبة للجريمة المعلوماتية أصبح العامل الفتّاك في كيان البشري في أمنه واستقرار موقعه الجغرافي؛ وبدا نوع من تأخّر المشرّع الجزائري في منافسة هاته العملية لوضع الحدّ لها؛ لأنّ وضعها

يزداد بتطور التكنولوجي وتزداد الجرائم المعلوماتية بكل أشكالها سواءاً كانت جريمة معلوماتية بالتهديد؛ والقتل؛ والقرصنة؛ وتحويل أموال أو اتّجار بأعضاء البشرية؛ أو اتّجار في السوق الإلكتروني بمختلف أصنافه.

أصبحت الجرائم الإلكترونية المرتكبة خفية أبشع من الجريمة العادية المرتكبة بمنظور واضح المرتكبة بأركانها (الركن الشرعي؛ والمعنوي؛ والمادي)، والجرائم الإلكترونية تسهّل وتمهّد السبيل في تنشيط وارتكاب عملية الإجرام والوصول إلى الهدف المبتغى منه والنيل منه بطريقة غامضة.

وعلى هذا المنبر؛ كان لزاماً على المشرّع الجزائري؛ حرصه على التقنين المستحدث والمعاصر تماشياً مع تبلور التكنولوجيا، مع طرح المشكل هذا أمام البساط التشريعي ومساهمته في توفير الإطار الإجرائي لمكافحة الجريمة الإلكترونية.

التوصيات:

ومن جملة التوصيات ما يلي:

- ✓ ضرورة تأطير إجراءات التحري الخاصة ووضع آليات لازمة لتطبيقها من الناحية العملية.
- ✓ إعطاء ضمانات كافية للمشتبه فيهم بغية احترام حرمة حياتهم الخاصة.
- ✓ ضرورة تكوين الضبطية القضائية من الناحية الالكترونية حتى تسهل مهمة الكشف عن الجرائم وذلك من خلال اعتماد التكوينات والتربصات المختلفة.
- ✓ يجب على المشرع الجزائري ضرورة الاستفادة من خبرات الدول الرائدة في هذا المجال والسباقة في تقنينه.

قائمة المراجع:

1) أمحمدي بوزينة، آمنة، (29 مارس 2017)، إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية _ دراسة تحليلية لأحكام قانون الإجراءات الجزائية وقانون الوقاية من جرائم الإعلام كلية الحقوق والعلوم السياسية جامعة حسيبة بن بوعلي-الشلف، مخبر القانون والأمن الإنساني، مركز الجيل البحث العلمي، كتاب أعمال ملتقى آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري المنعقد في الجزائري العاصمة يوم 29 مارس 2017، ص 57، على الساعة : 21 : 30 مساءاً، يوم : 13 أفريل 2022م، نقلاً عن الموقع الإلكتروني :
http://jilrc.com

2) الأمر رقم: 05/03 الصادر بتاريخ: 2003/07/19 المتعلق بحق المؤلف والحقوق المجاورة، 2003م.

3) برابح، السعيد، وبوبعاية، كمال، (2021م)، الأساليب المستحدثة ضمن إستراتيجية الكشف عن الجرائم المستحدثة في التشريع الجزائري _ التسرّب نموذجاً، دفاتر البحوث العلمية، المجلد: 09، العدد: 01، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، الجزائر.

4) بن علو، مديحة بن زكري، شيبان، ونصيرة، (12 جوان، 2019م)، تفعيل نظام الوضع تحت المراقبة الإلكترونية بالسوار الإلكتروني _ دراسة على ضوء القانون رقم: 01/18 المعدّل والمتمم، العدد: 12، جامعة عبد الحميد بن باديس، مستغانم.

5) بن عودة، نبيل، ونوار ، محمد، (2020م)، الصلاحيات الحديثة للضبطية القضائية للكشف وملاحقة مرتكبي الجرائم المتعلّقة بالتمييز وخطاب الكراهية، "التسرّب الإلكتروني نموذجاً"، مجلة الأكاديمية للبحوث في العلوم الاجتماعية، المجلد: 01، العدد: 02، جامعة عبد الحميد بن باديس، مستغانم، الجزائر.

6) بوضياف، إسمهان، (سبتمبر 2018م) الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد الحادي عشر، جامعة محمد بوضياف، المسيلة.

7) حوبة، عبد القادر، (2020/07/07م.)، المراقبة الإلكترونية في السياسة الجنائية للتشريع الجزائري: تعزيز للرقابة القضائية وإجراء بديل للعقوبة، مجلة الحقوق والعلوم الإنسانية، المجلد الثالث عشر، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر الوادي، الجزائر

8) خرشي، عثمان، وعمارة، فتيحة، (سبتمبر، 2020م)، الترصد الإلكتروني كآلية لمكافحة الجرائم المعلوماتية، مجلة الدراسات الحقوقية، المجلد:07، العدد: 03، كلية الحقوق والعلوم السياسية، جامعة سعيدة، الجزائر.

9) رامي، حليم، (2021م)، إجراءات استخلاص الدليل في الجرائم المعلوماتية، دفاتر البحوث العلمية، المجلد: 09، العدد: 01، كلية الحقوق والعلوم السياسية، جامعة البليدة 2، الجزائر.

10) روابح، فريد، (2020م)، ضمانات حرمة الحياة الخاصة أثناء إجراءات مراقبة الاتصالات الإلكترونية، مجلة الأبحاث القانونية والسياسية، المجلد: 02، العدد: 02، جامعة سطيف 2، الجزائر.

11) زوزو، زوليخة، (فيفري 2019م)، ضوابط المراقبة الإلكترونية في التشريع الجزائي، مجلة المفكر، العدد: 18، كلية الحقوق والعلوم السياسية، جامعة عباس لغرور، خنشلة، الجزائر.

12) شيخ ناجية، (ديسمبر 2018م) إجراء التسرّب في القانون الجزائري _ وسيلة لمكافحة الجرائم المستحدثة، مجلة معارف، العدد: 13، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو، الجزائر.

13) عثماني عزالدين، (جانفي، 2018م)، إجراءات التحقيق والتفتيش في الجرائم الماسّة بأنظمة الاتّصال والمعلوماتية، مجلة دائرة البحوث والدراسات القانونية والسياسية، مخبر المؤسسات الدستورية والنظم السياسية، العدد: الرابع، جامعة تبسة.

14) عنتر، أسماء، (2017م)، مكافحة الجرائم المستحدثة في التشريع الجزائري " التسرّب نموذجاً "، مجلة القانون العام الجزائري والمقارن، العدد :06، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم.

15) غزالي، لخضر، (2020م)، التحريات المستحدثة في جرائم التكنولوجيا الحديثة، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد: 05، العدد: 01، كلية الحقوق والعلوم السياسية، جامعة مولاي الطاهر، سعيدة.

16) فلاح، عبد القادر، وأيت عبد المالك، نادية، (2019م) التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد: 04، العدد: 02، جامعة الجيلالي بونعامة، خميس مليانة.

17) قادري، نسيمة، (2021)، عن أساليب التحقيق الخاصة المتعلّقة بالجريمة الإلكترونية ذات البعد الاقتصادي: أيّة فعالية؟ المجلّة الأكاديمية للبحث القانوني، المجلد: 12، العدد: 03، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميره، بجاية، الجزائر.

18) القانون رقم: 15/04 المؤرخ في: 27 رمضان 1425 هـ الموافق/ لـ: 10 نوفمبر 2004م المعدل والمتمم لقانون العقوبات رقم: 156/66 المؤرخ في: 18 صفر 1386 هـ/ الموافق لـ: 8 يوليو 1966م، الجريدة الرسمية، العدد 71، لسنة 2004م.

19) القانون رقم: 06/ 22 مؤرخ في: 29 ذي القعدة عام 1427هـ الموافق لـ: 20 ديسمبر سنة 2006م والمتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، العدد 84، سنة 2006م.

20) القانون رقم: 06-22 المؤرخ في: 20 ديسمبر، جريدة رسمية، العدد: 84، ص؛ 08، الفصل الرابع بعنوان: " في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، قانون الإجراءات الجزائية، 2007م.

21) قانون رقم: 09-04 مؤرخ في: 14 شعبان عام 1430هـ الموافق لـ: 5 غشت سنة 2009م، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتّصال ومكافحتها، جريدة رسمية، العدد: 47، 2009م.

22) مرنيز، فاطمة، (2016/09/22م)، المراقبة الإلكترونية كإجراء استدلالي في مواجهة الحق في الخصوصية، مجلة الحقيقة، العدد: 38، جامعة بشار.

23) مقلاتي، مونة، ومشري، راضية، (جوان، 2021)، الجريمة الإلكترونية: دلالة المفهوم وفعالية المعالجة القانونية، مجلة أبحاث قانونية وسياسية، المجلد: 06، العدد: 01، جامعة 08 ماي 1945م، قالمة.

24) يامة، إبراهيم، (جوان 2019م)، أساليب التحرّي الخاصة بالجريمة المنظمة في القانونين الجزائري والفرنسي، دفاتر السياسة والقانون، المجلد: 11، العدد الثاني، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية، أدرار، الجزائر.

دور المشرع الجزائري في مواجهة مخاطر الجرائم إلكترونية

The role of the Algerian legislator in facing the dangers of cybercrime

د. منير شمام/ جامعة مصطفي اسطمبولي، معسكر/الجزائر

Dr. Mounir chemmam / Mustafa Stambouli University, Mascara/-Algeria

ملخص الدراسة:

لقد شهد العالم تطورا تكنولوجي للفضاء الرقمي، الذي أدى إلى تسبيب تحولات عميقة على المستويات الاقتصادية والاجتماعية والثقافية، وهذا بفضل ما قدمته التكنولوجية الرقمية في التعاملات الإلكترونية، مما ولاد نتائج إيجابية ساهمت في ازدهار و تطور الدول التي استعملتها، إلا أنها شكلت عائق لكل المجتمعات بسبب انتشار الجرائم الإلكترونية، مما تشكل تحديا كبيرا للأمن الدولي، ولهذا اعتبر الفضاء الرقمي بمثابة الجوا المناسب لارتكاب الجرائم الالكتروني، وهو ما استدعى وجود حمايات القانونية تضمن هذه البيئة الرقمية التي تساهم في الأمن;الالكتروني.

الكلمات المفتاحية: الفضاء، جرائم، الكترونية، الرقمية، الأمن

Abstract:

The world has witnessed a technological development of the digital space, Which has caused profound transformations at the economic, social and cultural levels, thanks to what digital technology has provided in electronic transactions, which generated positive results that contributed to the prosperity and development of the countries that used it, but it formed an obstacle to all societies due to the spread of crimes electronic. Which poses a major challenge to international security and for this reason the digital space was considered as the appropriate atmosphere for the commission of electronic crimes, which necessitated the presence of legal protections that guarantee this digital environment that contributes to electronic security

Keywords: numérique, cybersécurité, crimes, electronic, protections

مقدمة:

لقد عرف المجتمع الدولي سنة 2019 ظاهرة انتشار فيروس كوفيد-19، الذي كبدا ومازال يكبد خسائر بشرية كل يوم، وذلك لسبب سرعة المرعب في انتشاره في العديد من الدول، دون أن يفرق ما بين الدول المتطور والدول نامي، حيث تخطت الإصابات مستوى الوباء العالمي ما دفع منظمة الصحة العالمية في شهر مارس 2020، عن إعلان فيروس كرونا المستجد المسبب لمرض كوفيد-19، والذي يتفشى في جميع انحاء العالم عن طريق العملة الوطنية والدولية، أي انتقال فيروس كورونا عبر النقود المعدنية والأوراق، التي أثبتت الدراسات أنها ناقل مهم للفيروس.

ولهذا جاءت وسائل الدفع الالكترونية كطريقة اضطرار بها الناس الى احترام برتوكول الصحي للتباعد الاجتماعي في مجال المعاملات الالكترونية، التي ساهمت في تطور الرقمي و المؤدي من خلالها إلى إنعاش العلاقات الاقتصادية والشخصية و التجارية و الإدارية، بما يعني تحول المجتمعات الكترونية من نمط الفضاء المغلق إلى نمط الفضاء المفتوح في كل المجالات وعلى كل المستويات (مهدي، 2021)، أي أصبح الفضاء الرقمي من أحد وسائل توفير الخدمات

والمستهلكات، التي تعتبر قيمة زائدة ودعامة أساسية، لأنشطة الحكومية والأفراد، وهذا في مجال التجارة الإلكترونية وغيرها.

ولهذا أصبحت مسألة الجرائم الالكترونية من التحديات الكبرى التي تواجهها كل الدول على الصعيد المحلي والعالمي، لاسيما مع ارتفاع حجم عمليات الدفع الإلكتروني كوسيلة الوفاء بالتعاقدات الإلكترونية أثناء ارتفاع مستوى الإصابات الافراد مما يجعلهم يخضعون للحجر الصحي، الذي يشكل خطرا على المواطن في حياته الشخصية والدول في سيادتها و اختراق أمنها الوطني، لدرجة أن العديد من الباحثين اعتبر الفضاء الإلكتروني، بمثابة المجال الخامس في الحروب بعد البر و البحر والجو والفضاء /political-encyclopedia-org/dictioary)الامن السيبراني(site vue 2022 ،، باعتبار أن التطور التكنولوجي والرقمي له تأثير على المستويات بشكل أو بأخر على أمن و استقرار الشعوب، أي أصبحت تداعيات هذه الثورة التكنولوجية تمس حرية المواطنين (مهدي، 2021) وعدم استقرار النظام العام داخلي الدولة.

الأمر الذي دفع الأمم المتحدة إلى انشاء أحد أفرقتها العاملة لهذه المسألة وتسابقت الدول في حماية فضائها الرقمي من تعديات الأخرين لما في ذلك من خطورة قصوى قد تؤدي الانهيار الاقتصادي، كما حدث في عدد من الدول بسبب ظاهرة القرصنة المنظمة على بنيتها الالكترونية (أبو حسين، 2021).

والجدير بالذكر، أن الدول الإفريقية دخلت الفضاء الالكتروني إلا حديثا، وذلك بتبني نهج التعاملات المصرفية الالكترونية، دون الأخذ بعين الاعتبار الانعكاسات الاستراتيجية على أمنها الداخلي، وتعتبر الجزائر من بين الدول التي دخلت مصاف الوفاء للالتزام عن طريق الدفع الإلكتروني وفتح نافذة الفضاء الرقمي (بوغرارة، 2018)، مما أبرز للمشرع الجزائري انعكاسات جراء التغيرات المتسارعة في التكنولوجيا تؤدي إلى خلق تهديدات الرقمية، لذا لابد من ضرورة لسن قوانين تضمن أمن المعلومات و محاربة الاستخدام غير الشرعي للشبكة العنكبوتية (عطية، د.ت.ن)من هذه المخاطر التي تمس الفضاء الرقمي، وأهم هذه التشريعات القانون 09-04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال و مكافحتها و غيرها من القوانين التي تساهم للحد من انتشار هذه الجرائم الالكترونية، الإشكالية ما هو الإطار القانوني الذي وضعه المشرع الجزائري لتحقيق الأمن من الجرائم الالكترونية ، سنحاول في هذه المداخلة ابراز اهم القوانين التي وضعها المشرع الجزائري لمواجهة والوقاية من جرائم الالكترونية، ولهذا انتهجت لوضع الخطة التالية:

مقدمة

المبحث الأول مفهوم الجرائم الإلكترونية

المطلب الأول المفاهيم المرتبطة بالجريمة الالكترونية

المطلب الثاني نموذج الجرائم الالكترونية المرتكب على المستوى الدولي

المطلب الثالث العقوبة الموقعة على الجرائم الالكترونية في ضل قانون العقوبات الجزائري

البحث الثاني إطار القانوني لتوفير الامن ضد الجرائم الالكترونية

المطلب الأول صور المختلفة للجرائم الالكترونية

المطلب الثاني سن قوانين مكافحة الجرائم الكترونية

المطلب الثالث الأجهزة الوطنية لتوفير الامن ضد الجرائم الالكترونية

خاتمة

المبحث الأول-مفهوم الجرائم الإلكترونية:

لقد اختلفت الآراء الفقهية على تعريف موحد للجرائم الالكترونية، فمنهم من ينظر إلى موضوع الجريمة، بأنه كل سلوك إيجابي أو سلبي يقع باستخدام تقنية المعلومات على مصلحة مشروعة بالاعتداء، في حين ينظر أخرون إلى الوسيلة المستعملة لارتكاب الجريمة على أساس أن كل فعل إجرامي يستخدم الكمبيوتر كأداة رئيسية في تحقيق الجريمة الالكترونية (القاضي، 2011)، (مكتب الامم المتحدة 2013المعني بالمخدرات و الجريمة دراسة شاملة عن الجريمة السيبرانية، 2013)

وكان هنا تعريف المضيقة ذهب البعض إلى القول بأن هذه الجرائم هي كل عمل أو امتناع عن عمل يأتيه الإنسان إضرار بمكونات الحاسب المادية والمعنوية وشبكات الاتصال الخاصة به، باعتبارها من المصالح والقيم المتطورة التي يحميها القانون (الشوابكة، 2011)

والجدير بالذكر أنه يصعب تحديد معنى جرائم الالكترونية ليست مهمة سهلة، فهي بنية واسعة للعديد من أنواع الجرائم الممكنة على تقنيات الاتصالات، والمعلومات، وتحتضن السلوكيات الإجرامية الضارة التي تحدث عبر الفضاء الرقمي، والتي تستهدف أعداد كبيرة من الأفراد أو الشركات عبر الحدود الدولية، والسبب الذي يؤدي ارتفاع نسبة انتشارها، هو راجع لصعوبة تحديد هوية الجناة والذين يعتقدون بأن إنفاد القانون لا يعمل في العالم الالكتروني (بارة، 2017)، ومن خلال ذلك يمكن أن ترتكب الجرائم الرقمية لصالح المنفعة المالية أو الإيديولوجية، عن طريق تشكيلة المنظمات الإجرامية أو الجماعات الإرهابية

المطلب الأول-المفاهيم المرتبطة بالجريمة الإلكترونية:

إن جريمة الالكترونية لها مفاهيم ذات صلة وهي كما يلي:

الفرع الأول-الفضاء الالكتروني:

يعتبر الفضاء الالكتروني مجال افتراضي من صنع الانسان يعتمد على نظم الكمبيوتر وشباك الانترنيت وكم هائل من البيانات و المعلومات والأجهزة، فأصبح الفضاء الالكتروني من أحد الوسائل الأساسية التي تؤثر في النظام الدولي على مختلف مجالات الحياة سواء الاقتصادية والعسكرية والسياسية، وهذا راجع فسهولة الاستخدام و قلة

التكلفة زادا من قيمته (زروقة، 2019)، كما عرفته الوكالة الفرنسية لأمن أنظمة الإعلام (kempf, cyberstratégie à la français, 2012) (ANSSI) على أنه "فضاء التواصل المشكل من خلال الربط البيئي العالمي لمعدات المعالجة الالية للمعطيات الرقمية(kempf, /introduction à la cyberstratégie/, 2012))-[1]، ويجدر القول أن هذا التعريف جاء على الجانب التقني للفضاء الالكتروني، حيث يولي الاعتبار إلى التجهيزات ، وأن البعد القضائي ناتج عن الربط والتواصل البيئي العالمي . (بوغرارة، 2018)، كما يمكن الاعتماد على تعريف الاتحاد الدولي للاتصالات الذي يصف الفضاء الالكتروني، بأنه المجال المادي وغير المادي الذي يتكون وينتج عن عناصر هي أجهزة الكمبيوتر، الشبكات، البرمجيات، حوسبة المعلومات، المحتوى، معطيات النقل والتحكم، ومستخدمو كل هذه العناصر، ومن خلاله ضهور العديد من المفاهيم المرتبطة بالفضاء الالكتروني(desforges, 2014)

الفرع الثاني-الأمن الالكتروني:

أن أصول نشأت المصطلح الأمن الالكتروني كان بعد ظهور الهجمات الرقمية التي تستغل نقطة ضعف معينة تمكن المهاجم من التلاعب بالنظام /political-encyclopedia-org/dictioary)الامن السيبراني (site vue 2022, داخلي الفضاء الإلكتروني، ومن هذا المنطلق يعتبر الامن الالكتروني مجموعة من الوسائل التقنية والإدارية، التي يتم استخدامها لمنع الدخول غير المصرح به على شبكات الكمبيوتر وسوء الاستغلال واستعادة المعلومات الإلكترونية التي تحتويها بهدف ضمان واستمرارية عمل نظم المعلومات، وتأمين حماية وسرية وخصوصية البيانات الخاصة بالأفراد على الفضاء الالكتروني(okaz.com.sa/article/1585529 , site vue 13/01/2022) ، ولهذا يعتبر مفهوم الأمن الالكتروني من أكثر المفاهيم المثيرة للاهتمام والدراسة، مما نتج عدت تعريفات المقدمة له ومن بينها الفقه قريتشارد كمرر Richard A.Kemmerer بقوله أن الأمن السيبرانية عبارة عن وسائل دفاعية من شأنها كشف واحباط المحاولات التي يقوم بها القراصنة (Kemmerer, 2003)(انظر (عطية، د.ت.ن) ، بينما عرفه الفقه إدوارد أمورسو Edward Amorso على أنه وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشباك، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات و وقفها...إلخ)(Amoroso, 2007) .

المطلب الثاني-أنواع الجرائم الإلكترونية المرتكب على المستوى الدولي:

تتنوع الجريمة الالكترونية التي ترتكب عبر الشبكة الانترنت، على سبيل المثال

الفرع الأول: المنظمات الإجرامية

تقوم هذه المنظمات الإجرامية بعمليات القرصنة الالكترونية، وذلك لاستهداف مواقع مالية، أي القيام بالسرقة المعلومات واختراق الحسابات البنكية وتحويل الأموال، كما يوجد سوق سوداء على الفضاء الالكتروني المظلمDARKWEB لتجارة المخدرات والأسلحة والبشر /political-encyclopedia-org/dictioary)الامن السيبراني , site vue 2022) (كركوري، 2020) .

الفرع الثاني: الجماعات الإرهابية

ترتكب الجماعات الإرهابية جرائم لأسباب إيديولوجية، تعد من أبرز الفواعل الدولية الخطيرة خاصة بعد أحداث 11 سبتمبر 2001 بأمريكا، حيث تستغل الفضاء الالكتروني في عمليات التجنيد والتعبئة والدعاية وجمع الأموال والمتطوعين، كما تحاول جمع المعلومات حول الأهداف العسكرية أو المدنية، وكيفية التعامل مع الأسلحة وتدريب المجندين الجدد عن بعد (political-encyclopedia-org/dictioary/)الامن السيبراني(site vue 2022 ,) (بن مرزوق و حرشاوي، 2017)

الفرع الثالث-جرائم التجسس الإلكتروني:

اعتمد هذا النوع من الجرائم على تقنيات عالية، حيث لم يعد التجسس (زروقة، 2019)على ما يتعلق بالمعلومات(Clarke & Knake, 2010) العسكرية (shakarian, shakarian, & Ruef, 2013) أو السياسية بل تعداه إلى المجال الاقتصادي والتجاري من خلال التجسس ما بين الشركات والمصانع لصالح الحصول على اسرار الإنتاج ....الخ، ومن الأساليب التجسس تتم عن طريق إخفاء برنامج داخل المعلومات موجودة في رسالة الكترونية أو إشهار بعد أن يتم فتحها من طرف الضحية يمكن للمجرم الإلكتروني التسرب للحصول على معلومات الموجودة داخل جهاز الحاسب الألي (شرا بشة، د.ت.ن)

المطلب الثالث: العقوبة الموقعة على الجرائم الالكترونية في ضل قانون العقوبات الجزائري

ركز استراتيجية المشرع الجزائري في مواجهة لظاهرة الإجرام المعلوماتي على سن في القسم السابع مكرر من الفصل الثالث الخاص بجرائم الجنايات والجنح ضد الأموال من قانون العقوبات رقم 04-15 تحت عنوان المساس بأنظمة المعالجة الالية للمعطيات (زعيطي، 2019)، باعتبارها قاعدة موضوعية مجرمة للأفعال الماسة بنظم المعالجة الالية للمعطيات وما يقابلها من عقوبة، وقد تم نص على الاحكام المنظمة للركن الشرعي للجريمة في النصوص التشريعية، بأن الجريمة الالكترونية ترتكب في نظام معلوماتي أو يسهل ارتكابها عليه، وهو الامر الذي من شأنه أن يوسع دائرة التجريم على الأفعال المجرمة والمكونة لقيام الجريمة الرقمية في مضمون الاحكام العقابية والمنصوص عليها (كركوري، 2020)كما يلي:

المادة 394 مكرر يعاقب بالحبس من 3 أشهر الى سنة وبغرامة من خمسين ألف إلى مائة ألف دينار من يدخل أو يبقى عن طريق الغش في كل أو جزء من المنظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، والمادة 394 مكرر1 من نفس القانون تنص على أنه تضاعف العقوبة إذا ترتب حذف أو تغيير لمعطيات المنظمة وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشغال المنظومة تكون العقوبة من 6 أشهر الى سنتين وغرامة من خمسين ألف الى مائة وخمسون ألف دينار.

المادة 394 مكرر 2 من نفس القانون يعاقب بالحبس من شهرين الى 3 سنوات وبغرامة من 1000.000 دج إلى 5000.000 دج كل من يقوم عمدا وعن طريق الغش بما يلي 1-تصميم أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو

معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن ترتكب بها الجرائم المنصوص عليها في هذا القسم.2-حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات للتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم

المادة 394 مكرر 3 من نفس القانون تضاعف العقوبة المنصوص عليها في هذا القسم إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام دون الاخلال بتطبيق عقوبات أشد (www.wipo.int/edocs/lexdocs/law/ar/dz/dz027ar.pdf, site vue 24/02/2022)

المادة 394 مكرر 4 يعاقب الشخص المعنوي الذي ارتكب احدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس مرات الحد الأقصى المقرر للشخص الطبيعي.

المادة 394 مكرر5 كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسد أو عدة أفعال مادية يعاقب بالعقوبات المقررة للجريمة ذاتها.

المادة 394 مكرر6 مع الاحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم على إغلاق المحل أو مكان استغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها.

المادة 394 مكرر 7 يعاقب على المشروع في ارتكاب الجنحة المنصوص عليها في هذا القسم بالعقوبات المقررة على الجنحة ذاتها قانون العقوبات الجزائري اخر تعديل ,(www.wipo.int/edocs/lexdocs/law/ar/dz/dz027ar.pdf (site vue 24/02/2022)

المبحث الثاني: الإطار القانوني لتوفير الأمن ضد الجرائم الإلكترونية

لقد وضع المشرع الجزائري إطار القانوني يوفر الأمن من مختلف صور الجرائم الالكترونية كما وضع أجهزة أمنية لمواجهة أي تهديد يمس الفضاء الالكتروني وهذا كما يلي:

المطلب الأول: الصور المختلفة للجرائم الإلكترونية

تكمن التهديدات الإلكترونية أساسا على الهجومات من أجل استغلال الحاسبات والمعلومات لهدف تخريب وتدمير البنية المعلوماتية للضحايا، بل أكثر من ذلك تعطيل منشأة العسكرية، عن طريق اختراق أنظمة المعلومات لصالح التجسس أو تعطيل أجهزة الدفاع، وفق خطة ممنهجة (عطية، د.ت.ن)،تهدد أمن المجتمع وأمن الاقتصاد الوطني والجانب الأمني والعسكري للدول، أي تمس كل من الجانب المعنوي والمادي وعلى جميع الأصعدة (الشهري، 2010)، (عطية، د.ت.ن)، وبالتالي يمكن ابراز أخطر التهديدات الالكترونية، التي يوجهها الأفراد والدول (مختار، 2015)

الفرع الأول: إتلاف المعلومات أو تعديلها:

وهي عملية تقنية تستهدف الوصول إلى معلومات الضحية عبر الفضاء الإلكتروني، وذلك بالتلاعب على المعلومات أو البيانات الأساسية، دون أن يكتشف الضحية لهذا الاختراق، فالبيانات تبقى موجودة لكنها مضللة قد تحدث نتائج سلبية، إذا كانت تمس خطط عسكرية أو مواعيد أو خرائط سرية (زروقة، 2019)

الفرع الثاني: التجسس على الشبكات:

ويقصد به اختراق غير المسموح به والتجسس على شبكات الضحية، دون تدمير أو تغيير في البيانات والهدف من وراء هذه العملية لصالح الحصول على معلومات الاستراتيجية والحساسة، قد تمس أسرار عسكرية أو الحربية أو السياسية أو اقتصادية أو المالية، مما تحدث نتائج كارثية تضعف الخصم ضحية التسرب الإلكتروني (زروقة، 2019)

الفرع الثالث: تدمير المعلومات

وهي عملية تستهدف إلى مسح وتدمير المعلومات والبيانات الموجودة على الشبكة، التي تهدد لسلامة المحتوى عن طريق الحذف أو التدمير من قبل مجرمين لهم تقنية القرصنة توفر لهم إمكانية اختراق جدار الحماية PARE-FEU الموجود في كل جهاز الكمبيوتر (زروقة، 2019) (https://fr.m-wikipedia.org, site vue 11/01/2022)

المطلب الثاني: سن القوانين لمكافحة الجرائم الإلكترونية

لقد وضع المشرع الجزائري قوانين لمكافحة التهديدات الالكترونية، والقوانين اللاحقة لها، وهذا لتوفير الأمن على الفضاء الإلكتروني وهي كما يلي:

الفرع الأول: تدبير لمكافحة الجرائم الإلكترونية على ضوء القانون 09-04

قام المشرع الجزائري بوضع مجموعة تدابير الوقائية وجرائية عبر القانون رقم 09-04 المتعلق بالوقاية من تكنولوجيات الإعلام والاتصال ومكافحتها وهي كما يلي:

أ-التدابير المراقبة الفضاء الالكتروني: وهذا في حالات محددة حصرها في المادة 4 من القانون 09-04 سابق الذكر أعلاه، ومن خلاله يمكن بموجب إذن مكتوب من السلطة القضائية المختصة، للوقاية من الأفعال الإرهابية أو التخريبية أو الجرائم الماسة بأمن الدولة، أو في حالة حصول على معلومات ترشد السلطة على احتمال وقوع اعتداء على المنظومة المعلوماتية تهدد النظام العام أو الدفاع الوطني...إلخ (مهدي، 2021).

ب-اللجوء إلى مقدم الخدمات للوقاية من الجرائم الالكترونية: وهو المكلف بتقديم المساعدة للسلطات أثناء التحري وتحقيق القضائي، من أجل جمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات تحت تصرف السلطة المختصة، طبقا للمادة 11 من القانون 09-04 سابق الذكر أعلاه، كما فرد المشرع في المادة 12 من نفس القانون على إجبارها التدخل الفوري لسحب المحتويات المخالفة للنظام العام أو حضر الدخول إليها (مهدي، 2021).

ج-'جراء التفتيش وحجز المنظومة المعلوماتية: لقد سمح المشرع الجزائري طبقا لأحكام المادتين 3 و 7 من القانون 09-04 المذكور أعلاه، إمكانية اللجوء إلى التفتيش بعد الحصول على إذن السلطة المختصة، وذلك عن بعد بسرعة لكل منظومة معلوماتية مشتبه بها، كما يمكن التفتيش أيضا عن بعد في منظومة تخزين معلوماتية، أنها تحتوي على معلومات تمس النظام العام، ويمكن أثناء القيام بعملية التفتيش من طرف السلطة القضائية، أن تسخر أي شخص له دراية بعمل المنظومة المعلوماتية المشتبه بها (مهدي، 2021).

الفرع الثاني: القوانين اللاحقة المدعمة للقانون 09-04 للحد من التهديد الإلكترونية

لقد سن المشرع الجزائري عدة قوانين اللاحقة لتدعيم القانون 09-04 سابق الذكر وهي كما يلي:

أ-القانون 18-04 المتعلق بالقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية: حيث استحدث المشرع هذا القانون رقم 18-04 سابق الذكر أعلاه، وذلك للتصدي للجرائم المتعلقة بالفضاء الالكتروني، وهذا بإعطاء الاستقلالية الوظيفية لسلطة ضبط البريد و الاتصالات الإلكترونية، وذلك بمنحها صلاحية تنظيم واستغلال إداري طبقا لأحكام المادة 11 من القانون 18-04 سابق الذكر (سعيود ، 2020)، كما استحدث مهام سلطة ضبط من أجل السهر على احترام متعاملي البريد والاتصالات الإلكترونية للأحكام القانونية المنصوص عليه في المادة 13 من القانون 18-04 سابق الذكر (القانون 18-04،الذي يحدد القواعد المتعلقة بالبريد و الاتصالات الالكترونية ج،ر عدد13/27 مايو 2018/ص10، 2018)، وذلك بتجريم انتهاك سرية الرسالات البريد الإلكترونية أو إفشاء مضمونها أو نشرها، وتجريم محاولة فتح أو تخريب أو تحويل البريد أو المساعدة في ارتكاب هذه الجريمة، ووضعت مجموعة من العقوبات ضمن المواد من 164 إلى 188 من هذا القانون (مهدي، 2021)

ب-القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي لقد ساهم التفتح نحو تداول البيانات والمعطيات الخاصة في مجال الفضاء الالكترونية على المتاجرة بالبيانات الشخصية للأفراد واستغلالها، من أجل التجارة والإعلام وخاصة لأغراض اقتصادية أو السياسية، مما ينشأ سلبيات تمس حياة الأفراد وهذا الباعث الذي ألزام المشرع الجزائري على فرض إجراءات قانونية صارمة تحمي الأشخاص الطبيعيين في مجال المعطيات ذات الطابع خاص من خلال إصدار القانون 18-07 سابق الذكر، والذي يهدف إلى حماية الأفراد إزاء استعمال تقنيات المعلومات والاتصال، بحيث نص على إنشاء السلطة الوطنية لحماية المعطيات الشخصية، وأيضا جزاء لكل من يخالف قواعد هذا القانون، والسبب من ذلك هو تشجيع المعاملات الإلكترونية و زرع الثقة في النفس الأفراد (بن عبيد ، 2021)

المطلب الثالث-الأجهزة الوطنية لتوفير الأمن ضد الجرائم الإلكترونية:

لقد وضع المشرع الجزائري إطار القانوني ينظم هياكل مخصصة لمواجهة التهديدات الالكترونية، ومدى فعاليتها، لأدائها مهام توفير الأمن على الفضاء الرقمي، ومتمثلة أساسا كما يلي:

الفرع الأول- مركز الوقاية من جرائم الإعلام الآلي للدرك الوطني:

لقد عملت الجزائر جهدا كبيرا الاستفادة من خبرة البلدان الأخرى في تأمين المنظومة المعلوماتية عن طريق هيكلة جهاز للوقاية الأمنية و المكافحة التهديد الالكتروني (علوي، 2008-2007)، وهذا من خلال إنشاء مركز مقره في بئر مراد رايس لسنة 2008، باعتباره الجهاز الوحيد المختص بهذا الصدد في الجزائر، لصالح تأمين منظومة المعلومات لخدمة الأمن الالكتروني، وذلك لاعتباره بمثابة مركز توثيق، ويقوم بتحليل المعطيات والبيانات للجرائم المعلوماتية المرتكبة أو لمحاولة كشف هوية المجرمين سواء كانوا فاعلين منفردين أو عصابات منظمة، وهذا من أجل حماية الأنظمة المعلوماتية والحفاظ عليها من أي قرصنة تمس بالمؤسسات الرسمية (رابحي، 2010-2009)و البنكية (عطية، د.ت.ن)، والجذير بالذكر أن المركز استطاع معالجة أزيد من 100 جريمة إلكترونية سنة 2014، وما يقوق 500 قضية رقمية خلال 2015، وهذا بفضل التركيبة البشرية المؤهلة التي اكتسبها الجهاز من التكوين المستمر والملتقيات الوطنية والدولية، وتبادل الخبرات مع الدول (بارة، 2017)المتحالفة (بوغرارة، 2018)

الفرع الثاني: المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني:

لقد تم إنشاءه بموجب المرسوم الرئاسي 133/04، المؤرخ في 2004/06/26، ودخل حيز الخدمة من جانفي 2009، حيث يتضمن هذا الجهاز 11 دائرة متخصصة في عدة مجالات متباينة وتقدم جميع المساعدات التقنية، كما تقوم دائرة الإعلام الألي و الإلكتروني المكلفة بمعالجة وتحليل وتقديم كل الدليل رقمي يساعد العدالة مع توفير المساعدة للمحققين (فصيلة، 2017)، كما يحتوي هذا المعهد على المصالح المختصة أهمها مصلحة البصمات ، مصلحة البيئية، أما في ما يخص مجال الأمن الإلكتروني هناك مصلحة الإعلام الألي على مستوى هذه المصلحة يتم رصد ومراقبة وتتبع عمليات الاختراق والقرصنة المعلوماتية وكذا الاكتشاف المعلومات المسروقة وتفكيك البرامج المعلوماتية (غزال، مشاريع الحكومة الالكترونية من الاستراتجية الى التطليق مشروع الجزائر الحكومة الالكترونية، 2014)،انظر (عطية، د.ت.ن)مخالفة للنظام العام.

الفرع الثالث-المصلحة المركزية لمكافحة الجريمة المعلوماتية للأمن الوطني:

قامت مصالح الأمن بإنشاء المصلحة المركزية للجريمة الإلكترونية استجابة لمطالب الأمن الإلكتروني ومكافحة التهديدات الأمنية الناجمة عن الجرائم الإلكترونية، الذي أنشيء سنة 2011، وأضيف للهيكل التنظيمي في سنة 2015، (حملاوي ، 2015/09/16)، (بوغرارة، 2018)وذلك بهدف حماية الأمن المعلوماتية ومحاربة التهديدات الأمنية التي تمس الفضاء الإلكتروني.

خاتمة:

إن الجرائم الالكترونية باعتبارها من الجرائم المعلوماتية المستحدث في العصر الحالي، وذلك راجع للتقدم التكنولوجي خصوصا بعد ظهور شبكة المعلومات الدولية أي انترنت، مما ساهم على انتشار وتنوع هذا السلوك الاجرامي والذي أصبح يشكل التهديد إلكتروني خطرا يمس مختلف المجالات الاقتصادية والاجتماعية والثقافية، مما جعل ظاهرة الإجرام الإلكتروني متطور وسريع الانتشار مع صعوبة اكتشاف هوية المرتكب جريمة الإلكترونية وعدم معاقبته لغياب

اثبات مادي للجريمة، ولهذا ساهم المشرع الجزائر لوضع اطار قانوني يمكن من وقاية ضد هذا نوع من الجرائم الإلكترونية ووضع قانون عقوبات لردع من يرتكبها

إن التهديدات الفضاء الالكتروني هو خطر والحاضر والمستقبل، والتي مست جميع الدول العالم مهما كانت متخلفة أو متقدمة، على حد السواء، حيث أصبحت تشكل خطرا مدمرا لمختلف المجالات الاقتصادية والاجتماعية والسياسية، وحتى الشخصية وهذا التهديد لم تنجي منه الجزائر، التي أدركتها أجهزتها الأمنية، مما دفعها لسن قوانين تدافع عنها وتوفر الأمن السيبراني للتصدي لكل التهديدات الموجود داخل الفضاء السيبراني.

قائمة المراجع:

1) امنة، زعيطي. (2019). مكافحة الجرائم الالكترونية في ضوء قانون العقوبات الجزائري دراسة مقارنة. مجلة حقوق الإنسان و الحريات العامة، 4(1)، صفحة ص233.

2) مباركة، حنان كركوري. (2020). خصوصية ارتكاب الجريمة السيبرانية في النظام المعلوماتي-دراسة تحليلية على ضوء القانون الجزائري. مجلة الدراسات الاستراتيجية والعسكرية-المركز الدمقراطي العربي، 2(8)، الصفحات ص-12-13.

3) Amoroso, E. (2007). cyber security. silicon press.

4) Clarke, A. R., & Knake, R. (2010). cyberwar the next threat the national security and what to do about it. harper Collins.

5) desforges, A. (2014). les représentation ducyberespace un outil géoplitique/. revue hérodote, 1-2(n°152-153)), pp. p67-81. Récupéré sur www.cairn.info/revue-herodot-2014-1-page-67.htm

6) Kemmerer, A. r. (2003). cybersecurity. clifornia, santa Barbara: university of clifornia santa Barbara department of computer science.

7) kempf, o. (2012, novembre). /introduction à la cyberstratégie/. economica, p. p09. Récupéré sur www.cairn.wfo/revu

8) kempf, o. (2012). cyberstratégie à la français. revue internationale et stratégique, 3(87), p. p121. Récupéré sur www.cairn.wfo/revue-internationale-et-stratigique-2012-3-p121

9) okaz.com.sa/article/1585529 . (site vue 13/01/2022). Récupéré sur okaz.com.sa: https://www.okaz.com.sa/article/1585529 site vue 13/01/2022))

10) political-encyclopedia-org/dictioary/الامن السيبراني. (site vue 2022, 01 23). Récupéré sur https://political-encyclopedia-org/dictioary/الامن السيبراني site vue 23/01/2022

11) shakarian, P., shakarian, j., & Ruef, A. (2013). introduction to cyber-warfare a multidisciplinary approach. Elsevier.

12) (site vue 11/01/2022). Récupéré sur https://fr.m-wikipedia.org: https://fr.m-wikipedia.org

13) (site vue 24/02/2022). Récupéré sur www.wipo.int/edocs/lexdocs/law/ar/dz/dz027ar.pdf: https ;//www.wipo.int/edocs/lexdocs/law/ar/dz/dz027ar.pdf

14) اخلاص، بن عبيد . (2021). الحماية القانونية للمعطيات الشخصية في ظل القانون 18-07 المتعلقة بحماية الاشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي. مجلة الجزائرية للحقوق والعلوم السياسية، 6(1)، الصفحات ص676-677.

15) إدريس، عطية. (د.ت.ن). /مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري//مجلد1/العدد1//ص102. مجلة مصداقية، 1(1)، الصفحات ص108-104-102-112-113.

16) إسماعيل، زروقة. (2019). الفضاء السيبراني والتحول في مفاهيم القوة والصراع. مجلة العلوم القانونية والسياسية، 10(1)، الصفحات ص.ص -2027-1023-1017-1018.

17) القانون 18-04،الذي يحدد القواعد المتعلقة بالبريد والاتصالات الالكترونية ج،ر عدد27/13 مايو 2018/ص10. (13 مايو، 2018). جريدة الرسمية(27)، ص10. الجزائر.

18) حسن بن احمد، الشهري. (2010). /الانظمة الالكترونية الرقمية المطورة لحفظ وحماية سرية المعلومات من التجسس. مركز النور للابحاث الاكتروتية، صفحة ص11.

19) حنين جميل، أبو حسين. (2021). الإطار القانوني لخدمات الأمن السيبراني2. رسالة ماجستير، 2. عمان: جامعة الشرق الأوسط.

20) خيرة، رابحي. (2009-2010). اتفاقية الانترنت دراسة ميدانية لاستعلامات الشبكة بمدينة تيصيرت. رسالة ماجستير، ص78. وهران: جامعة وهران علم المكتبات والعلوم الوثائقية.

21) رامي متولي، القاضي. (2011). مكافحة الجرائم المعلوماتية. مصر، مصر: /دار النهضة العربية.

22) رضا، مهدي. (2021). الجرائم السيبرانية وأليات مكافحتها في التشريع الجزائري. مجلة إيليزا للبحوث و الدراسات، 6(2)، الصفحات ص -119-120-121-112-118.

23) سمير، بارة. (2017). الامن السيبراني((cybersecurity الجزائر السياسات والمؤسسات. (4)، الصفحات ص-35-259.

24) عادل، غزال. (مارس، 2014). مشاريع الحكومة الالكترونية من الاستراتجية الى التطليق مشروع الجزائر الحكومة الالكترونية. مجلة المكتبات و المعلومات(34)، صفحة ص64.

25) عاقلي، فصيلة. (2017). الجريمة الالكترونية في القانون الجزائري والقانون المقارن. المؤتمر الدولي الرابع الجريمة الكترونية، (صفحة ص133). لبنان.

26) عبد الرحمان، حملاوي . (2015/09/16). دور المدير العامة للامن الوطني في مكافحة الالكترونية الجريمة المعلوماتية بين الوقاية والمكافحة. ملتقي وطني في مكافحة الجرائم الالكترونية (صفحة ص10). بسكرة : جامعة بسكرة .

27) عنترة، بن مرزوق، و حرشاوي. (2017). الامن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية. مؤتمر الدولي استراتيجيات الدفاع الوطني (صفحة ص68). ورقلة: جامعة ورقلة.

28) ليندة، شرا بشة. (د.ت.ن). السياسة والإقليمية في مجال مكافحة الجريمة الالكترونية الاتجاهات الدولية في مكافحة الجريمة الالكترونية. 1(1)، صفحة ص242.

29) محمد الطاهر، سعيود . (2020). استقلالية سلطة ضبط البريد والاتصالات الالكترونية في ظل احكام القانون 18-04. مجلة الدراسات حول فعلية القاعدة القانونية، 4(1)، صفحة ص46.

30) محمد، مختار. (2015). هل يمكن ان تتجنب الدول مخاطر الهجمات الالترونية. مجلة اتجاهات الاحداث(6)، الصفحات ص5-6.

31) محمد امين، الشوابكة. (2011). الشوابكة، محمد امين 2011جرائم الحاسوب و الانترنت. دار الثقافة.

32) (2013). مكتب الامم المتحدة 2013المعني بالمخدرات والجريمة دراسة شاملة عن الجريمة السيبرانية. مكتب الامم المتحدة.

33) مهدي، رضا. (2021). لجرائم السيبرانية وأليات مكافحتها في التشريع الجزائري. مجلة إيليزا للبحوث و الدراسات، 6(2)، صفحة ص112.

34) هند، علوي. (2008-2007). المرصد الوطني لمجتمع المعلومات الجزائري قياس النفاذ الى التكنلوجيا المعلومات والاتصالات بقطاع التعليم بالشرق الجزائري. رسالة الدكتوراه، ص1. قسنطينة: قسنطينة تخصص علم المكتبات.

35) يوسف، بوغرارة. (2018). الأمن السيبراني :الإستراتجية الجزائرية للأمن والدفاع في الفضاء السيبيري. مجلة الدراسات الإفريقية وحوض النيل-المركز الديمقراطي العربي، 1(3)، الصفحات ص101-103-111.

الإكتشاف الإلكترونى & حجية الأدلة الرقمية بالجرائم الإلكترونية

Electronic Discovery & Digital Crime Evidence Authority

د.أمل فوزي أحمد عوض/ جامعة حلوان/ مصر

Dr. Amal Fawzy Ahmed Awad/ Helwan University/ Egypt

ملخص الدراسة:

تلعب البيانات دورًا مركزيًا لتطوير خوارزميات الذكاء الاصطناعي للاستخدام الفعلي فى مجال القانون وخاصة بالاكتشاف الإلكترونى للوصول الاسرع للبيانات القانونية والذى يحقق بالتبعية وصولا اسرع للعدالة، ولكن تطوير واستخدام خوارزميات الذكاء الاصطناعي مقيد بنقص البيانات التي يسهل الوصول إليها. كما ان الإشكالية فيما يتعلق بالإثبات التي تثيرها الإستعانة بالوسائط الرقمية بالتقاضي هي إنه في الوضع العادي عندما يوجد ملف ورقي وآخر رقمي، فيمكن الوقوف علي صحة الأخير بمقارنته بالأول، أما في فرض البيئة الرقمية والدليل الرقمي كيف يمكن التحقق من سلامة بيانات مستند معين ؟، وكيف يمكن التعويل علي الدليل الرقمي في الإجراءات عموما خاصة ان التبديل أو التعديل في الملفات الرقمية لا يترك أي أثر عليه ؟، وجميع ما سبق يشكل تحديات غاية في الصعوبة أمام مستقبل الاكتشاف الإلكترونى وقبول الدليل الرقمى ... ترى كيف يتم التغلب علىها؟؟؟؟؟

الكلمات المفتاحية: الاكتشاف الإلكترونى، البيانات، الذكاء الاصطناعي، دليل، رقمي، قبول، حجية

Absract :

Data play a central role in the development of artificial intelligence algorithms for actual use in the field of law, in particular in the electronic discovery of faster access to legal data, which, by extension, will achiee faster access to justice, but the development and use of artificial intelligence algorithms is constrained by a lack of easily accessible data. The problem with proof raised by the use of digital media in litigation is that, in the normal situation where a paper file and a digital file exist, the validity of the latter can be seen by comparing it to the former, but in the imposition of the digital environment and the digital directory, how can the integrity of the data of a particular document be verified? How can digital evidence be relied upon in procedures in general, especially since switching or modifying digital files leaves no impact on it? And all of the above poses extremely difficult challenges to the future of electronic discovery and acceptance of digital evidence... You see how it's overcome?

Keywords: Electronic discovery , data , artificial intelligence , evidence , digital , acceptance , authority.

مقدمة:

بعد ما يقرب من 20 عامًا من الابتكار المستمر الذي يركز بشكل أساسي على الاكتشاف الإلكترونى، يبدو أن التكنولوجيا القانونية تدخل مرحلة جديدة في حين أن المهنة القانونية ككل لا تزال متشككة إلى حد ما في التكنولوجيا وحذره من التغيير - خاصة عند مقارنتها بالصناعات الأخرى في حين يقبل معظم المحامين الآن فرضية أن الأتمتة

ضرورية لإدارة مكاتب المحاماة والإدارات القانونية بشكل أكثر كفاءة في ديناميكية بيئة أعمال شديدة التنافسية تعتمد على البيانات بشكل متزايد[1].

وهو ما يترتب عليه ان يتغير فهمنا لما يجعل الأتمتة ضرورية ومهمة، وحيث أن الاستثمارات في التكنولوجيا يمكن أن تكون فخًا، مع وجود تكاليف باهظة للوصول السريع للبيانات، في ظل التطور المستمر في تكنولوجيا المعلومات وتحديث البيانات.

تتعرض مكاتب المحاماة وعملائها من الشركات لضغوط هائلة لتقديم قيمة أكبر في مقابل أقل ولأن تكون أكثر عرضة للمساءلة أمام أصحاب المصلحة، يتم الشعور بهذا الضغط أيضًا بشكل حاد في قطاع التكنولوجيا القانونية، حيث ستحتاج الشركات التي تبحث عن طريق إلى النجاح المستدام إلى تكييف نماذج أعمالها مع التطور المستمر في تكنولوجيا المعلومات وأمن البيانات، هذا ويترتب على استخدام تطبيقات تكنولوجيا المعلومات والتحول الرقمي في مجال القانون أن لدينا الكثير من الأدوات الرقمية لابد من الوقوف عليها والمعرفة بها، فنحن كثيرًا ما ننقل البيانات من أداة إلى أخرى، ونقوم باستمرار بتسجيل الدخول والخروج من تطبيقات متعددة، وهذا يعني أيضًا أن البيانات الحساسة أكثر عرضة للضياع والتلف والاختراق .

مشكلة البحث:

حيث تلعب البيانات دورًا مركزيًا لتطوير خوارزميات الذكاء الاصطناعي للاستخدام الفعلي فى مجال القانون وخاصة بالاكتشاف الإلكترونى للوصول الاسرع للبيانات القانونية والذي يحقق بالتبعية وصولا أسرع للعدالة، ولكن تطوير واستخدام خوارزميات الذكاء الاصطناعي مقيد بنقص البيانات التي يسهل الوصول إليها. فالمؤسسات والإدارات والهيات القانونية غنية بالوثائق وفقيرة للبيانات "كالآراء القضائية إما لأنها غير متوفرة أو متنوعة في الشكل بحيث يصعب استخدامها بفعالية. بالإضافة إلى ذلك، يمكن أن تؤدي مجموعات البيانات ذات الجودة الرديئة أو المعيبة إلى قيام أنظمة الذكاء الاصطناعي بإخراج نتائج غير عادلة، وقد تؤدي تقنيات جمع البيانات، وإعدادها، وتحليلها إلى تحيزات إحصائية في مجموعة البيانات. كما ان الإشكالية فيما يتعلق بالإثبات التي تثيرها الإستعانة بالوسائط الرقمية بالتقاضي هي إنه في الوضع العادي عندما يوجد ملف ورقي وآخر رقمي، فيمكن الوقوف علي صحة الأخير بمقارنته بالأول، أما في فرض البيئة الرقمية والدليل الرقمي كيف يمكن التحقق من سلامة بيانات مستند معين؟ وكيف يمكن التعويل علي الدليل الرقمي في الإجراءات عموما خاصة ان التبديل أو التعديل في الملفات الرقمية لا يترك أي أثر عليه ؟ وهل وجهة النظر القائلة بأن أي عيوب تتبدي بالنظام الرقمى لا يمكن ان تتساوي بحال من الأحوال مع الوضع قبل الإستعانة بتكنولوجيا المعلومات في القضاء على صواب؟ وكيف يمكن إنتقاء ايجابيات الدليل الرقمي والتعويل عليها؟ وإتقاء سلبيات الدليل الرقمي ومعالجتها؟، فقد يتم التلاعب بمجموعات البيانات أو إتلافها عمدًا للحصول على تحليلات غير عادلة فبالإضافة إلى مشكلات جودة البيانات ومعالجتها، تنشأ أيضًا مخاوف كبيرة بشأن خصوصية البيانات والأمن السيبراني مع استخدام كميات هائلة من البيانات بواسطة أنظمة الذكاء الاصطناعي. وجميع ما سبق يشكل تحديات

[1] راجع فى ذلك :

https://www.lawtechnologytoday.org/2019/07/client-driven-innovation-the-future-of-legal-technology/

غاية في الصعوبة أمام مستقبل الاكتشاف الإلكترونى والدليل الرقمى ... ترى كيف يتم التغلب عليها؟ وبأي الوسائل قانونية؟ أم تقنية؟

أن أول ما يُطرح في موضوع الإثبات هو توفر السند الخطي، سواء كُتب بخط اليد أو بالآلة الكاتبة، وما يحتويه من البيانات، وتوقيع أطرافه، وتعدد النسخ في العقود المتبأدلة ، والشكل الذي قد يفرضه القانون في حالات معينة. هذا بالاضافة إلى معضلة تحديد القانون الواجب التطبيق على العقود الرقمية الدولية وقوتها الثبوتية، وإشكالية إستعماله، وإثباته، وطريقة تقديمه للمحكمة الناظرة في النزاع المتعلق به. وكذلك اشكالية تحديد مفهوم أصل السند الرقمي وصورته؛ إذ أن النسخة هي تكرار الأصل في كل جزئياته، لذلك تعتبر النسخة أصلاً جديداً من دون تمييز بينهما. لكن التساؤل الأساسي[1] في هذا الصدد والذي يستتبع تبني الإستعانة بالوسائل الرقمية في التقاضي **هو:**

- ✓ هل هذه الآليات-أي الوسائل الرقمية-على درجة من الكفاءة بحيث يمكن الإعتماد عليها في ضمان سلامة البيانات وأمن المعلومات المتداولة رقميا؟[2]
- ✓ كيف يمكن التحكم في الصعوبات المرتبطة بإستخدام التكنولوجيا دون الإخلال بالتنظيم القضائي والضمانات الأساسية لحسن سير العدالة؟[3]

ذلك ان الإشكالية [4] فيما يتعلق بالإثبات التي تثيرها الإستعانة بالوسائل الرقمية[5] في التقاضي هي إنه في الوضع العادي عندما يوجد ملف ورقي وآخر رقمي، فيمكن الوقوف على صحة الأخير بمقارنته بالأول، أما في فرض البيئة الرقمية والدليل الرقمي كيف يمكن التحقق من سلامة بيانات مستند معين (ويمكن التعويل عليه في الإجراءات عموما خاصة ان التبديل أو التعديل في الملفات الرقمية لا يترك أي أثر عليه و العكس[6]) من هذا النقد يري البعض أن أي عيوب تتبدي في النظام الرقمي لا يمكن ان تتساوي بحال من الأحوال مع الوضع قبل الإستعانة بتكنواوجيا المعلومات في القضاء .

إن الذي يضفي الرسمية على الأوراق / المستندات في النظام الورقي هو التوقيع، وهو نفس الآلية التي سوف يعتمدها المشرع لإضفاء الرسمية على المحررات الرقمية.

[1] راجع فى ذلك: د/فاطمةعادل سعيد «التقاضي عبر وسائل التكنولوجيا والاتصال الحديث " ، بحث مقدم الى مؤتمرالقانون واللتكنولوجيا - كلية الحقوق – جامعةعين شمس ، فى الفترة من 8 الى 10 ديسمبر 2017.

[2] يقصد بمصطلح **سلامة البيانات:** "التحقق من ان البيانات التى تضمنتها الوثيقة لم يحدث بها أى تعديل أو حذف سواء لأسباب طبيعية أو عمدية." راجع د.محمد محمد سادات ،. حجية التوقيع الرقمى فى الاثبات، رسالة دكتوراه، ج. المنصورة، ٢٠١٠، ص ١٩٥

3راجع فى ذلك: أسامة المناعسة وآخرون؛ د. هلالي عبداللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي . دراسة مقارنة، الطبعة الأولى ، دار النهضة العربية . القاهرة ، 1997 ، وقد آثرنا الاشارة دون الافاضة لعدم اتساع المجال لذلك .

[4] Helmut Rüßmann, Electronic Documents. Security and Authenticity, Electronic Technology and Civil Procedure- New Paths to Justice from Around the World, Springer, 2012, p.235.

[5] راجع فى ذلك كلا من :

-Walker, Janet, and Garry D. Watson. "New Trends in Procedural Law: New Technologies and the Civil, Litigation Process." Hastings International and Comparative Law Review 31.1 (2008), http://www.delmarlearning.com/companions/content/1401824293/guides/CH6.

[6] Jay Thornton, (Cost, Accuracy, and subjective fairness in legal information technology: a response to technological due process critics), New York university law review, December 2016, Vol.91, p.

أهداف البحث:

1. الوقوف على أهم مصطلحات الإثبات الرقمى: كالدليل الرقمى، التوقيع الرقمى، المحررات الرقمية
2. الوقوف على أهم إشكاليات قبول الأدلة بالإثبات الرقمى.
3. الوقوف على ماهية إدارة المعلومات الذكية لإدارة الخصومة القضائية رقميًا " من خلال عملية الاكتشاف الإلكترونىE -discovery .

منهج البحث:

سوف نستخدم في هذه الورقة البحثية المنهج التحليلي والتأصيلي لعرض مسائله وطرح المعالجات والحلول الملائمة

خطة البحث:

سوف نطرح معالجات للتساؤلات السابق ذكرها على مستوى عدد من المباحث على النحو التالى:

المبحث الأول: الاكتشاف الإلكترونى

المطلب الأول: ماهية الاكتشاف الإلكترونى

المطلب الثانى: متطلبات الاكتشاف الإلكترونى

المطلب الثالث: الذكاء الاصطناعي والاكتشاف الإلكترونى

المطلب الرابع :تحديات الاكتشاف الإلكترونى

المبحث الثانى: الأدلة الرقمية

المطلب الأول: ماهية الأدلة الرقمية

المطلب الثاني: أنواع الأدلة الرقمية والمستندات الرقمية

المطلب الثالث: تحديات قبول الأدلة الرقمية

المبحث الأول: الاكتشاف الإلكترونى

وللوقوف على ماهية الاكتشاف الإلكترونى ومعرفة ما اذا كان مزايا ام تحديات ماهية إدارة المعلومات الذكية والاكتشاف الإلكترونى بالمطلب الأول، التخطيط الناجح للأكتشاف الرقمى بالمطلب الثانى، **متطلبات** الاكتشاف الإلكترونى بالمطلب الثالث، **الذكاء** الاصطناعي والاكتشاف الإلكترونى بالمطلب الرابع، تحديات الاكتشاف الإلكترونى (الخصوصية / امن المعلومات) بالمطلب الخامس وذلك على النحو التالى

المطلب الأول: الاكتشاف الإلكترونىE - DISCOVERY

الفرع الأول: ماهية الاكتشاف الإلكترونى E - discovery؟[1]

[1]راجع في ذلك كلا من :

- https://en.wikipedia.org/wiki/Electronic_discovery
- https://www.exterro.com/basics-of-e-discovery
- https://www.logikcull.com/what-is-ediscovery-software
- https://www.exterro.com/basics-of-e-discovery/e-discovery-process

الاكتشاف هو المصطلح المستخدم للمرحلة الأولية من التقاضي حيث يتعين على الأطراف في النزاع تقديم المعلومات والسجلات الأخرى ذات الصلة، إلى جانب جميع الأدلة الأخرى المتعلقة بالقضية .المفتاح لمعالجة - E discoveryهو أن تكون استباقيًا في إدارة المعلومات والسجلات مع التحكم في معالجة طلبات E - discovery المحتملة. فالمقصود من تبادل الأدلة والمستندات هو[1] تسليم صورة من المذكرة بالمناولة للخصم أو وكيله مع توقيع المستلم على الأصل قبل تقديمها للمحكمة، في حين أن الأصل أن يتم إيداع المذكرة في مكتب إدارة الدعوي بالمحكمة المختصة (سواء أكانت محكمة أول درجة أو محكمة ثاني درجة) ويتم إبلاغ الخصم بذلك الإيداع ويتم اطلاعه عليها في ملف القضية بمكتب إدارة الدعوي، كما يترتب على إيداع مذكرة الدفاع اعتبار المدعي عليه حاضراً حكماً ولو تخلف عن الحضور. وتري الباحثة إنه يجب تعديل نصوص القانون بما يسمح للخصوم بالتقديم والتبادل والاطلاع عل هذه المستندات رقميا [2]. وهو ما يعرف الآن بالإكتشاف الإلكترونى[3]، والذي يعد من تطبيقات التقاضي الرقمي، ويتم تعريف الإكتشاف الإلكترونى علي أنه العملية القانونية السابقة الأطراف علي المعلومات المخزنة رقميًا ومراجعتها، وهو إجراء مطبق بالنظم القضائية المقارنة حيث عملت القواعد الفيدرالية للإجراءات المدنية لعام 2006 (FRCP) علي وضع المعلومات المخزنة رقميًا (ESI) علي قدم المساواة مع المستندات الورقية في نظر المحكمة[4].

يمكن استخدام ESI5 أي نوع من بيانات أو الأجهزة ESI بما في ذلك على سبيل المثال لا الحصر، النصوص، والصور، والصوت، وقواعد البيانات، وجداول البيانات، والأنظمة القديمة، والشري، والهواتف الذكية، والأجهزة اللوحية، والرسائل الفورية، والبريد الإلكترونى، وملفات التقويم، ومواقع الويب[6].

فالإكتشاف الإلكترونى[7] ISE (électronica Discovery) يشبه إلي حد كبير E-filing ، هو موجة الحاضر والمستقبل، وتحدي للواقع أيضاً [8].

[1] راجع في ذلك : د/ سيد احمد محمود ،"نحو رقمية القضاء المدني الاماراتي" ، ص327.

[2] راجع في ذلك :

– كيفية إرسال مستندات المحكمة المدنية:

– https://docplayer.net/13527036-File-how-to-transmit-civil-court-documents-by-fax-for-filing-in-court-registries-in-b-c-transmitting-by-fax-court-services-court-services-branch.html 2020/9/22 (تاريخ آخر دخول علي الموقع

[3] راجع في ذلك:

Mikl s Kengyel; Zolt n Nemess nyi; International: Electronic technology and civil procedure : new paths to justice from around the world,p285. http://www.worldcat.org/title/electronic-technology-and-civil-procedure-new-paths-to-justice-from-around-the-world/oclc/773670695

[4] راجع في ذلك:

– Legal Technology Vision Towards the digital transformation of the legal sector , Legal Technology Cluster Committee , Singapore Academy of Law , p33

– https://bok.ahima.org/doc?oid=107115#.YDekLujXLx4 تاريخ آخر دخول علي الموقع 21/2/2021

[5] راجع في ذلك:

Ediscovery And Digital Forensics , Solving Legal And Regulatory Issues , P1-6 , Cyber@Bsigroup.Com , Bsigroup.Com

[6] راجع في ذلك:

ADAM I. COHEN, DAVID J. LENDER, ELECTRONIC, DISCOVERY, PRACTICE, GUIDELINES, p2-37

[7] راجع في ذلك :

AHIMA. "E- Discovery Litigation and Regulatory Investigation Response Planning: Crucial Components of Your Organization's Information and Data Governance Processes." Journal of AHIMA 84, no.11 (November–December 2013): expanded web version , p 1-91 .

[8] راجع في ذلك :

ثانيا: الاكتشاف الإلكترونى -التكوين الحقيقي لحركة إدارة المعلومات والبيانات اليوم[1]

دون علم الكثيرين، فإن الأصل الحقيقي لحركة إدارة المعلومات والبيانات اليوم يكمن في دعوى التمييز بين الجنسين العادية التي رفعتها متداولة الأوراق المالية لورا زوبولاك في المنطقة الجنوبية من نيويورك .(SDNY) عندما رفعت متداولة الأوراق المالية، لورا زوبولاكي دعوى قضائية ضد صاحب عملها، يو بي إس واربورغ، في عام 2002، لم يكن من المحتمل أن يفهم يومًا ما أنها ستعرف بأنها رائدة في حركة إدارة المعلومات والبيانات اليوم - أو أن قضيتها ستؤثر وتغير الطريقة إلى الأبد يدير المستشار القانوني والمنظمات التي يمثلونها معلوماتهم وبياناتهم - أو قد تكون العواقب المترتبة على المعالجة غير الصحيحة للمعلومات المخزنة رقميًا من قبل المستشار القانوني أو الادارة التي يمثلونها في سياق التقاضي وخيمة. حتى يومنا هذا، بالنسبة إلى قرارات Zubulake [2]، تعد قرارات من أهم قرارات القانون (إن لم تكن الأكثر أهمية) بشأن إدارة المعلومات والبيانات في عصرنا، و أربعة من خمسة من هذه القرارات أثرت على تعديلات FRCP لعام 2006 ، وكذلك العديد من تعديلات 2013 المقترحة على FRCP لإدارة الاكتشاف الإلكترونى بنجاح .

عملية E -discovery القانونية - تعمل E - discovery من وقت رفع الدعوى حتى وقت تقديم الدليل الرقمي في المحكمة كما يلي[3]:

1. يتم تحديد البيانات على أنها ذات صلة من قبل المحامين ويتم وضعها قيد الحجز القانوني.
2. يقوم المحامون من كلا الجانبين بتحديد نطاق الاكتشاف، وتحديد ESI ذي الصلة، وتقديم طلبات E - discovery
3. يمكن التفاوض مع المستشار القانوني لتحديد ما يتم البحث عنه وللتأكد من تحديد الأدلة المطلوبة واستبعاد عدم وجود أدلة، وبالتالي تقليل الجهد الإجمالي المطلوب للبحث والمراجعة وتقديمه.

e-Discovery: What Litigation Lawyers Need to Know , Risk Management Practice Guide of Lawyers Mutual, LAWYERS MUTUAL LIABILITY INSURANCE COMPANY OF NORTH CAROLINA , p 2-17

, www.lawyersmutualnc.com

[1] راجع فى ذلك :

https://www.google.com/search?sxsrf=ALeKk03chjd_CNkdk1Fnsot6owkUFOs-4Q:1622449002937&q=Digital+Evidence+and+Computer+Crime:+Forensic+Science,+Computers+and+the+Internet&stick=

[2] راجع في ذلك:

- https://nydailyrecord.com/2013/07/22/an-interview-with-laura-zubulake/،
- https://www.relativity.com/blog/the-end-of-an-e-discovery-era-judge-scheindlins-law-from-zubulake-to-today/،
- https://en.wikipedia.org/wiki/Zubulake_v._UBS_Warburg،
- https://cloudnine.com/ediscoverydaily/case-law/ediscovery-history-a-look-back-at-zubulake/،
- https://www.larkinhoffman.com/files/OTHER/bjd_ppp_elecdis.pdf

[3] راجع في ذلك: التحول الرقمي: الآثار الرئيسية لخدمات وعروض تكنولوجيا شركة المحاماة

https://www.lawtechnologytoday.org/2019/05/digital-transformation-key-implications-for-law-firm-technology-services-and-offerings

4. ثم يتم استخراج الأدلة وتحليلها باستخدام إجراءات الطب الشرعي الرقمية، والتي عادة ما يتم تحويلها إلى صيغة PDF[1]أو TIFF[2] لاستخدامها في المحكمة

مفتاح النجاح مع E - discovery هو أن يكون لديك سياسة تشدد على:

- ✓ التخلص من المعلومات التي ليس لها قيمة تجارية وفقًا للسياسة وفي سياق العمل العادي
- ✓ تخزين السجلات التي لها قيمة للمؤسسة وإدارتها بشكل صحيح، تحت سيطرة الادارة.
- ✓ تنفيذ مخطط التصنيف الذي يوفر بنية إدارة المعلومات والسجلات لتحقيق الاتساق والتحكم
- ✓ تدمير السجلات التي لم تعد هناك حاجة إليها بطريقة منهجية وموثقة وآمنه.

كما تُمكِّن تطبيقات E - discovery[3] المؤسسات من سحب المعلومات والسجلات من الأحجام الهائلة للمحتوى ، بما في ذلك رسائل البريد الإلكترونى .

الفرع الثانى: متطلبات الاكتشاف الإلكترونى[4]

ما يتم تجاهله أحيانًا في صياغة طلبات الاكتشاف والتفاوض بشأنها هو *شكل* إنتاج المستندات، يمكن أن يؤدي تحديد شكل الأدلة الرقمية بالاكتشاف إلى توفير قدر كبير من الوقت والمال في مرحلة مراجعة المستندات ويؤدي إلى إنتاج بيانات قيمة لن يتم إنتاجها على الإطلاق.

أولا: البيانات الوصفية

يجب أن تحتوي جميع عمليات إنتاج المستندات الرقمية، واستخراج الأدلة الرقمية على بعض حقول البيانات الوصفية الأساسية، بما في ذلك:(اسم الملف ;تعديل التواريخ;تاريخ إرسال البريد الإلكترونى;مؤلف الرسالة;التعديل الأخير من قبل المرسل;المستلمون (بما في ذلك النسخ المخفية (نسخة مخفية الوجهة); مسار المصدر;سطر الموضوع) الغرض من البيانات الوصفية هو الحفاظ على المعلومات حول المستندات التي قد تضيع إذا تم إعادة معالجتها.

لا توفر هذه المعلومات حقائق أساسية غير واضحة من المستند فحسب، بل تساعد أيضًا في المراجعة الفعالة والدقيقة للوثائق، ويعد تحليل البيانات الوصفية أحد الطرق الرئيسية التي يمكن لفريق مراجعة المستندات من خلالها التعرف بذكاء على المستندات ذات الاهمية دون الحاجة إلى الانخراط في مراجعة خطية يدوية.

[1] صيغة الPDF هي صيغة رقمية للملفات صممتها أنظمة ال Adobe باستخدام بعض الأكواد الملحقة بخصائص اللغات. يأتي البرنامج الرسمي لمشاهدة الملفات بصيغة ال Adobe Reader. وعادة ما يكون ملف ال PDFدمجًا بين النصوص ذات الرسوميات التسامتية والموجّهة والنصوص والنصوص المكتوبة بالجافا وعناصر أخرى.

[2] الTIFF : هي صيغة لتخزين الرسوميات النقطية. تُستخدّم للمسح الضوئي وفي مجال نصوص الOCR، لإرسالها بالفاكس وطباعتها كما أنه مدعوم من العديد من التطبيقات الرسومية. طوّرت الصيغة شركة Aldus بالتعاون مع مايكروسوفت لاستخدامها مع الأكواد اللاحقة بالصيغة المستخدّمة لتخزين الصور بعمق رائع للون، والتي تمتلك حقوق النشر الخاصة بها أنظمة أدوبي.

[3] https://www.getapp.com/legal-law-software/electronic-discovery/

[4] راجع فى ذلك :

https://www.lawtechnologytoday.org/2017/08/e-discovery-request-youre-requesting/

ثانيا: تنسيق المستندTIFFs[1]

في حين أن تنسيق TIFF هو شكل مقبول من أشكال الإنتاج للعديد من المستندات، يجب إنتاج أنواع معينة من الملفات بتنسيق أصلي بالنسبة إلى مستندات معينة حتى لا يتم فقد المحتوى المهم، مثل ملاحظات المتحدث في العروض التقديمية أو تتبع التغييرات والتعليقات في مستندات معالجة الكلمات.

يمكن أن تكون المعلومات الإضافية في هذه المستندات مفيدة جدًا أيضًا في صياغة استراتيجية مراجعة المستندات والأدلة

الرقمية مما يسمح لشركة المحاماة والعميل لاكتساب فهم أشمل للحقائق في وقت مبكر من عملية الاكتشاف.

ثالثا: تحديد "المستندات"

من المهم أيضًا تحديد جميع أنواع البيانات المطلوبة حيثران الفشل فيعرض كل فئات "المستندات" المطلوبة بشكل فردي يمكن أن يؤدي إلى إغفال مصادر البيانات الرئيسية والمعلومات الهامة فمن المحتمل أن تكون هناك بيانات غير عادية، مثل الدردشات والنصوص ومحركات الأقراص المشتركة والبريد الصوتي والتسجيلات الهاتفية.

يضمن طلب هذه الأنواع من المستندات في طلبات الاكتشاف أن يحصل العميل على الحقائق والاتصالات بشكل أساسي لبناء القضية، لا سيما في الصناعات المعروفة بالاعتماد على هذه الأشكال من الاتصالات.

عند التفكير في أنواع المستندات المطلوب تقديمها كدليل رقمى بالتقاضى، من المهم أن تضع في اعتبارك أنه سيُطلب منك أيضًا على الأرجح إنتاج هذه الأنواع من المستندات أيضًا .إذا اعتقد أحد الأطراف أن العبء سيكون أكبر بكثير على عاتق الطرف الآخر لمراجعة وإنتاج فئة معينة من المستندات، وهذا العبء لا يفوقه المنفعة المحتملة لتلقي إنتاج الطرف الآخر لنفس البيانات، لذا يجب إجراء دراسة متأنية من جانب أطراف الدعوى المعنيين بالتفاصيل الأخرى للتقاضي المطروح للتأكد من أنهم يركزون على أنواع المستندات التي من المرجح أن تحتوي على المعلومات المطلوبة مما يسمح بمراجعة مبسطة وفعالة لـESI وتطوير فهم كامل للحقائق والقضايا التي تنطوي عليها القضية.

المطلب الثانى: الذكاء الاصطناعي والاكتشاف الإلكترونى[2]

مع بداية العام الحالى، توقع البعض في المجال القانوني أن الذكاء الاصطناعي ("AI") سيلعب دورًا مؤثرًا بشكل متزايد في تقديم الخدمات القانونية وسيجلب فهمًا أكبر لكيفية تعزيز [تحليلات البيانات والذكاء الاصطناعي].

أولا: تعريف الذكاء الاصطناعي[3]

[1]راجع فى ذلك:

https://www.lawtechnologytoday.org/2020/02/5-ways-to-retake-control-of-your-document-intensive-business-processes

[2]راجع فى ذلك:

https://www.lawtechnologytoday.org/2021/02/using-artificial-intelligence-to-improve-law-firm-performance

[3]راجع فى ذلك:

"Intellectual property and artificial intelligence Reality & the Future", BISKRA UNIVERSITY - FACULTY OF LAW AND POLITICAL SCIENCES Laboratory impact of jurisprudence on the dynamics of legislation, Jurisprudence Journal - Vol 35 – (Special Issue - S N 42) – 19 January 2021.

ببساطة، الذكاء الاصطناعي هو استخدام "التكنولوجيا لأتمتة المهام التي تتطلب عادةً ذكاءً بشريًا " تتضمن هذه المهام القدرات البشرية على التفكير والتحليل والتعميم وحل المشكلات والتعلم، ويُصنف أنظمة الذكاء الاصطناعي بأنها "قوية" أو "ضعيفة" بناءً على درجة قدرتها على أداء القدرات البشرية، ويساعد هذا التمييز في تحديد نطاق قدرات أنظمة الذكاء الاصطناعي الحالية، على الرغم من أن هذه القدرات تقع عبر نطاق وليس ضمن فئات متميزة.

يكون الذكاء الاصطناعي "قويًا" حقًا عندما يمكنه على الأقل "أداء أي مهمة فكرية يستطيع الإنسان فعلها بنجاح"، إن لم يكن لديه أيضًا القدرة على تجربة الوعي وفهم مفاهيم مثل اللغة، وعلى الرغم من "ضعف" أنظمة الذكاء الاصطناعي مثلAlphaGo ، يمكن للذكاء الاصطناعي الضعيف أداء مجموعة متنوعة من المهام البشرية .

ثانيا: فائدة الذكاء الاصطناعي في الصناعة القانونية

على وجه التحديد لاستخدامه في الصناعة القانونية، يمكن تعريف الذكاء الاصطناعي على أنه أتمتة المهام عبر البرامج لتحقيق نفس النتيجة "كما لو أن ممارسًا قانونيًا قد قام بالعمل كما "يمكن تجميع المهام القانونية التي تؤديها أنظمة الذكاء الاصطناعي حاليًا في واحد من ثلاثة مجالات: تحليل المستندات[1] ، والبحث القانوني ، وأتمتة المهام .

ثالثا: حدود الذكاء الاصطناعي

تطوير واستخدام الذكاء الاصطناعي محدودان فيما يتعلق بالبيانات والخوارزميات والتنفيذ وحيث تلعب البيانات دورًا مركزيًا في أنظمة الذكاء الاصطناعي كمواد تدريبية لتطوير خوارزميات الذكاء الاصطناعي ومواد الإدخال للاستخدام الفعلي للذكاء الاصطناعي .لكن تطوير واستخدام خوارزميات الذكاء الاصطناعي مقيد بنقص البيانات التي يسهل الوصول إليها والتحليل" فمكاتب المحاماة" غنية بالوثائق وفقيرة للبيانات "والبيانات العامة مثل الآراء القضائية إما أنها غير متوفرة أو متنوعة في الشكل بحيث يصعب استخدامها بفعالية .علاوة على ذلك، يمكن أن تؤدي مجموعات البيانات ذات الجودة الرديئة أو المعيبة إلى قيام أنظمة الذكاء الاصطناعي بإخراج نتائج متحيزة فقد يكون لمجموعات البيانات جودة رديئة أو عيوب لعدة أسباب، وقد تؤدي تقنيات جمع البيانات أو إعدادها إلى تحيزات إحصائية في مجموعة البيانات مثل العينات غير التمثيلية (انحياز الاختيار) .قد يتم التلاعب بمجموعات البيانات أو إتلافها عمدًا

[1] تشمل الفئة الواسعة لتحليل المستندات تحليل العقود ومراجعة المستندات والإكتشاف الإلكتروني والعناية الواجبة تقدم الشركات القديمة والجديدة أدوات تحليل المستندات المدعومة بالذكاء الاصطناعي على سبيل المثال استخدمت JPMorgan برنامجها الخاص بعنوان Contract Intelligence ، الملقب بـ "COIN" ، لتقليل وقت مراجعة العقد السنوي بمقدار 360.000 ساعة، و تقدم الشركات الأحدث مثل Kira Systems و eBrevia كما ازداد استخدام الذكاء الاصطناعي في الإكتشاف الإلكتروني بشكل كبير نظرًا للكفاءات التي يوفرها.

للحصول على تحليلات غير عادلة .بالإضافة إلى مشكلات جودة البيانات، وقد تنشأ أيضًا مخاوف كبيرة بشأن خصوصية البيانات[1] والأمن السيبراني[2] مع استخدام كميات هائلة من البيانات بواسطة أنظمة الذكاء الاصطناعي [3].

يجب على مستخدمي الذكاء الاصطناعي المحتملين إدراك أن النشر الفعال للتكنولوجيا قد يكون أصعب مما يتوقع فالتحدي الأكبر هو ببساطة جعل المستخدمين المحتملين يثقون بالتكنولوجيا [4].

هذا ويفترض الباحثون أن الذكاء الاصطناعي سيؤثر على الواجبات الأخلاقية للمحامين فيما يتعلق بالكفاءة التقنية، والسرية، والإشراف، والتواصل مع العميل، والحكم المستقل، والممارسة غير المصرح بها للقانون، والرسوم الزائدة، وتضارب المصالح، ووتيرة التطور السريع للذكاء الاصطناعي تجعل من تحديد حدود تلك الواجبات من جانب التشريعات مسألة ملحة.

رابعا: كيف ينبغي للمحامين التعامل مع صعود الذكاء الاصطناعي في تقديم الخدمات القانونية والتكيف معه؟[5]

الذكاء الاصطناعي لديه القدرة على التأثير بشكل كبير على مهنة القانون، يخشى البعض أن يلحق الذكاء الاصطناعي الضرر بالمحامين وغيرهم من المهنيين القانونيين لأن التكنولوجيا تحل محل أجزاء على الأقل من وظائفهم وتقلل من فرص التدريب كما يتوقع آخرون أن الذكاء الاصطناعي سيساعد المحامين على تطوير ممارساتهم للتركيز على المهام ذات القيمة الأعلى والأدوار الجديدة أو فرص تقديم الخدمات ولقد قدم الكثيرون نصائح عملية حول كيفية تكيف المحامين مع استخدام الذكاء الاصطناعي في الصناعة القانونية، ولكن كيف يتعامل كل محام مع الذكاء الاصطناعي ويتكيف معه في السوق القانوني هو سؤال يجب أن يجيب عليه المحامى بنفسه.

[1]راجع فى ذلك:

Ossama Ahmed Attalla, Is The Legal Protection Of Digital Privacy Enough In Egypt"? Protection Of Digital Data Privacy ", A Paper Submitted For The Conference Of Cyber Crimes, National Institute Of Intellectual Property April 2020

بحث بعنوان " معالجات تشريعية لضبط الحقوق والحريات فى البيئة الرقمية" المؤتمر العلمى السادس ، القانون والشائعات ،كلية الحقوق ،جامعة طنطا ،23-24 ابريل 2019.

[2]راجع فى ذلك :

الأعمال الصغيرة: تدابير اختبار الأمن السيبراني:

https://www.lawtechnologytoday.org/2021/05/small-business-cyber-security-testing-measures

بحث بعنوان " الامن الانسانى فى ظل تحديات التحول الى الرقمية لمستقبل حقوق الانسان " ، الملتقى الدولى الموسوم " الأمن الإنساني في ظل التحديات العالمية المعاصرة " ، 9 و10 يناير 2021.

[3]راجع فى ذلك:

اتبع أفضل ممارسات أمان البريد الرقمي:

https://www.lawtechnologytoday.org/2021/05/working-from-home-7-cybersecurity-tips-to-protect-your-data

[4]راجع فى ذلك:

مساعد افتراضي مزايا وجود مساعد افتراضي في فريقك

https://www.lawtechnologytoday.org/2021/05/advantages-of-having-a-virtual-assistant-in-your-team

الابتكار الذي يحركه العميل: مستقبل التكنولوجيا القانونية

https://www.lawtechnologytoday.org/2019/07/client-driven-innovation-the-future-of-legal-technology

التحول الرقمي: الآثار الرئيسية لخدمات وعروض تكنولوجيا شركة المحاماة

https://www.lawtechnologytoday.org/2019/05/digital-transformation-key-implications-for-law-firm-technology-services-and-offerings

[5]راجع فى ذلك :

https://www.lawtechnologytoday.org/2019/04/artificial-intelligence-will-change-e-discovery-in-the-next-three-years

إن تطور واستخدام الذكاء الاصطناعي (AI) آخذ في الارتفاع ولا يظهر أي علامات على التوقف في المستقبل القريب، ومن المتوقع أن تزيد الإيرادات العالمية من تطبيقات المؤسسات التي تستخدم الذكاء الاصطناعي بنحو 30 مليار دولار بحلول عام 2025. مع هذا النمو الهائل، ولحسن الحظ، فإن المجال القانوني هو أرض خصبة لفوائد تكنولوجيا حيث يمكن الآن إنجاز المهام التي تستغرق وقتًا طويلاً باستخدام الأتمتة والتعلم الآلي في وقت أقل وبتكلفة أقل.

خامسا: الوضع الحالي لتكنولوجيا الذكاء الاصطناعي

الذكاء الاصطناعي هو أداة مفيدة يتم استخدامها على نطاق واسع في تطبيقات العالم الواقعي التي تتعلم إكمال المهام التي يقوم بها البشر عادة. حتى بالنسبة للعباقرة، من غير الواقعي للمحامين الاحتفاظ بقائمة كاملة لكل ما يحتاجون إلى معرفته في رؤوسهم في جميع الأوقات .ومع ذلك، فإن الوصول إلى كل جزء من البيانات ذات الصلة بشأن إجراء ونتائج مسألة سابقة يمكن أن يكون ميزة كبيرة في تحقيق نتائج إيجابية في مسائل مماثلة في المستقبل .هذا هو المكان الذي يأتي فيه الذكاء الاصطناعي.

"نظرًا لأن الذكاء الاصطناعي يمكنه الوصول إلى المزيد من البيانات ذات الصلة، فإنه يمكن أن يكون أفضل من المحامين في التنبؤ بنتائج النزاعات والإجراءات القانونية، وبالتالي مساعدة العملاء على اتخاذ القرارات .على سبيل المثال ، استخدمت شركة محاماة بلندن بيانات عن نتائج 600 قضية على مدى 12 شهرًا لإنشاء نموذج لجدوى حالات الإصابة الشخصية .في الواقع، تم تدريب الذكاء الاصطناعي على 200 عام من سجلات المحكمة العليا، وهو بالفعل أفضل من العديد من الخبراء البشريين في توقع قرارات.[1]

للذكاء الاصطناعي أيضًا العديد من التطبيقات الأخرى -الأكثر وضوحًا -التي يمكن لمكاتب المحاماة الاستفادة منها. بدلاً من قضاء ساعات العمل في إكمال المهام الشاقة والحذرة، والتي يمكن للذكاء الاصطناعي القيام بها بكفاءة. فالذكاء الاصطناعي "ليس ظاهرة جديدة تمامًا، والصناعة القانونية تستخدم الذكاء الاصطناعي في عملية اكتشاف التقاضي منذ ما يقرب من 10 سنوات."لقد شق الذكاء الاصطناعي طريقه بالفعل إلى مهنة القانون من خلال البحث القانوني ، ومراجعة العقود، والإدارة، ومراجعة الوثائق ، والتنبؤ بالنتائج القانونية ، وغير ذلك فمن المحتمل أن يكون ظهور الاكتشاف الإلكترونى هو أقرب مثال على استخدام الذكاء الاصطناعي في المهنة القانونية مع كل شيء منظم في شكل رقمي ، و يتيح الذكاء الاصطناعي للمتقاضين تنظيم المعلومات ذات الصلة وترابطها والبحث عنها بطرق أكثر فاعلية بكثير مما تسمح به المراجعة اليدوية للوثائق الورقية.

علاوة على ذلك، وفقًا لـ Bloomberg Law ، فإن الذكاء الاصطناعي "يساعد الباحثين القانونيين على اكتشاف الوثائق التي لم يكن بإمكانهم العثور عليها سابقًا وتحديد أوجه التشابه بين آراء المحاكم بسهولة أكبر. هذا بالإضافة إلى القدرة على تحليل الملايين من نقاط البيانات القانونية، بكفاءة كل ذلك بضغطة زر كما يمكن للذكاء الاصطناعي تزويدك بمعلومات لم تكن تعرف حتى للبحث عنها.

[1] راجع في ذلك: استخدام الذكاء الاصطناعي لتحسين أداء شركة المحاماة:
https://www.lawtechnologytoday.org/2021/02/using-artificial-intelligence-to-improve-law-firm-performance

المطلب الثالث: تحديات الاكتشاف الإلكترونى

كشفت دراسة حديثة أجرتها شركة تأمين ضد الممارسات الخاطئة أن المحاماة كانت ضحية للهجمات الرقمية .كان الضحايا أسماء في هذا المجال مما قد تتوقعه، لكن الشركات الأصغر ليست مستثناة بأي حال من الأحوال .على سبيل المثال ، وجدت نقابة المحامين الأمريكية مؤخرًا أن هذا الرقم كان 35٪ في مكاتب المحاماة التي تضم 10-49 محامًا - مما يعني أن أكثر من ثلث مكاتب المحاماة الصغيرة قد تم اختراقها ،ومع ذلك، بعيدًا عن كونه مسؤولية، تفيد تقارير منظمات المجتمع المدني أن الذكاء الاصطناعي يوفر دعمًا إضافيًا في مكافحة التهديد المستمر للهجمات الرقمية .تسمح خوارزميات التعلم الذاتي المدمجة في تقنية الذكاء الاصطناعي بفهم التهديدات المحتملة والتنبؤ بها بشكل أفضل بطرق لا يستطيع البشر في كثير من الأحيان توقعها. في الواقع، ويتسبب تطبيق الذكاء الاصطناعي في انخفاض مخاطر الأمن السيبراني.

1/ حاجة المستخدمين إلى المعلومات: و هي أحدى التحديات الأساسية التي تواجه عملية تطوير النظم والاحول بها الى الرقمية، وقد أثبتت التجربة أن النظم الرقمية الناجحة هى التى يتم تطويرها إما على يد أو بمساعدة متخصصين ومبرجين، حيث يوفر التقارب بين مطوري تلك النظم وبين المتخصصين فهما أعمق فيما يتعلق بطبيعة وخصائص المعلومات وكيفية استخدامها.

2/ سهولة الإستخدام: يجب على مطوري النظم أخذ عدة نقاط في الإعتبار أهمها طبيعة القانونين وحاجاتهم والفرق بينهم وبين محترفي العمل فى مجال تكنولوجيا المعلومات وأمن الشبكات.

3/ المعايير: فهي تساعد على زيادة الدقة والتكامل بين مختلف المؤسسات وتقلل من الأخطاء والتكاليف وترفع من قيمة البحث العلمي وتزيد من تكامل جهود التطوير واستثماراته

4/التحديات الاجتماعية والقانونية: وهي تحديات تتعلق بمدى خصوصية وأمن المعلومات الرقمية، فكلما زادت سهولة الوصول إلى تلك المعلومات زادت أهمية إنشاء المزيد من قواعد ا لأمن والخصوصية التي تحكم عملية استخدام المعلومات وحق الإطلاع عليها.

5/**التكاليف مقابل المميزات:** وهي أهم التحديات الإقتصادية أمام صناعة نظم السجلات الرقمية، فكلما زادت الخواص والمميزات المطلوبة زادت في المقابل تكاليف إنتاجها وتوفيرها، ومن الضروري أن يتم الوصول إلى توازن مناسب بينهما[1] .

سابعا: أمن المعلومات وخصوصيتها[2]

على الرغم من أنه كثيرا ما يستخدم مصطلحا «الخصوصية» و«الأمن» بالتبادل، فإنهما تخصصان مختلفان؛ فأمن المعلومات وخصوصيتها هما تخصصان متميزان مرتبطان معا. ومن أجل الحماية المناسبة للخصوصية، تدعو الحاجة إلى آليات أمنية سليمة. ونظرا لحساسية المعلومات الشخصية التي يتم جمعها، واستخدامها، ومشاركتها في

[1] أمن البيانات الصحية في الأنترنت السحابي/ملف-المريض-السجل-الطبي-للمريض/https://linkitsys.com/ar

[2] Ossama Ahmed Attalla , Is The Legal Protection Of Digital Privacy Enough In Egypt" ? Protection Of Digital Data Privacy ", A Paper Submitted For The Conference Of Cyber Crimes , National Institute Of Intellectual Property April 2020 .

بيئة العمل القانونى، فمن المهم تحديد وتنفيذ الآليات الأمنية المناسبة التي من شأنها حماية البيانات وخصوصية الأفراد[1]. ويجب تحديد متطلبات الأمن والخصوصية واختيار وتنفيذ الضوابط اللازمة خلال مراحل دورة تطوير النظام، وتحديث حماية الأمن والخصوصية حسب الحاجة. ومن المهم أيضا أن يتعاون الأفراد في منظمات أمن المعلومات والخصوصية لإدارة المخاطر الأمنية وحماية الخصوصية.

1: ما الفرق بين الأمان والخصوصية؟[2]

في هذه الحقبة الرقمية التي تعتمد على التكنولوجيا يجب أن يكون الأمان والخصوصية من المطالب الرئيسية. حيث أصبح كل شيءٍ مرتبطًا ببعضه البعض ويمكن الوصول إليه بسهولة، فأغلب بياناتنا ومعلوماتنا الشخصية متاحة للقرصنة والتهديدات الأمنية، لذلك أصبح الجميع بحاجة للحماية والخصوصية ولاسيما الأشخاص الذين يعملون في مجالات الاتصالات. لكن معظمنا لا يدري ما هو الفرق بين الأمان والخصوصية.

ولسوء الحظ أصبحت الخروقات الأمنية شائعة جدًا، فوفقًا لتقرير جرائم الإنترنت لعام 2017 تمت سرقة أكثر من مليار سجل شخصي، وفي الولايات المتحدة وحدها أكثر من 100 مليون أميركي سُرقت سجلاتهم الطبية في عام 2016، وإن دلت هذه الإحصائيات على شيءٍ فإنها تدل على الحاجة الملحة لتعزيز الأمان والخصوصية.[3] وقبل الخوض في مسألة الفرق بين الأمان والخصوصية لا بد من تعريف كل منهما على حدي:

- ✓ **الأمان**:حالة تشير إلى الحرية الشخصية من القوى الخارجية والتحرر من الأخطاء المحتملة والتهديدات. ومثل نظام الأمان المنزلي الذي يحمي أسرتكم، فأمن البيانات يحمي البيانات والمعلومات الشخصية من خلال حمايته لكلمات مروركم ومستنداتكم. وكمثال عن الأمان البرامج المضادة للفيروسات على حاسوبك الشخصي التي تحمي جهازك وتجعل ملفاتك آمنة. ومع تطور التكنولوجيا وُضعت إجراءات صارمة وتدابير لحماية البيانات الرقمية من الوصول غير المصرح به وحماية هذه البيانات من قراصنة الإنترنت والمجرمين الرقميين، وتحاول جميع التدابير الأمنية معالجة هدف واحدٍ من **أهداف الأمان وهي**: حماية السرية والحفاظ على سلامة أصول المعلومات وتعزيز توافر البيانات والمعلومات.
- ✓ **الخصوصية**:هي حق الشخص بالتحرر من الأعين المتطفلة، وهي إحدى المبادئ الأساسية للكرامة الانسانية وتتضمن السرية وحماية المعلومات الحساسة كمعلومات لتعريف الشخصية[4]، وبالتالي من المستحيل تنفيذ برنامج خصوصية مِن دون وجود برنامجٍ أمني [5].

[1] راجع فى ذلك:

- http://www.alkhaleej.ae/alkhaleej/page/aaf7afa4-f9ac-4974-ab6e-cdb1ab5102b8#sthash.jTiWe8R0.dpuf
- https://www.consumersinternational.org/news-resources/news/arabic-news/blog-will-gdpr-be-the-global-standard-for-data-protection-arabic/ للائحة العامة لحماية البيانات: هل ستكون المعيار العالمي لحماية البيانات؟

[2] المهندس/ سعيد عطا الله, ما الفرق بين الأمان والخصوصية , مقال منشور بتاريخ :2020/5/14 على موقع : https://www.arageek.com/l/ما-الفرق-بين-الأمان-والخصوصية

[3] HIV.gov، The Difference between Security and Privacy and Why It Matters to Your Program، من موقع: www.hiv.gov2019-3-7 ، اطّلع عليه بتاريخ

[4] للمزيد حول معنى الخصوصية راجع فى ذلك:

Ossama Ahmed Attalla , Is The Legal Protection Of Digital Privacy Enough In Egypt" ? Protection Of Digital Data Privacy ", A Paper Submitted For The Conference Of Cyber Crimes , National Institute Of Intellectual Property April 2020 .

[5] What's the Difference Between Privacy and Security?، من موقع: www.globalsign.com2019-3-7 ، اطّلع عليه بتاريخ

✓ هذا ولقد نتج عن استخدام الإنترنت تحديات مختلفة لموضوع حماية الخصوصية، وتختلف أنواع القوانين المختصة بالخصوصية في الفضاء الرقمي فهي تتراوح بين حماية البريد الإلكتروني، وفرض قيود على نشر بيانات التواصل الاجتماعي، ومتابعة نشاط متصفح الإنترنت والمخالفات للبيانات المحفوظة. وفيما يلي الأنواع المختلفة لقوانين الخصوصية الرقمية:

✓ **قانون حماية البيانات** :تفرض على الشركات المقدمة لخدمات الانترت والتي تقوم بتخزين معلومات رقمية لعملائها من نشر هذه المعلومات أو مشاركتها مع أطراف أخري دون إفادة من العميل[1].

✓ **قانون مراقبة الاتصالات:** تُقيد مراقبة وسائل الإتصال بالإنترنت، والتي تكون في مجال العمل أو الموجودة في الأماكن العامة أو حتى في المنزل.

✓ **قانون الحماية من جرائم الإنترنت** :تمنع الاستيلاء على الهوية أو سرقة البريد الإلكتروني وكل ما يخص حماية البيانات الشخصية التي يشاركها الفرد أثناء استخدامه للانترنت.

2: كيف يعمل الأمن والخصوصية معا؟

هناك حاجة إلى تدابير أمنية لحماية خصوصية الأفراد. تُعرف التقنيات والأدوات التي تدعم الخصوصية بالتقنيات المعززة للخصوصية، وغالبا ما تتكون من تقنيات أمنية يحمي استخدامها خصوصية الأفراد. ويمكن استخدام التقنيات المعززة للخصوصية لأداء وظائف مثل تمكين الوصول إلى البيانات واستخدامها على نحو ملائم داخليا، ومنع الإفصاح غير الملائم عن البيانات خارجيا. ومع ذلك، فمثلما تستخدم الآليات الأمنية للمساعدة على جهود الخصوصية، فإن بعض تدابير الخصوصية تساعد أيضا في الجهود الأمنية.

المبحث الثاني: الأدلة الرقمية

يحتل عنصر الإثبات مكانة مرموقة في كافة العلاقات والمجالات الشخصية والمدنية والتجارية، وهو الوسيلة الأساسية للحصول على الحقوق وإلزام الآخرين بالوجبات. ومن الناحية العملية ليس للحق أية قيمة عندما يعجز صاحبه عن إثباته، إذ أن إثبات الفعل المولّد للحق هو الذي يعطي هذا الحق فعاليته الكاملة.

والإثبات هو نظام قانوني[2] بحيث لا يُقبل من طرقه ووسائله إلا تلك التي حددها القانون. وقد اعتبر القانون أن بعض هذه الوسائل يتمتع بقوة ثبوتية كاملة لإثبات جميع التصرفات القانونية والوقائع المادية؛ مثل: السند الكتابي (الرسمي أو العادي)، الإقرار، اليمين الحاسمة والقرائن القانونية.

لكن دخول العالم في عصر الثورة الصناعية الرابعة **4.0** ، والتحول إلى الرقمية، أدي إلي تغير مفهوم الإثبات تبعاً لإمكانية إنشاء الحقوق والالتزامات بطرق رقمية، والاستغناء في غالبية الأحيان عن الكتابة الورقية.

ولم يعد بالإمكان سوي الاعتراف بهذا العالم الجديد الذي يقوم علي علم المعلوماتية والتكنولوجيا، وهو يعتمد أسلوباً غير ورقي، مرئياً ومنقولاً عبر الشاشة الرقمية. وقد تم استبدال الملفات الورقية والمخطوطات بالأسطوانات

[1] راجع فى ذلك:

www.dlapiperdataprotection.com., Data Protection Laws of the World

[2] راجع في ذلك: د/عبد التواب مبارك، الدليل الرقمي أمام القاضي المدني، دار النهضة العربية، بدون سنة نشر، ص 5 وما بعدها.

الممغنطة والسندات الرقمية المحفوظة على أسطوانات ضوئية رقمية أو على أقراص ممغنطة، وهي تنتقل من مكان إلى آخر بسهولة وسرعة خارقة من دون أية حاجة للورق.

ولقد أصبحت غالبية الالتزامات والعقود والمعاملات تقوم بالوسائل الرقمية، تبعاً لما يوفره الإنترنت كوسيلة سهلة وفعالة، ومتوافرة للعموم، وتتيح الحصول على المعلومات وحفظها وتبادلها، من دون أن تعترضها الحدود الجغرافية،

المطلب الأول: ماهية الادلة الرقمية[1]

الأدلة الرقمية: والتي تُعرف أحيانًا **بالأدلة الرقمية**[2]، أو **بالأدلة السيبرانية هي**[3] مصطلح يشير إلى المعلومات الإثباتية التي يتم إرسالها أو تخزينها بتنسيق رقمي والتي يمكن استخدامها بعد ذلك في محاكمة أو دعوي قضائية. قبل قبول الأدلة الرقمية[4] من قبل المحكمة، يجب تحديد ما إذا كان هذا الدليل أصيلًا أو ذا صلة أو إشاعات أو ما إذا كان سيتم قبول النسخ أو ما إذا كان يجب تقديم الأصل[5].

إيجابيات وسلبيات الأدلة الرقمية[6]:

فيما يتعلق بموثوقية هذه الأدلة، يعتقد بعض القضاة أن دقة وموضوعية الأدلة الرقمية تجعلها أكثر موثوقية في حين يعتقد قضاة آخرون أن الافتقار إلى الوسائل اللازمة للتحقق من صحة الأدلة الرقمية[7] يجعلها أكثر عرضة للخطر وبالتالي، فهي أقل موثوقية من الأدلة التقليدية عمومًا.

هذا ويبرز العديد من الخبراء التقنيين **بعض الخصائص الإيجابية حول الأدلة الرقمية** فهي: دقيقة، كاملة، واضحة، دقيقة، حقيقية، موضوعية، ومحايدة. في كثير من الحالات، يبدو أن الأدلة الرقمية ضرورية لحل نوع معين من الجرائم. بالنسبة للقضاة، من السهل جمع الأدلة الرقمية وتخزينها وحفظها. بشكل عام. وبالنظر الي النظم

[1] راجع في ذلك

– Mike L. Bridenback, Consultant ,Study of State Trial Courts Use of Remote Technology Final Report, National Association for Presiding Judges and Court Executive Officers, April 2016, p2-27

[2] راجع في ذلك: د. محمد كمال شاهين، حجية الدليل الرقمي في الإثبات الجنائي دراسة مقارنة، المؤتمر العلمي الخامس (الافتراضي) ، كلية الحقوق جامعة السلطان قابوس ، " نظم التقاضي وتحديث قواعد الإثبات "تطوير نظم التقاضي وتحديث قواعد الإثبات" ، ٢٢ ديسمبر ٢٠٢٠ ، ص 4 وما بعدها ، و راجع أيضا : تاريخ آخر دخول : (تاريخ آخر دخول: 2021/1/20)

– https://phys.org/news/2015-03-digital-forensics.html

– https://www.lawgazette.co.uk/news/law-enforcers-struggle-with-electronic-evidence-challenges-/5066471.article

[3] راجع في ذالك: (تاريخ آخر دخول: 2020/11/12)

– http://www.stephenmason.eu/articles/electronic-evidence.html

[4] راجع في ذالك (تاريخ آخر دخول: 2021/1/3)

حول القبول القانوني للأدلة الرقمية :

– https://www.tandfonline.com/doi/abs/10.1080/13600860420002235O8?src=recsys&journalCode=cirl2

[5] راجع في ذالك: (تاريخ آخر دخول: 2021/1/12)

): نتائج دراسة أوروبية: (تاريخ آخر دخول: 2021/1/12)AEECحول مقبولية الأدلة الرقمية في المحكمة (

– https://www.tandfonline.com/doi/full/10.1080/15567280701418049?src=recsys

[6] راجع في ذلك: (تاريخ آخر دخول: 2021/1/12)

– https://www.tandfonline.com/doi/full/10.1080/15567280701418049?src=recsys

[7] حول تفاصيل اكثر عن الأدلة الرقمية، راجع: (تاريخ آخر دخول: 2021/1/12)

– https://en.wikipedia.org/wiki/Digital_evidence

القضائية المقارنة نجد بالمملكة المتحدة، قانون للشرطة والأدلة الجنائية، والذي ينظم جمع "أدلة الكمبيوتر" بطريقة محددة [1]. كما تضمن القانون البلجيكي لجرائم الكمبيوتر بعض التعاليم حول جمع الأدلة التي يمكن تطبيقها أيضًا على الأدلة الرقمية.

وفيما يتعلق بسلبيات الأدلة الرقمية[2] يري أخصائيو القانون أن تحديد القيمة القانونية لهذا النوع من الأدلة يمثل صعوبة بسبب الجهل الحالي بإجراءات معالجة البيانات[3]. وتنشأ هذه الصعوبة بسبب عدم وجود تنظيم مناسب ومنتظم وكذلك عدم وجود فقه متجانس. وبالنسبة لخبراء الكمبيوتر، تتمثل بعض السلبيات في الافتقار إلى الدعم القانوني ونماذج الشهادات، ونقص الفهم الذي أبدته الهيئات القضائية في أوروبا[4]، فضلاً عن التكاليف الباهظة المتعلقة بالحصول على الأدلة الرقمية وتفسيرها[5]، وهي مهمة تستغرق وقتًا كبيرًا. كما لا تشمل المعايير الإجرائية أي إجراء محدد لتنظيم جمع الأدلة الرقمية وحفظها وعرضها في المحكمة. وفقًا لجميع الموثقين الذين تمت مقابلتهم، لا يوجد أي إجراء محدد لحفظ الأدلة الرقمية، والإجراءات الوحيدة التي ذكروها هي تلك الخاصة بإنشاء التوقيعات الرقمية.

-المبادئ التي تؤثر على مقبولية الأدلة الرقمية[6]:

تلعب المبادئ المتعلقة بالفعالية والفائدة والشرعية دورًا مهمًا في التشريعات الأوروبية المختلفة في مجال قبول الأدلة الرقمية. إن الحاجة إلى الحصول على أدلة، والشفافية أثناء جمعها، واحترام حرية التعبير هي مبادئ تنعكس في المعايير في أوروبا، ولكن لها وضع ثانوي فيما يتعلق بقبول الأدلة. **فالمبادئ** التي تؤثر على الأدلة الرقمية هي أساسًا

- **احترام معايير حماية البيانات واحترام سرية الاتصالات وحق حرية التعبير**[7]: وفي الممارسة العملية، يذكر الفقهاء الأوروبيون إن مبادئ الشرعية، وملاءمة الصلة، واستخدام هذه الأدلة لها تأثير أكبر. كما يؤكد الخبراء الفنيون

[1] راجع في ذلك: (تاريخ آخر دخول: 2021/1/12)
https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/handling-of-digital-evidence.html

[2] حول مشاكل الاستخدام في الوثائق الرقمية كدليل في العملية المدنية، راجع: (تاريخ آخر دخول: 2021/1/12)
_ http://aurora.turiba.lv/editor/Conference14/vBook/proceeding/pages/EN030_Simeblyte_Nemeiksis/EN030_Simeblyte_Nemeiksis.htm

[3] راجع في ذلك: (تاريخ آخر دخول: 2021/1/12)
_ https://docplayer.net/10509033-Content-management-for-courts-improve-court-operations-by-reducing-costs-speeding-response-times-and-simplifying-paper-intensive-processes.html

[4] حول مقبولية الأدلة الرقمية في المحكمة: (تاريخ آخر دخول: 2021/1/12
(https://www.tandfonline.com/doi/full/10.1080/15567280701418049?src=recsys

[5] راجع في ذلك: (تاريخ آخر دخول: 2021/1/12)
_ https://www.lawgazette.co.uk/news/law-enforcers-struggle-with-electronic-evidence-challenges-/5066471.article

[6] للتفصيل أكثر راجع في ذلك كلا من : (تاريخ آخر دخول: 2021/1/12)
_ حول المقبولية القانونية للأدلة الرقمية، راجع:
- https://www.tandfonline.com/doi/abs/10.1080/13600860420002235 08?src=recsys&journalCode=cirl2
_ حول صعود الطب الشرعي الرقمي، راجع:
- https://www.lexology.com/library/detail.aspx?g=29828d6d-8396-4070-9424-05ac2e0ecfae
_ حول الأدلة الرقمية ومقبوليتها في المحكمة، راجع:
- https://blog.signaturit.com/en/electronic-evidence-and-its-admissibility-in-court

[7] راجع في ذلك: (تاريخ آخر دخول: 2021/1/12)

على أنهم يتصرفون وفقًا لاحترام الحقوق الفردية. على سبيل المثال، يذكر خبراء الطب الشرعي الرقمي[1] من ألمانيا واليونان احترام معايير حماية البيانات، بينما يسلطون الضوء في فرنسا ولوكسمبورغ وأيرلندا على الحفاظ على السرية. بينما يفضل المتخصصون في إيطاليا والمملكة المتحدة تطوير وظائفهم من خلال المواد المشفرة كمبادئ أساسية. علاوة على ذلك، يذكر خبراء آخرون إن بإمكانهم الاعتماد على الدعم القانوني القادم من كاتب عدل أو شاهد، كما في إسبانيا ورومانيا.

المطلب الثانى-أنواع الأدلة الرقمية[2] والمستندات الرقمية[3]

أولا: المحرر الرقمي[4]، الكتابة الرقمية:

يعرف **المحرر الرقمي** [5]بأنه:" المعلومات والبيانات المسجلة رقميا[6] والتي تم تبادلها رقميا باستخدام نظام معالجة المعلومات عبر وسيط رقمي[7]. " الأمر الذي يمكن القول معه أن المراسلات بين المحكمة والخصوم بحسب التعبير هي محررات رقمية كما في نظام رفع الدعوي E-Filing رقميا.

وبناءا على ما سبق تُعد المحررات الرقمية[8] من قبيل المحررات المعترف بها ولها ذات الحجية المقررة للمحررات الرسمية أو العرفية في أحكام قانون الإثبات في المواد المدنية والتجارية وفي نطاق المعاملات المدنية والتجارية والإدارية.

1. المحررات الرسمية الرقمية[9]:

بحسب تعريف المحرر الرسمي وفقا للمادة العاشرة من قانون الإثبات المصري باعتباره المحرر الذي يثبت فيه موظف عام أو شخص مكلف بخدمة عامة ما تم علي يديه أو ما تلقاه من ذوي الشأن، فإن المحرر الرقمي لن يختلف في تعريفه عن المحرر الورقي إلا مع مراعاة خصوصية التكنولوجيا فيكون هذه العملية يوثق المرسل البصمة الرقمية باستخدام المفتاح الخاص الذي هو بمثابة توقيع بشكل رقمي، ثم يقوم بعملية الإرسال وعند وصول الرسالة إلىالمرسل

_ https://articles.forensicfocus.com/2017/06/29/an-introduction-to-challenges-in-digital-forensics

1 راجع في ذلك كلا من : (تاريخ آخر دخول: 2021/1/12)

حول الطب الشرعي الرقمي، راجع:

_ https://www.researchgate.net/publication/327644306_Digital_Forensics_Review_of_Issues_in_Scientific_Validation_of_Digital_Evidence

[2]راجع فى ذلك المادة (11) من قانون 175 لسنة 2018 .

3 راجع في ذلك :

_ https://www.lawteacher.net/free-law-essays/international-law/can-electronic-documents-be-used-as-evidence-international-law-essay.php

[4] راجع في ذلك : محمد جميل إبراهيم ، اثر التقنيات الحديثة في مجال الدليل الكتابي ، رسالة دكتوراه ، كلية الحقوق ، جامعة الزقازيق، ص135 وما بعدها .

5 راجع في ذلك : عقد البيع عبر الإنترنت ، د. عمر خالد محمد الزريقات ، دراسة تحليلية ، رسالة دكتوراه، ج. عين شمس ، ص ١٩١ .

6 ولقد عرفت المادة الأولي من قانون 175 لسنة 2018 البيانات الرقمية بانها:

(البيانات والمعلومات الإليكترونية: كل ما يمكن إنشاؤه أو تخزينه ، أو معالجته ، أو تخليقه ، أو نقله ، أو مشاركته ، أو نسخه بواسطة تقنية المعلومات : كالأرقام والأكواد والشفرات والحروف والرموز والإشارات والصور والأصوات وما في حكمها) .

7 هذا وقد نصت المادة 13 من قانون 146 لسنة 2019 بتعديل بعض أحكام قانون المحاكم الاقتصادية الصادر بالقانون رقم 120 لسنة 2008 علي تحديد المقصود بالمستند أو المحرر الرقمي انه:

(رسالة بيانات تتضمن معلومات تنشا أو تدمج أو تخزن أو ترسل أو تستقبل كليا أو جزئيا بوسيلة رقمية أو رقمية أو ضوئية أو بغيرها من الوسائل المشابهة. وهو ما يمكن القياس عليه والاستئناس به في مجال إجراءات التقاضي الرقمي أمام القضاء المدني) .

[8] راجع في ذلك : د/ الأنصاري حسن النيداني، القاضي والوسائل الرقمية الحديثة ، مرجع سابق ، ص58 وما بعدها .

[9] راجع في ذلك : محمد جميل إبراهيم ، اثر التقنيات الحديثة في مجال الدليل الكتابي ، مرجع سابق، ص 155 وما بعدها.

إليه يتأكد من صحة التوقيع الرقمي بإرسال نسخة منه إلي الجهة التي أصدرته أو من خلال الشهادة الرقمية التي بعثها المرسل إلي المرسل إليه مع المحرر الرقمي وهو ما يطلق عليه التصديق الرقمي وفي حالة التأكد من صحة التوقيع الرقمي يقوم المرسل إليه بخطوة أخيرة، وهي إعادة حساب البصمة الرقمية ، فإذا نتج عن عملية الحساب بيانات غير بيانات البصمة الرقمية المرسلة، فهذا يعني إنه تم العبث بالمحرر، وتستطيع البصمة الرقمية اكتشاف أي تغيير يلحق بالمحرر الرقمي وتتكرر العملية في كل مرة بين المرسل والمرسل إليه.

إن الشروط العامة لقبول المحرر الرقمي[1] كدليل في الإثبات هي قابلية المحرر الرقمي للقراءة وإمكانية الاطلاع عليه وذلك لتبين ماورد به[2]، والحفاظ علي سلامة بيانات المحرر بما يحميه من أي تغيير أو تحريف، وضمان عدم الاختراق واعتراض المحتوي كدليل رقمي [3]، والمحرر اذا أصبح رقميا في صورة pdf مثلا فإن هذا لا يضمن الحماية بصورة مطلقة ففي العالم الافتراضي مخاطر أيضا وإن كانت مختلفة من حيث الطبيعة والتقنية المستخدمة، لذا اشترط المشرع الفرنسي في م١ من القانون المدني لقبول الكتابة في الشكل الرقمي أن يكون من الممكن تحديد الشخص الذي صدر عنه، وان تحفظ في ظروف من طبيعتها ضمان سلامة المحرر وهو نفسه موقف المشرع المصري والذي نص علي ذلك في قانون التوقيع الرقمي، وقد ورد في م 11 من اللائحة التنفيذية للقانون[4] ضوابط حماية بيانات المحرر، وهي ذاتها – من حيث المبدأ– ذات الآليات الخاصة بالتوقيع الرقمي.

والهدف الأساسي أن يتم حفظ ملفات القضايا وما يتصل بها من بيانات بحالتها وفي ظروف تضمن لها السلامة والبعد عن أي تحريف أو تغيير، وذلك حتى يضمن الرجوع إليها في أي وقت سواء أثناء سير القضية، أو في مرحلة الطعن في الحكم، أو حتى لأغراض الحفظ عموما.

والمحررات الرقمية عبارة عن كل رسالة بيانات تتضمن معلومات تنشأ وتدمج أو تخزن أو ترسل أو تستقبل كليا أو جزئيا بوسيلة رقمية أو رقمية أو ضوئية أو بأية وسيلة آخري مشابهة[5].

[1] راجع في ذلك: د/عبد التواب مبارك ، الدليل الرقمي أمام القاضي المدني ، مرجع سابق ، ص 91 وما بعدها.

[2] راجع في ذلك :

_ https://www.tandfonline.com/doi/full/10.1080/15567280500541462?src=recsys

[3] راجع في ذلك المادة الأولي من جرائم تقنية المعلومات رقم 175 لسنة 2018 .

[4] م ١١ من **اللائحة التنفيذية لقانون التوقيع الرقمي**: (مع عدم الإخلال بما هو منصوص عليه في المواد ٢،٣،٤ يتم من الناحية الفنية ، التقنية كشف أي تعديل أو تبديل في بيانات المحرر الرقمي باستخدام تقنية شفرة المفتاحين (العام والخاص) وبمضاهاة شهادة التصديق الرقمي وبيانات إنشاء التوقيع الرقمي بأصل هذه الشهادة وتلك البيانات أو بأي وسيلة مشابهة) .

5 راجع في ذلك : بدر بن عبدالله الجعفري، بحث بعنوان الإثبات الرقمي في المنازعات التجارية، مقدم للمتلقي العدلي "وسائل الإثبات" الذي نظمته الغرفة التجارية بمدينة الأحساء ، المملكة العربية السعودية، يناير 2013، ص 30.

وهذه البيانات الرقمية تثبت على دعائم رقمية[1] غير ورقية ذات خواص محددة كالأقراص الممغنطة وذاكرة الحاسب الآلي المثبتة والغير مثبتة أو قد تكون مثبتة على دعائم رقمية غير مادية من خلال شبكة الإنترنت بما في ذلك البريد الإلكترونى[2].

وتشمل المحررات الرقمية[3] أيضا السجل الرقمي وهو عبارة عن البيانات التي تنشأ أو ترسل أو تستلم أو تبث أو تحفظ بوسيلة رقمية وتكون قابلة للاسترجاع أو الحصول عليها بشكل يمكن فهمها. **ولقد ايد حكم محكمة النقض[4] الصادر بالطعن12415 لسنة78 ق – جلسة 2018/12/23 حجية** المحررات الرقمية في الإثبات.

- **التوقيع الرقمي وأهمية في الإجراءات القضائية[5]:**

وضع التوقيع على مستند يحتوي على معلومات معينة يعني واقعة **توقيع**، ويأتي التوقيع في صورة علامة خطية خاصة ومميزة يضعها الموقع وتسمح بتمييز شخص الموقع فتنسب إليه شخصيا دون غيره وتعبر عن إقراره بما جاء في المستند[6]. وعرفت الفقرة الثالثة من المادة الأولي من قانون **التوقيع الرقمي** المصري التوقيع الرقمي بإنه (ما يوضع علي محرر رقمي ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها ويكون له طابع منفرد يسمح بتحديد شخص الموقع وتميزه عن غيره).

في بدايات ظهور فكرة التوقيع الرقمي[7] كان التركيز عليها بالأساس لأغراض التجارة الرقمية وعقود البيع الرقمي فنجد قانون الاؤنسيترال النموذجي للتوقيعات الرقمية الصادر عام ٢٠٠١، أي أن التوقيع نظراً لما له من أهمية في الإثبات وله أهمية قصوى في الإجراءات القضائية، إذ يجب الاستيثاق من صحة البيانات وما تقرره المحررات، لما لها من أثر على الإجراءات المتبعة في القضية (الصحة أو البطلان)، وعلي الحكم الصادر من القاضي. لذا يجب ضمان الموثوقية عن طريق نظام قانوني محدد للتوقيع الرقمي وآلية تقنية تضمن تحقق سلامة البيانات.[8]

[1] **دعامة رقمية:** (أي وسيط مادي لحفظ وتداول البيانات والمعلومات الرقمية ومنها الأقراص المدمجة أو الأقراص الضوئية أو الذاكرة الرقمية أو ما في حكمها) . راجع في ذلك المادة الأولي من جرائم تقنية المعلومات رقم 175 لسنة 2018 .

[2] راجع في ذلك: أ.د. عابد فايد عبد الفتاح فايد، القاضي والتنازع بين الأدلة الكتابية التقليدية والرقمية . دراسة مقارنة . بين القانون الفرنسي وقوانين بعض الدول العربية، المؤتمر العلمي الخامس (الافتراضي) ، كلية الحقوق جامعة السلطان قابوس ، " نظم التقاضي وتحديث قواعد الإثبات "تطوير نظم التقاضي وتحديث قواعد الإثبات" ، ٢٢ ديسمبر ٢٠٢٠ ، ص5 وما بعدها

[3] راجع في ذلك: محمد جميل إبراهيم، اثر التقنيات الحديثة في مجال الدليل الكتابي ، مرجع سابق، ص 149

[4] راجع في ذلك : (تاريخ آخر دخول: 2021/1/10)

_ https://www.cc.gov.eg/judgment_single?id=111387601&&ja=270764

[5] راجع في ذلك: د/ الأنصاري حسن النيداني، القاضي والوسائل الرقمية الحديثة ، ص195 وما بعدها .

[6] راجع في ذلك : د. محمد المرسي زهرة ، الحاسب الرقمي ، الإثبات والقانون دراسة حول حجية. مخرجات الحاسب في الإثبات ، مكتبة سعيد عبد الله ، القاهرة ، ١٩٩٢ ، ص ٧٩.

[7] راجع في ذلك: د/عبد التواب مبارك، الدليل الرقمي أمام القاضي المدني، ص 95 وما بعدها.

[8] من أجل مواءمة تشريعاتها مع المعايير الأوروبية، اعتمد المشرع الإيطالي في 23 يناير 2002 مرسوم تشريعي (مرسوم) ينقل التوجيه الأوروبي CE / 93/1999 بشأن التوقيع الرقمي. تعتبر الوثيقة الرقمية الآن بمثابة نسخ ميكانيكي بالمعني المقصود في المادة 2702 من كوديس سيفيلوله نفس الصلة كما في الوثيقة المكتوبة بخط اليد. علاوة علي ذلك، فإن التوقيع الرقمي المرتبط بالمستند الرقمي يعطي نفس التأثير الذي سيكون عليه في العالم الورقي، بقدر ما يطيع التوقيع شروط التوقيع المتقدمة ويضمنه مزود شهادة معتمد.

ويقصد بالموثوقية [1] البيانات التي يتم استقبالها وتتضمن ذات المعلومات التي كانت موجودة بها عند إرسالها، فتصل إلي المرسل إليه (الطرف المستقبل) دون أي تعديل سواء بالإضافة أو الحذف أثناء إرسالها من المرسل إلي المرسل إليه والآلية التي تتحقق بها هي في الأساس التوقيع إذ إنها تضفي علي المحرر نوع من التصديق، ولأغراض الموثوقية يكون التوقيع الرقمي مؤمنًا إذا استوفي الشروط الآتية[2]:

- أن يكون خاص بالموقع وحده
- أن يتم إنشائه بوسيلة تقع تحد سيطرة الموقع وحده .
- أن يضمن الكشف عن أي تعديل لاحق في البيانات.

إلى جانب أن التوقيع الرقمي والسرية في تداول كل ما يخص القضية من أوراق خاصة حال إرسالها من المحكمة إلى الخصوم أو العكس بالنظر إلى الإجراءات في الخصومة ذاتها، فإن الوقوف على حجيتها على درجة كبيرة من الأهمية لأن من المتصور أن تقدم للمحكمة لغرض الإثبات محررات رقمية وأدلة رقمية.

2. التوقيع الرقمي وآثاره القانونية[3] كدليل رقمي[4]:

يعد التوقيع الرقمي أداة تكنولوجية تسمح بضمان صحة وسلامة المستندات الرقمية. وفقًا للائحة الاتحاد الأوروبي رقم 2014/910 والقانون الإسباني للتوقيع الرقمي 2003/59 (يتألف التوقيع الرقمي من أداة قادرة على السماح بالتحقق من أصل وسلامة الرسائل المتبادلة من خلال شبكات الاتصالات السلكية واللاسلكية، مع توفير قواعد لتجنب الرفض أو الطعن في الدليل) بيان دوافع القانون الإسباني 2003/59 بشأن التوقيع الرقمي.

3. ألية ضمان موثوقية التوقيع الرقمي والمحررات الرقمية لضمان حجيتها في الإجراءات القضائية:

يجدر الإشارة إلى أن المشرع المصري في قانون التوقيع الرقمي قد قرر حجية المحررات الرقمية وقبولها في الإثبات علي قدم المساواة مع المحررات الورقية. **وهو ما أيده حكم محكمة النقض الصادر بالطعن12415 لسنة78 ق – جلسة 2018/12/23 بحجية المحررات الرقمية في الإثبات.**

وفي إطار الإجراءات القضائية إذا قام أحد الأشخاص برفع دعوي بتقديم المطالبة القضائية رقميا فإن التوقيع الرقمي هو ما يؤكد صدور هذا التصرف عن هذا الشخص بالذات وإقراره به ونسبته إليه، وبالمثل في إعلان المحكمة (الإعلانات أو الإخطارات اللاحقة لانعقاد الخصومة) لأحد أطراف الخصومة رقميا، أيضا عند إصدار القاضي لمسودة الحكم هل من الممكن أن يغني توقيع القاضي الرقمي عن التوقيع العادي، فضلا عن الاعتراف بكافة هذه الإجراءات فإن "**التوقيع الرقمي المؤمن** " له أهمية قصوى في كل هذه الإجراءات[5].

[1] راجع في ذلك: د. محمد محمد سادات ، حجية التوقيع الرقمي في الإثبات ، رسالة دكتوراه ، مرجع سابق ، ص ٦٩ .

[2] راجع في ذلك: د/ نور خالد عبد المحسن العبد الرازق، حجية المحررات والتوقيع الرقمي في الإثبات، عبر شبكة الإنترنت، رسالة دكتوراه، ج.عين شمس ، ٢٠٠٩ ، ص ١٩٦ ، وراجع أيضا : راجع في ذلك: د/عبد التواب مبارك ، الدليل الرقمي أمام القاضي المدني ، مرجع سابق ، ص 95 وما بعدها.

[3] راجع في ذلك: د/عبد التواب مبارك، الدليل الرقمي أمام القاضي المدني، المرجع السابق، ص. 91 وما بعدها.

[4] راجع في ذلك: د/عبد التواب مبارك، الدليل الرقمي أمام القاضي المدني، المرجع السابق، ص. 70 وما بعدها.

5 راجع في ذلك: د/أسامة أحمد بدر، حماية المستهلك في التعاقد الرقمي، دراسة مقارنة، دار الجامعة الجديد للنشر، 2005، ص. 20، 13 .

إن التركيز على فكرة الموثوقية والرسمية في الأساس يمكن إجماله في نقطتين أساسيتين[1]:

النقطة الأولي: إنه في إطار تطور الإجراءات القضائية والاستعانة بالتكنولوجيا فيها فإن التركيز يكون على ضرورة التثبت من نسبة الورقة / المحرر إلى من صدر عنه وبمعني آخر إيجاد صلة بين الإجراء والشخص الذي صدر عنه الإجراء والوسيلة لذلك هو "التوقيع الرقمي".[2]

النقطة الثانية[3]: أيضا في إطار إجرائي نجد ضرورة بيان ماهية الإجراء ذاته بما يوازن بين الضمانات الإجرائية Le contenu d'acte، والطبيعة الرقمية[4] للوسائل التي يتخذ من خلالها الإجراء وهو ما يوجد له صدد في قانون الإجراءات المدنية الكندي الجديد الصادر في ٢٠ فبراير ٢٠١٤ والذي أعتمد التكنولوجيا بصورة ملحوظة في الإجراءات المدنية، وتناولت م ٩٩ بفقرتها الثلاث هذا الأمر وبصفة خاصة في علاقته بإجراء المطالبة القضائية سواء تم هذا الأخير بإرساله عبر الإنترنت أو تم إيداعه بواسطة المدعي لدي قلم الكتاب مثبت علي دعامة رقمية[5] فحددت في الفقرة الأولي والثانية مضمون الإجراء والبيانات التي يتطلبها من ناحية وهوما يثير شروط المحررات الرقمية [6] وحددت الفقرة الثالثة متطلب التوقيع الرقمي.

[1] أعلنت المحكمة البلجيكية العليا منذ عشر سنوات ما يلي:

'le juge apprécie la culpabilité du prévenu selon son intime الإدانة: il le condamne lorsqu'il a la certitude humaine qu'il s'est rendu coupable du fait mis à sa charge '(Cass، 10 November 1992، Pas، 1992، I، 1247 p}.

ترجمة غير مصرح بها: 'يقدّر القاضي بحرية ذنب المدعي عليه وفقًا لتقديره الشخصي للأدلة ؛ لا يمكن إدانته إلا عندما يكون مقتنعًا بأن المتهم ارتكب فعلًا الجرم الذي حوكم من أجله يتعين علي القاضي أن يزن مدي اعتماده علي الأدلة (خاصة ملاحظاته وبيانات المشتبه فيهم والشهود والخبراء ، وكذلك الوثائق المكتوبة).

وراجع في ذلك أيضا : (تاريخ آخر دخول علي الموقع : 2020/9/22)

_ قانون الإجراءات الجنائية الفرنسي علي الإنترنت:

_ http://www.adminet.com/code/index-CPROCPEL.html

_ قانون الإجراءات الجنائية الإيطالي علي الإنترنت:

_ http://www.camerapenale-bologna.org/codice_procedura_penale/codice_di_procedura_penale_index.htm#cpbo.

[2] راجع في ذلك أيضا : علي سبيل المثال ، القاعدة 96 (استبعاد الأدلة لعدم وجود موثوقية أو تأثير علي نزاهة المحكمة بالوسائل التي تم الحصول عليها) القاعدة 89 ، الفقرة واو (الأصالة) ، القاعدة 92 مكرر أ (ب) (ب) (موثوقية التنفيذ أدلة المحكمة) ، القاعدة 94 مكرر (الخبراء) ، القواعد الإجرائية وقواعد الإثبات ، المحكمة الجنائية الدولية ليوغوسلافيا السابقة ؛ FRE (الولايات المتحدة) المادة السادسة ، التي تحدد أوراق اعتماد الشهود ؛ المادة السابعة ، تحدد مؤهلات الشهود الخبراء وآرائهم ؛ المادة الثامنة ، التي تحدد الاختبارات المتعلقة بالإشاعة خارج بيانات المحكمة المستخدمة في المحكمة ؛ المادة التاسعة ، التي تحدد اختبارات التصديق علي الأدلة.

[3] راجع في ذلك: (تاريخ آخر دخول علي الموقع: 2020/9/22)

_ https://www.tandfonline.com/doi/abs/10.1080/13600860420002235O8?src=recsys&journalCode=cirl

[4] راجع في ذلك: د/ الأنصاري حسن النيداني، القاضي والوسائل الرقمية الحديثة مرجع سابق، ص.178 وما بعدها.

[5] وقد عرفت المادة الأولي من قانون 175لسنة 2018 الدعامة الرقمية بانها:

دعامة رقمية: أي وسيط مادي لحفظ وتداول البيانات والمعلومات الرقمية ومنها الأقراص المدمجة أو الأقراص الضوئية أو الذاكرة الرقمية أو ما في حكمها.

[6] Art.99 Alinéa 1 Canadienne NCPC:« L'acte de procédure doit indiquer sa nature، exposer son objet، énoncer les faits qui le justifient، ainsi que les conclusions recherchées. Il doit indiquer tout ce qui، s'il n'était pas énoncé، pourrait surprendre une autre partie ou soulever un débat imprévu. Ses énoncés doivent être présentés avec clarté، précision et concision، dans un ordre logique et être numérotés consécutivement.».

4. موقف المشرع المصري بشأن التوقيع الرقمي[1]:

إن الهدف من دراسة موقف المشرع المصري في هذا الصدد هو ضمان أكبر قدر من الأمان المعلوماتي للتوقيع الرقمي بما يمنع من التبديل أو التزوير في بيانات المحرر المذيل بالتوقيع الرقمي، عندما قام المشرع المصري بتنظيم أحكام التوقيع الرقمي بموجب القانون الصادر في ٢٠٠٤ فقد أخذ بمبدأ الحياد التكنولوجي (بمعني ألا يتطلب القانون إلزاما باستخدام تكنولوجيا معينة في التوقيع الرقمي تاركا للمتعاملين باستخدام التوقيع الرقمي حرية اختيار التكنولوجيا المناسبة لهم في إطار معاملتهم الخاصة) [2] ويتبدى ذلك من أن المشرع ذكر دائما التوقيع الرقمي دون تخصيص أو ربط بنوع معين، وهو ما يقودنا إلى أن أنواع التوقيع الرقمي [3] وتحديد نوع التوقيع المعتمد علي درجة عالية من الأهمية لأن أثره القانوني يتحدد بقوة الاتصال بين أدوات التوقيع والوثيقة التي سيتم توقيعها والقدرة علي حماية الوثيقة من أي تلاعب، وتنقسم صور التوقيع علي هذا النحو علي أساس درجة الأمان التي يتيحها كل توقيع إلي[4]:

أ. التوقيع بالنقر على لوحة المفاتيح; ب. التوقيع بواسطة الرقم السري، والبطاقة الممغنطة ;ج. التوقيع عن طريق قياس الخواص الحيوية لجسم الإنسان (بصمة الصوت، بصمة العين، بصمة الأسنان) ;د. التوقيع الرقمي.إلا إنه بالرجوع إلى نصوص اللائحة التنفيذية لقانون التوقيع الرقمي والمذكرة الإيضاحية نرى أن المشرع اقتصر على ذكر صورة واحدة هي **"التوقيع الرقمي"**[5]، كما إن كافة الضوابط التقنية التي اشترطها في الاعتراف بالتوقيع لا يحققها إلا التوقيع الرقمي علي نحو ما سيلي بيانه

وما يهمنا في هذا الصدد هو التوقيع الرقمي والذي نوصي بأن يقرر المشرع صراحة اعتماده كوسيلة للتوقيع الرقمي في اطار الإجراءات القضائية فخلافا للمعاملات الخاصة تتعلق إجراءات التقاضي بالنظام العام لاتصالها بتنظيم مرفق القضاء وان يتم ذلك التقرير صراحة دون حاجة إلي أن يستشف من اللائحة التنفيذية [6].

والتوقيع الرقمي هو أكثر صور التوقيع الرقمي ضمانا لأمن وسلامة البيانات[7]، ويعتمد التوقيع الرقمي علي التشفير[8] الذي يحمي صحة وأصالة البيانات، فعن طريق التشفير يتم تحويل الرسائل إلي أشكال غير مفهومة ثم إعادتها إلي أشكالها الأصلية ، ويعبر عن التوقيع الرقمي الذي يعتمد علي التشفير وشهادة التصديق[9] "بالتوقيع الرقمي المتقدم" وقد تطلب المرسوم الصادر من مجلس الدولة الفرنسي رقم ٢٧٢ لسنة ٢٠١٠ بخصوص تطبيق نصوص التوقيع الرقمي، إنه لكي يصدق على التوقيع وصف "المتقدم" أن يستوفي عدة شروط أن يكون التوقيع خاص بالموقع ويتم إنشائه بوسائل تقع تحت سيطرته ورقابته الخاصة، وان يتم التثبت من أن التوقيع يقوم علي استخدام شهادة رقمية

[1] راجع في ذلك: د/ الأنصاري حسن النيداني، القاضي والوسائل الرقمية الحديثة، ص47 وما بعدها .

[2] وقد أخذت بذات المبدأ الولايات المتحدة وإنجلترا، راجع د. محمد محمد سادات، ص ٩٦ .

[3] راجع في ذلك: د./عيسي غسان عبد الله الربضي، القواعد الخاصة بالتوقيع الرقمي، رسالة دكتوراه، ج.عين شمس ، ص ٥٧ وما بعدها.

[4] راجع في ذلك: د/عبد التواب مبارك، الدليل الرقمي أمام القاضي المدني، دار النهضة العربية، بدون سنة نشر، ص 74 وما يليها.

[5] راجع في ذلك: د/ يوسف احمد النوافلة، رسالة دكتوراه بعنوان "الإثبات الرقمي" ، كلية الحقوق ، جامعة الإسكندرية ، 2010 ، ص62 وما يليها.

[6] راجع د. محمد محمد سادات، حجية التوقيع الرقمي في الإثبات، رسالة دكتوراه، المرجع السابق، ص ١١٣–١١٩ .

[7] يقصد بمصطلح سلامة البيانات: (التحقق من أن البيانات التي تضمنتها الوثيقة لم يحدث بها أي تعديل أو حذف سواء لأسباب طبيعية أو عمدية) . راجع في ذلك : د./ محمد محمد سادات. حجية التوقيع الرقمي في الإثبات، رسالة دكتوراه، مرجع سابق، ص ١٩٥.

[8] راجع في ذلك: د/ يوسف احمد النوافلة ، رسالة دكتوراه بعنوان "الإثبات الرقمي" ، مرجع سابق ، ص88

[9] راجع في ذلك : د/ يوسف احمد النوافلة ، رسالة دكتوراه بعنوان "الإثبات الرقمي" ، مرجع سابق ، ص90 وما بعدها.

مؤهلة [1]، وهو نفس موقف المشرع المصري، وباستيفاء تلك المتطلبات يمكن القول أن التوقيع الرقمي والمحرر يعترف بهم القانون ويتمتعوا بأقصى قدر من الأمان[2].

ثانيا: الرسائل النصية (SMS)[3]:

تثير الرسائل النصية التي ترسلها أجهزة الهواتف المحمولة (اللاسلكية) التساؤل حول إمكانية قبولها كدليل في الإثبات.

وقد قبلت محكمة النقض الفرنسية في حكمها الصادر بتاريخ 2007/5/23 الرسائل النصية كدليل في الإثبات، ولكن بشرط أن يكون الحصول عليها قد تم بطريقة لا خداع فيها.

وقد اعتد المشرع المصري برسائل البريد العادي كدليل للإثبات وفقا لنص المادة (16) من قانون الإثبات، وقد سوي المشرع بينها وبين المحررات العرفية في الإثبات، فالرسالة وإن لم يقصد بها أن تكون دليلا كتابيا فإنها تعد كذلك ما دامت موقعا عليها، وقد تكون حجة على المرسل بصحة المدون فيها إلى أن يثبت العكس بالطرق المقررة قانونا للإثبات.

فإذا لم يكون موقعا عليها من المرسل فإنها تعتبر مبدأ ثبوت بالكتابة متى كانت مكتوبة بخطه أما إذا لم تكن بخطه فلا قيمه لها في الإثبات.

أما بالنسبة للرسائل النصية[4] الصادرة من الهواتف المحمولة (SMS) فإنها دائما وأبدا لا تكن موقعه من مرسلها وبالتالي فإنه فيما يتعلق بهوية كاتب أو مرسل الرسالة النصية فإنه من حيث المبدأ يمكن القول بأن الرسالة النصية تعد صادرة من قبل صاحب الخط الهاتفي الذي تم إرسال هذه الرسالة منه إلا إذا ثبت غير ذلك، ذلك أن صاحب الخط هو الذي لجأ بداية إلى المشغل للخطوط الخلوية واقتني أو ملك خط الهاتف الذي من خلاله تم إرسال الرسالة النصية.

[1] راجع في ذلك :

être créée par des moyens - aux exigences suivantes، en outre،Art. 1/ 2 : « Signature électronique sécurisée : une signature électronique qui satisfait : contrôle exclusif ،garantir avec l'acte auquel elle s'attache un lien tel que toute -que le signataire puisse garder sous son être propre au signataire modification ultérieure de l'acte soit détectable

.last visited 22 October 2017 0000404810https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT00

[2] وما يتكفل بضمان تحقيق ذلك أيضا بجانب كل ما سبق اذا ما تعدي شخص واتلف محرر او دليل رقمي فأنه يطبق عليه المادة 17 من قانون 175 لسنة 2018

.

[3] راجع في ذلك: د/ أحمد محمد عبدالرحمن، "نظرة حول نظام التقاضي الرقمي في مصر" ، مرجع سابق ، ص 24 .

4 راجع في أمن الرسائل الفورية:

https://docplayer.net/680438-Instant-messaging-security.html

ثالثا: الإثبات بالبريد الإلكترونى[1]:

تعد رسائل البريد الإلكترونى[2] ضمن الوسائل الحديثة التي تصلح كدليل في الإثبات[3]. وكما سبق وأشرنا فإنه لا بد من التأكد من هوية الشخص المرسل، وفي هذا الصدد فإنه لابد من الإشارة إلى أن البريد الإلكترونى لا يمكن أن يكون دليلا كافيا لإثبات هوية المرسل لذلك لابد من إضافة ما يفيد ويؤكد هذه الجهة المرسلة وذلك من خلال مركز الخدمات التقنية للاتصالات الذي يقوم بدور توزيع البريد الإلكترونى، ويمكن اشتراط أن تكون رسالة البريد الإلكترونى موقعه من مرسلها حتى يمكن الاعتداد بها كوسيلة من وسائل الإثبات.

وأخيرا فإنه لكي تقوم الكتابة الرقمية مكان الكتابة التقليدية في مجال الإثبات فإنه يجب أن تكون هذه الكتابة قابلة للقراءة أولا حتى يتم التعرف على محتوي المحرر وأن تكون هذه الكتابة غير قابلة للتعديل حتى لا يغير أحد الأطراف محتواها دون علم الطرف الآخر وأن يتم حفظ هذه المحررات حتى يتم الرجوع إليها عند الحاجة لذلك[4].

- **حجية البريد الالكترونى في الإثبات[5]:**

لقد كانت الكتابة على الورق هي الأصل الغالب، إلا أن المحرر لم يكن في أي وقت مقصورًا على ما هو مكتوب علي ورق وحده، وكل ما يتطلبه المشرع للإثبات هو ثبوت نسبة المحرر إلي صاحبه، فلا ارتباط قانونًا بين فكرة الكتابة والورق، ولذلك لا يُشترط أن تكون الكتابة علي ورق بالمفهوم التقليدي ومذيلة بتوقيع بخط اليد، وهو ما يوجب قبول كل الدعامات الأخرى – ورقية كانت أو رقمية أو أيًا كانت مادة صنعها – في الإثبات. البريد الإلكترونى (e - mail) هو وسيلة لتبادل الرسائل الرقمية بين الأشخاص الذين يستخدمون الأجهزة الرقمية من أجهزة كمبيوتر أو هواتف محمولة أو غيرها، تتميز بوصول الرسائل إلي المرسل إليهم في وقت معاصر لإرسالها من مُرسِلها أو بعد برهة وجيزة، عن طريق شبكة المعلومات الدولية (الإنترنت) أيًا كانت وسيلة طباعة مستخرج منها في مكان تلقي الرسالة، وسواء اشتملت هذه الرسائل علي مستندات أو ملفات مرفقة Attachments أم لا. ولقد أجازت القوانين الوطنية والاتفاقيات الدولية للقاضي استخلاص واقعتي الإيجاب والقبول - في حالة التعاقد الرقمي - من واقع تلك الرسائل الرقمية دون حاجة لأن تكون مفرغة كتابيًا في ورقة موقعة من طرفيها، ذلك أن هذه الرسائل يتم تبادلها عن طريق شبكة المعلومات الدولية (الإنترنت)، ولذلك فإن أصول تلك الرسائل - مفهومة علي أنها بيانات المستند أو المحرر الرقمي - تظل محفوظة لدي أطرافها - مهما تعددوا - المُرسِل والمُرسَل إليهم داخل الجهاز الرقمي لكل منهم، فضلًا عن وجودها بمخزنها الرئيسي داخل شبكة الإنترنت في خادمات الحواسب Servers للشركات مزودة خدمة البريد الإلكترونى للجمهور. وفي كل الأحوال، فإنه في حالة جحد الصور الضوئية، فلا يملك مُرسِل رسالة البريد الإلكترونى أن يقدم أصل المستند أو المحرر الرقمي، ذلك أن كل مستخرجات الأجهزة الرقمية، لا تعدو أن تكون نسخًا ورقية مطبوعة خالية من توقيع طرفيها، ومن ثم فإن المشرع وحرصًا منه علي عدم إهدار حقوق المتعاملين من خلال تلك الوسائل الرقمية الحديثة

[1] راجع في ذلك: د/ أحمد محمد عبدالرحمن، "نظرة حول نظام التقاضي الرقمي في مصر" ، مرجع سابق ، ص 24 .

[2] - البريد الرقمي: (وسيلة لتبادل رسائل رقمية علي عنوان محدد، بين أكثر من شخص طبيعي أو اعتباري، عبر شبكة معلوماتية، أو غيرها من وسائل الربط الرقمية، من خلال أجهزة الحاسب الآلي وما في حكمها) . المادة الأولي من قانون تقنية المعلومات رقم 175 لسنة 2018 .

[3] راجع في ذلك: د/ يوسف احمد النوافلة، رسالة دكتوراه بعنوان "الإثبات الرقمي" ، مرجع سابق ، ص126 وما بعدها.

[4] راجع في ذلك: د. محمد محمد سادات. حجية التوقيع الرقمي في الإثبات، رسالة دكتوراه، ج. المنصورة، ٢٠١٠ ، ص ١٩٥ .

[5] راجع في ذلك: د/ يوسف احمد النوافلة، رسالة دكتوراه بعنوان "الإثبات الرقمي" ، مرجع سابق ، ص 129 وما بعدها .

حال عدم امتلاكهم لإثباتات مادية علي تلك المعاملات، قد وضع بقانون تنظيم التوقيع الرقمي ولائحته التنفيذية الضوابط التي تستهدف التيقن من جهة إنشاء أو إرسال المستندات والمحررات الرقمية وجهة أو جهات استلامها وعدم التدخل البشري والتلاعب بها للإيهام بصحتها، ولا يحول دون قبول الرسالة الرقمية كدليل إثبات مجرد أنها جاءت في شكل رقمي، ولهذا فإنها تكون عصية علي مجرد جحد الخصم لمستخرجاتها وتمسكه بتقديم أصلها؛ إذ إن ذلك المستخرج ما هو إلا تفريغ لما احتواه البريد الإلكترونى، أو الوسيلة الرقمية محل التعامل، ولا يبقي أمام من ينكرها من سبيل إلا طريق وحيد هو المبادرة إلي الادعاء بالتزوير وفق الإجراءات المقررة قانونًا تمهيدًا للاستعانة بالخبرة الفنية في هذا الخصوص.

رابعا: الإثبات بالتسجيلات الرقمية (المسموعة والمرئية)[1]

وهي التسجيلات التي يتم ضبطها وتخزينها بواسطة الآلة الرقمية ويقصد بها تسجيل المحادثات الهاتفية سواء صوتيا أو فيديو وسواء أكانت هاتفيا أو على الإنترنت من أحد الأطراف.

ولقد ثار خلاف بين الفقه حول شرعية استعمال التسجيل الصوتي كدليل إثبات وانقسموا إلى عدة آراء منهم من يؤيد الأخذ بهذه الوسيلة في الإثبات بصفة مطلقة ومنهم من يعارض الأخذ بها ومنهم من يحيط هذا الدليل بشروط معينة ومنهم من يجيز التسجيلات الصوتية إذا كان التسجيل مقدما للتدليل على براءة المتهم ولو كان الحصول عليه بطريق غير مشروع.[2]

ولقد حسم المشرع في قانون الإجراءات الجنائية الأمر فأجاز إجراء تسجيلات لأحاديث جرت في مكان خاص متي كان لذلك فائدة في ظهور الحقيقة ولقد ربط ذلك بشروط معينة هي أن يكون هذا الحديث له فائدة في ظهور الحقيقة وأن يكون في جناية أو جنحة معاقب عليها بالحبس لمدة تزيد على ثلاثة أشهر ويجب أن يكون هذا التسجيل بناء علي أمر مسبب ولمدة لا تزيد علي ثلاثين يوما قابلة للتجديد لمدة أو مدد آخري مماثلة[3]، وهو ما يمكن الاستئناس به فى مجال القضاء المدنى.

خامسا: الإثبات بشهادة الشهود[4]

ترتب أدلة الإثبات على درجات تأتي في أعلاها الإثبات الخطي أي بالكتابة وبعده مباشرة الإثبات الشفهي أي شهادة الشهود أو البينة، إلا إنه لا تقبل الشهادة للإثبات إلا في أحوال محددة نص عليها القانون.

ويقصد بشهادة الشهود قيام شخص من غير أطراف الخصومة بالإدلاء بأقواله أمام مجلس القضاء حول حقيقة وقائع تصلح محلا للإثبات نشأ عنها حق أو مركز قانوني لغيره.[5]

[1] راجع في ذلك : د/ يوسف احمد النوافلة ، رسالة دكتوراه بعنوان "الإثبات الرقمي" ، مرجع سابق ، ص 28 ، ص 244 وما بعدها وراجع أيضا : https://www.lexology.com/library/detail.aspx?g=29828d6d-8396-4070-9424-05ac2e0ecfae

[2] راجع في ذلك : د/ أحمد محمد عبدالرحمن، "نظرة حول نظام التقاضي الرقمي في مصر" ، مرجع سابق ، ص25 .

[3] لدراسة أعمق في المسائل القانونية التي تعتمد علي التعامل مع الأدلة الرقمية وحماية الخصوصية ، انظر "القيود القانونية لحماية البيانات والخصوصية والشخصية في التعامل مع الأدلة الرقمية" ماريا فيرونيكا بيريز-Asinari المجلة الدولية للقانون الحاسبات و Technology، Vol 18، No 2، 2004، 250–231 pp.

[4] راجع في ذلك : د/ أحمد محمد عبدالرحمن، "نظرة حول نظام التقاضي الرقمي في مصر" ، مرجع سابق ، ص25 .

[5] راجع في ذلك : نظر Ken Chasse ، "السجلات التي تنتجها الكمبيوتر في إجراءات المحكمة" ، (1994) الملحق ياء لوقائع المؤتمر القانوني الموحد لكندا ، الاجتماع السنوي 1994 ، المحفوظ في :www.law.ualberta.ca/alri/ulc/94pro/ e94j.htm

وللمحكمة السلطة التقديرية بشأن الاستجابة لطلب الخصوم لسماع شهادة الشهود كدليل للإثبات من عدمه، فقد تري المحكمة أن المستندات والوثائق المكتوبة كافية للفصل في النزاع أو أن الواقعة التي سيتم الاستعانة بشأنها بالشهود قد أصبحت واضحة للمحكمة، كما قد تري أن الجوانب الموضوعية والقانونية للدعوي لم تكتمل وإنه يجب الاستعانة بشهادة الشهود من أجل أيضاح تلك الأمور، وللمحكمة أن تطلب من تلقاء نفسها سماع شهادة الشهود دون طلب من الخصوم وذلك إذا وجدت أن هناك فائدة جمة من سماعهم.

وقد أجاز قانون الإثبات المصري في حالة عدم استطاعة الشاهد الحضور إلمقر المحكمة التي تنظر النزاع لأسباب جدية تمنعه من **ذلك كالمرض الشديد مثلا**، ففي مثل هذه الحالة يمكن للمحكمة أن تندب أحد قضاتها للانتقال للشاهد وسماع أقواله وإثباتها في محضر تحقيق يوقعه القاضي المنتدب والكاتب.

كما أجازت المادة (90) من قانون الإثبات المصري بصفة استثنائية أن تكون الشهادة مكتوبة إذا كانت طبيعة الدعوي تسمح بذلك، ويجب أن يكون محرر الشهادة ممن تتوافر فيه الشروط العامة التي يجب أن تتوافر في الشاهد، أما فيما يخص شكل الشهادة فيجب أن تكتب الأقوال وتوقع وتؤرخ من الشاهد ويجب أن يتم توثيقها أمام مكتب التوثيق والشهر العقاري.

ويثور التساؤل في هذا الصدد في حالة تعذر حضور الشاهد لمقر المحكمة لظروف قهرية خارجة عن إرادته حول مشروعية استجواب الشهود في العالم الافتراضي عبر الإنترنت عن طريق استخدام تقنية الفيديوكونفرانس وذلك متي ثبت استحالة أو عدم ملائمة مثول الشاهد بنفسه أمام المحكمة، ومدي تأثير هذا الإجراء على احترام مبدأ المواجهة وحق الدفاع عن طريق ضمان تقديم كل طرف لبيناته علي أكمل وجه؟

ويري البعض أن مناقشة الشهود وإن جاز إجراؤها في ظل التقدم التكنولوجي بطريقة رقمية عبر شبكة الإنترنت أو ما شابه[1] من وسائل الاتصالات اللاسلكية إلا أن مناقشة الشهود بالطريقة التقليدية هي الطريقة الأكثر قوة ووضوحا في استجلاء وجه الحقيقة نظرا لإمكانية مشاهدة تعبيرات وجه الشاهد ودرجة تأثره ومدي اتزانه وغيرها من العوامل التي قد تؤثر على تقدير صحة الشهادة على الواقعة محل الخلاف.

إلا أننا نري إنه في حالة تعذر حضور الشاهد لمقر المحكمة لسفره للخارج أو لمرضه الشديد أو إقامته بالمنزل أو المستشفى أو لوجود كوارث طبيعية كفيضان وغيره يستحيل معها مثول الشاهد بنفسه أمام المحكمة فإن إجراء استجواب الشهود عبر الإنترنت عن طريق استخدام تقنية الفيديوكونفرانس أو أي وسيط رقمي آخر سيتم استحداثه.

أما في حالة ما إذا كان الشاهد مقيما بالخارج فإن كان مصريا فإنه يمكن استدعائه عن طريق السفارة المصرية بالدولة التي يقيم بها ويحضر في موعد الجلسة المحدد لمقر السفارة المصرية ويتم الاتصال بالسفارة من قبل المحكمة أثناء انعقاد الجلسة عبر تقنية الفيديو كونفرانس وسماع شهادة الشاهد بمقر السفارة المصرية وكذلك الحال بالنسبة لغير المصريين بعد أن تتم مخاطبة البعثة الدبلوماسية للبلد التابع لها وأخذ موافقتها على سماع شهادته بمقر السفارة المصرية بالخارج.

[1] راجع في ذلك : د/ يوسف احمد النوافلة ، "الإثبات الرقمي" ، رسالة دكتوراه ، مرجع سابق ، ص 247 وما بعدها ، وراجع أيضا : طارق بن عبد الله بن صالح العمر ، أحكام التقاضي الرقمي ، رسالة دكتوراه ، ص299 .

ومن ثم فإن سماع شهادة الشهود عن بعد عبر تقنية الفيديوكونفرانس هو وسيلة احتياطيه يمكن اللجوء إليها في حالة الضرورة بعد تعذر اللجوء إلى استدعاء الشخص المطلوب سماع شهادته أو تعذر إرسال إنابة قضائية للسلطة القضائية إلى موطن الشخص المطلوب سماع شهادته فعند استنفاد هاتين الوسيلتين وعدم إمكانية استخدامهما فإنه يجوز للسلطات القضائية أن تطلب القيام بهذا الإجراء عبر تقنية الفيديوكونفرانس أو أي وسيط رقمي آخر يتم استحداثه في هذا الأمر[1].

المطلب الثالث: تحديات قبول الأدلة الرقمية

تواجه الأدلة الرقمية التحدي، في أنها تقنية فبعض القوانين لا تعترف بالأدلة التي تم الحصول عليها من خلال هذه المعاملة، وتعامل كدليل ثانوي بسبب طبيعتها. ومن الأمثلة علي ذلك القسم 4 من قانون العقود (تنزانيا) .[2] **والتحديات الرئيسية** [3]التي ستواجه مقبولية الأدلة الرقمية (عبر الإنترنت) في طبيعتها في مجال المصادقة لوجود العديد من الفيروسات علي شبكة الإنترنت والتي من الممكن أن تصيب الملفات بالإضافة إلي الهاكر وهو ما سيكون معه من الصعب على محكمة القانون أن تتأكد من عدم وصول أي متسللين إلي المعلومات أو التأكد من عدم إصابة الملفات التي يتم الحصول عليها رقميًا.

- **هل الأدلة الرقمية مقبولة؟** [4]

تقضي المحاكم أحيانًا بعدم قبول الأدلة الرقمية[5] نظرًا لأنه قد تم الحصول عليها دون إذن من الشخص المعني. ففي العديد من النظم القضائية، تعتبر أوامر القبض ضرورية لأخذ أي أجهزة رقمية والتحقيق فيها، وقد يؤدي ذلك إلى ظهور مشكلات، خاصة في الحالات التي يتم فيها تحديد أدلة على وجود جريمة أثناء التحقيق في جريمة أخري.

- **آليات قبول الأدلة الرقمية في المحكمة:**

يستخدم واحد وتسعون بالمائة من البالغين على الإنترنت اليوم شكلاً من أشكال الاتصال الرقمي بشكل منتظم في حياتهم اليومية. وبالتالي، أصبحت الأدلة الرقمية جزءًا كبيرًا من العديد من القضايا المدنية والجنائية؛ ومع ذلك، هناك معايير محددة لتحديد مقبولية الأدلة الرقمية.

تم تدوين قواعد الإثبات الفيدرالية (FRE)، وكذلك القواعد الفيدرالية للإجراءات المدنية (FRCP)، بقصد توجيه المحاكم -المدنية والجنائية -لآلية قبول الأدلة. في حين تم تطوير FRCP وFRE لإملاء الإجراءات في المحاكم

[1] راجع في ذلك: (تاريخ الدخول :2021/2/13)
_ https://www.tandfonline.com/doi/full/10.1080/15567280701418049?src=recsys

[2] راجع في ذلك: (تاريخ الدخول :2021/2/13)
_ https://www.lawteacher.net/free-law-essays/international-law/can-electronic-documents-be-used-as-evidence-international-law-essay.

[3] راجع في ذلك: (تاريخ الدخول :2021/2/13)
_ https://blog.signaturit.com/en/electronic-evidence-and-its-admissibility-in-court

[4] راجع في ذالك: (تاريخ الدخول :2021/2/13)
– https://www.mailxaminer.com/blog/admissibility-of-electronic-evidence-in-court

[5] راجع في ذلك: (تاريخ الدخول :2021/2/13)
– https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/digital-evidence-admissibility.html

الفيدرالية، حيث اعتمدت العديد من محاكم الولايات قواعد تعكسها عن قرب. كما أن قانون السوابق القضائية ، وكذلك الآراء الصادرة عن المحاكم ، توجه الأطراف في تحديد قبول الأدلة.

- **الأدلة الرقمية والقانون:**

في المملكة المتحدة، تم استخدام قانون PACE لعام 1984 لتأسيس وتقييم الأدلة في المحكمة ولكن هذا القانون ينطبق على إنجلترا وويلز وليس إسكتلندا. تم تطبيق CMA لعام 1990 (بصيغته المعدلة بموجب قانون الشرطة والعدل لعام 2006) عند ظهور قضايا جرائم الكمبيوتر في محاكم المملكة المتحدة. ويتبع الفاحصون عادةً المبادئ[1] التوجيهية التي تصدرها رابطة كبار ضباط الشرطة (ACPO) لتوثيق الأدلة وسلامتها[2]. تم تحديثها إلى الإصدار 5 في أكتوبر 2011 عندما تم استبدال الأدلة المستندة إلى الكمبيوتر بالأدلة الرقمية التي تعكس تطور التحقيق في حوادث أمن المعلومات في سياق أوسع. وهذه المبادئ هي:

المبدأ 1: يجب ألا يغير أي إجراء تتخذه وكالات إنفاذ القانون ، الأشخاص العاملون في تلك الوكالات أو وكلائهم ، البيانات التي يمكن الاعتماد عليها لاحقًا في المحكمة; **المبدأ 2:** في الحالات التي يجد فيها الشخص أنه من الضروري الوصول إلي البيانات الأصلية ، يجب أن يكون ذلك الشخص مختصًا بالقيام بذلك ويكون قادرًا علي تقديم أدلة تشرح أهمية أفعالهم والآثار المترتبة عليها;**المبدأ 3:** يجب إنشاء والحفاظ علي سجل لجميع العمليات المطبقة علي الأدلة الرقمية; **المبدأ 4:** يتحمل الشخص المسؤول عن التحقيق المسؤولية الكاملة عن ضمان التقيد بالقانون وهذه المبادئ.

يتم قبول هذه المبادئ التوجيهية على نطاق واسع في محاكم إنجلترا وإسكتلندا، لكنها لا تشكل شرطًا قانونيًا وإنما استخدامها طوعي.

- **القواعد الفيدرالية لقبول الأدلة الرقمية[3] :**

طبقت العديد من المحاكم في الولايات المتحدة قواعد الإثبات الفيدرالية على الأدلة الرقمية بطريقة مماثلة للوثائق التقليدية، على الرغم من وجود اختلافات مهمة مثل عدم وجود معايير وإجراءات ثابتة. بالإضافة إلى ذلك، تميل الأدلة الرقمية إلى أن تكون أكثر ضخامة، وأكثر صعوبة في التدمير، وتعديلها بسهولة، وتكرارها بسهولة، وربما تكون أكثر تعبيرية، ومتاحة بسهولة أكبر، وفي ديسمبر 2006، تم سن قواعد جديدة صارمة داخل القواعد الفيدرالية للإجراءات المدنية التي تتطلب الحفاظ على الأدلة المخزنة رقميًا والكشف عنها. فغالبًا ما تتعرض الأدلة الرقمية للهجوم بسبب أصالتها نظرًا للسهولة التي يمكن بها تعديلها.

تستخدم العديد من التطبيقات والمواقع الرقمية والأجهزة الرقمية خدمات التخزين السحابية. المستخدمين وبالتالي، يمكن تخزين البيانات كلياً أو على شكل أجزاء بواسطة العديد من مقدمي الخدمات المختلفين في خوادم في

[1] راجع في ذلك: (تاريخ الدخول :2021/2/13)

– https://en.wikipedia.org/wiki/Digital_evidence Tech. 5 (2011)

[2] راجع في ذلك: (تاريخ الدخول :2021/2/13)

– https://www.bcs.org/content-hub/presenting-digital-evidence-to-court

[3] راجع في ذلك: (تاريخ الدخول :2021/2/13)

– ISO / IEC 27037 : Cybercrime Module 4 on Introduction to Digital Forensics

مواقع متعددة ولهذا السبب، يعد استرداد البيانات من هؤلاء أمرًا صعبًا.[1] وتختلف إجراءات التجميع تبعًا لنوع الجهاز الرقمي والموارد العامة والخاصة حيث توجد الأدلة الرقمية (علي سبيل المثال، أجهزة الكمبيوتر والهواتف والوسائط الرقمية والسحابة الرقمية؛ لكل منها طريقة للمعالجة في **الطب الشرعي الرقمي** وخاصة فيما يتعلق بالوسائط المتعددة والفيديو والجوال .[2]

تقوم العديد من **محاكم الولايات المتحدة** الآن بتطبيق قواعد الإثبات الفيدرالية علي الأدلة في شكل رقمي بطريقة مشابهة تمامًا للطريقة التي يتم بها تطبيقها علي الأعمال الورقية التقليدية، ومع ذلك تم الاعتراف بالاختلافات من حيث الإجراءات والمعايير المعمول بها. الأدلة الرقمية هي أيضًا أكثر ضخامة ويصعب تدميرها فضلاً عن تكرارها أو تعديلها بسهولة أكبر. أدخلت القواعد الفيدرالية للإجراءات المدنية قواعد جديدة تتطلب الكشف عن جميع الأدلة المخزنة رقميًا وحفظها. علي الرغم من أن الأدلة الرقمية تتعرض للهجوم بشكل متكرر بسبب وجود مشاكل محتملة في أصالتها [3]، إلا أن المحاكم بدأت الآن في رفض هذه الحجج ما لم يكن هناك دليل علي أنه تم التلاعب بالأدلة.

وفي المملكة المتحدة، أصبحت سجلات أجهزة الكمبيوتر التي تُسمع بالسمع مقبولة في عام 1995 من خلال تعديل قانون الأدلة المدنية لعام 1968 بسبب عدم وجود اعتراضات من جانب أطراف على هذه الأدلة علي مدار فترة زمنية، مما يشير إلي قبولها بين عامة الجمهور.

وفي الهند، جاء التغيير في المواقف مع تعديل قانون الأدلة الهندي في عام 2000. تم إدخال القسمين A و B في الفصل المتعلق بالأدلة الوثائقية. ينص القسم A على أنه يجوز قبول محتويات السجلات الرقمية كدليل إذا تم الامتثال للمعايير المنصوص عليها في القسم .B تنص المادة B علي أنه يجب اعتبار المستندات، مما يجعلها دليلًا أساسيًا، إذا كان الكمبيوتر الذي أنتج السجل قيد الاستخدام بانتظام، فالمعلومات التي يتم إدخالها في الكمبيوتر كانت جزءًا من الاستخدام المنتظم للكمبيوتر وكان الكمبيوتر يحتوي علي سجل كان يعمل بشكل صحيح. وينص كذلك على أن جميع مخرجات الكمبيوتر تعتبر منتجة بواسطة الكمبيوتر نفسه، سواء تم إنتاجه بشكل مباشر أو غير مباشر، سواء بتدخل بشري أو بدونه. يلغي هذا البند مفهوم الأدلة الحاسوبية على أنه سماع.

النتائج:

هذا وبعد ان عرضنا بالمبحث الاول **للاكتشاف الإلكترونى من حيث** ماهيتة ومتطلباته، والذكاء الاصطناعي بمجال الاكتشاف الإلكترونى، وتحديات الاكتشاف الإلكترونى. كما عرضنا **بالمبحث الثانى للأدلة الرقمية من حيث** ماهيتها ، وأنواعها، وتحديات قبول الأدلة الرقمية يتضح الآتى:

[1] لمزيد من المعلومات، انظر موقع: Cybercrime Module 7 حول التعاون الدولي ضد الجريمة السيبرانية وقد آثرنا الإشارة دون الإفاضة لعدم اتساع المجال لذالك .

[2] راجع في ذلك: (تاريخ الدخول :2021/2/13)

– https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/handling-of-digital-evidence.html

[3] وللوقوف علي المقبولية القانونية للأدلة الرقمية راجع في ذلك:

– https://www.tandfonline.com/doi/abs/10.1080/13600860420002235 08?src=recsys&journalCode=cirl20(تاريخ آخر دخول علي الموقع : 2021/1/8)

- ✓ يتيح الجمع بين التعرف على الأنماط البشرية الطبيعية ودعم قدرات التعلم الذاتي للذكاء الاصطناعي للمحامين القدرة على استخراج المعلومات ذات الصلة بشكل أسرع وأسهل من أي وقت مضى.
- ✓ يعد اعتماد تقنية الذكاء الاصطناعي حاليًا وسيلة لاكتساب مزايا زيادة الإنتاجية والكفاءة، ومع تطور التكنولوجيا قد لا يمر وقت طويل قبل أن تصبح التزامًا أخلاقيًا كأداة ليس هناك سبب وجيه لعدم استخدامها.
- ✓ من أجل الحفاظ على أمن المعلومات يجب تدبّر الآتي:

1. ستكون هناك عولمة للخصوصية، تكون فيها مبادئ ممارسة المعلومات متسقة نسبيا في جميع أنحاء العالم، مع زيادة المساءلة وتشديد جهود الإنفاذ.
2. توقع نشوء اقتصاد من المعلومات المفتوحة التي تتغلغل عبر الحدود الجغرافية، حيث يطلع على البيانات أعداد متزايدة من الأشخاص، ومن ثم سيكون من الضروري زيادة الشفافية وتحسين توعية مستهلكي البيانات على مستوى العالم.
3. إن أهم ما قد يحافظ على خصوصية الأفرد الرقمية ليس فقط تشريع قانوناً ولكن أيضا ضمان تطبيقه بالإضافة لقابليته للتعديل بناء على ما قد يجد من انتهاكات تمس الخصوصية الرقمية.

التوصيات:

هذا وقد المحنا فى ثنايا البحث الى عدد من التوصيات:

- لقد كان تقاطع الذكاء الاصطناعي والقانون موضوع بحث ومناقشة لمدة خمسين عامًا على الأقل لكن تطوير ونشر الذكاء الاصطناعي آخذان في التسارع مع ظهور "عصر جديد للذكاء الاصطناعى فعلى الرغم من قيود الذكاء الاصطناعي، وربما بسببها:

1. يجب على المحامين النظر في كيفية تأثير صعود الذكاء الاصطناعي على واجباتهم الأخلاقية.
2. يجب على المتخصصين القانونيين عمومًا تعلم كيف يمكنهم الاستفادة من الفرصة الآن لتحسين تقديم الخدمات القانونية عبر العمليات والتقنيات الجديدة وضمان التطوير الأخلاقي للذكاء الاصطناعي وبذلك، سيكونون أكثر قدرة على التأقلم مع التغييرات القادمة في السوق القانوني.

- ✓ يجب تطبيق سياسات صارمة للتحكم بالوصول للمعلومات والبيانات.
- ✓ يجب تطبيق سياسات المراجعة المستمرة للتأكد من جودة عملية الحماية والخصوصية.
- ✓ **يجب** دمج تدريب الاكتشاف الإلكترونى والادلة الرقمية في كليات الحقوق والتعليم القانوني على موضوعات تشمل:
- ✓ احتضان مستقبل التكنولوجيا القانونية لتجنب التخلف عن الركب.
- ✓ دورات اكتشاف رقمية منفصلة أو موضوع تكامل أو معسكر تدريب
- ✓ مواكبة الأشخاص الذين تمثلهم ثقافيًا وتقنيًا.
- ✓ يجب تنظيم محدد على الصعيدين الوطني والدولى يوفر الأمن القانوني للادلة الرقمية بكافة أنواعها.

- ✓ يجب التدريب المستمر والمتخصص لجميع القانونيين لمعرفة كيفية المضي قدما في جمع وتخزين الأدلة الإلكترونية والحفاظ على قيمتها الإثباتية أمام المحكمة عند الحاجة.
- ✓ يجب تنفيذ بروتوكولات لحماية الحقوق الأساسية أثناء جمع الأدلة الإلكترونية وحفظها وعرضها.
- ✓ يجب الوفاء باتفاقية بودابست بشأن الجريمة السيبرانية (مجلس أوروبا).
- ✓ يجب تحقيق تعاون أفضل بين الدول في مجال جمع الأدلة الإلكترونية وحفظها.

وفي النهاية لا يخالجني شك في أن هذه الدراسة المتواضعة قد اعتراها بعض الأخطاء، وعذري فى ذلك انني بشر، يصيب ويخطأ، فالكمال لله وحده سبحانه، والخطأ والقصور هما من سمات الإنسان مهما أبدع وأتقن وجد واجتهد، وغاية ما ينشده كل باحث في عمله، هو تجويد هذا العمل، ومحاولة إتقانه فحسب، فإن كنت قد قاربت ما أنشده أو شارفت عليه فهذا فضل من الله ونعمه وحسبي ان اردد فى ذلك قوله تعالى "**وما توفيقي الا بالله**، والشكر فيه لكل من علمنى حرفا ، وإن كانت الآخرى فحسبى أن أردد فى ذلك قوله تعالى "**وقل رب زدنى علما** " .

تم بحمد الله وفضله وتوفيقه،،،

المركز الديمقراطي العربي
للدراسات الاستراتيجية، الاقتصادية والسياسية
Democratic Arabic Center
for Strategic, Political & Economic Studies

المؤتمر الدّولي العلمي الافتراضي بعنوان:

الجرائم الإلكترونية في الفقه الإسلامي والقانون الوضعي

Cybercrime in Islamic jurisprudence and positive law

رئيس المركز الديمقراطي العربي: أ. عمار شرعان

مدير النشر: د. أحمد بوهكو

رقم تسجيل الكتاب

VR .3383- 6628 B

جوان 2022


الدراسات الإستراتيجية والسياسية والإقتصادية
D.A.C
المركز الديمقراطي العربي