جامعـــة كربـــلاء
كلية القانـون
الفرع العام

الجرائم الناشئة عن التطور التكنولوجي وأثرها في السياسة الجنائية

أطروحة مقدمة إلى مجلس كلية القانون ـ جامعة كربلاء

وهي جزء من متطلبات نيل شهادة الدكتوراه في فلسفة القانون العام

كتبت بواسطة الطالب

أحمد صباح عبدالكريم

بـــإشراف

أ. د. علي حمزة عسل الخفاجي

مارس / 2023 م شعبان / 1444 هـ

بسم الله الرحمن الرحيم

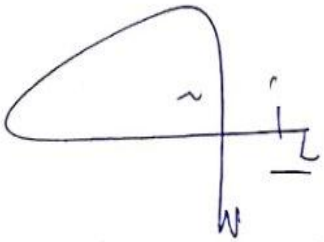
{ قُلۡ هَلۡ نُنَبِّئُكُم بِٱلۡأَخۡسَرِينَ أَعۡمَٰلًا * ٱلَّذِينَ ضَلَّ سَعۡيُهُمۡ فِي ٱلۡحَيَوٰةِ ٱلدُّنۡيَا وَهُمۡ يَحۡسَبُونَ أَنَّهُمۡ يُحۡسِنُونَ صُنۡعًا * أُوْلَٰٓئِكَ ٱلَّذِينَ كَفَرُواْ بِـَٔايَٰتِ رَبِّهِمۡ وَلِقَآئِهِۦ فَحَبِطَتۡ أَعۡمَٰلُهُمۡ فَلَا نُقِيمُ لَهُمۡ يَوۡمَ ٱلۡقِيَٰمَةِ وَزۡنٗا }

((صدق الله العظيم))

سورة الكهف الآيات (103، 104، 105)

إقرار المشرف

أشهد أن اطروحة الدكتوراه الموسومة بـــــ (الجرائم الناشئة عن التطور التكنولوجي وأثرها في السـياسـة الجنائية) المقدمة من قبل الطالب (أحمد صـباح عبد الكريم) إلى مجلس كلية القانون – جامعة كربلاء بوصـــفها جزء من متطلبات نيل درجة الدكتوراه في القانون العام قد جرت تحت إشرافي ورشحت للمناقشة ... مع التقدير .



التوقيع :

الأسم : أ.د. علي حمزة عسل الخفاجي

الدرجة العلمية : استاذ

الاختصاص : القانون الجنائي

جامعة كربلاء – كلية القانون

إقرار المقوم اللغوي

أشهد أني قرأت أطروحة الدكتوراه الموسومة بـ (**الجرائم الناشئة عن التطور التكنولوجي وأثرها في السياسة الجنائية**) المقدمة من قبل الطالب (**أحمد صباح عبدالكريم**) إلى مجلس كلية القانون – جامعة كربلاء، وقد وجدتها صالحة من الناحتين اللغوية والتعبيرية، بعد أن أخذ الطالب بالملاحظات المسجلة على متن الاطروحة .

مع التقدير ...

التوقيع :

الأسم : أ.م.د. عبد الكريم خالد عناية

الاختصاص العام : لغة عربية

الاختصاص الدقيق : النحو

إقرار لجنة مناقشة دكتوراه

نحن رئيس لجنة المناقشة وأعضائها نُقر أننا اطلعنا على هذه الاطروحة الموسومة بـ(الجرائم الناشئة عن التطور التكنولوجي و أثرها في السياسة الجنائية), وناقشنا الطالب (احمد صباح عبدالكريم) في محتواها, وفيما لها علاقة بها, ونعتقد إنها جديرة بالقبول لنيل درجة الدكتوراه في القانون / فرع القانون العام وبدرجة (جيد جداً) .

التوقيع :

الاسم: أ.د.ضياء عبدالله عبود

(رئيساً)

التاريخ: 23/ 2 / 2023

التوقيع :

الاسم: أ.د. عادل يوسف الشكري

(عضواً)

التاريخ: / / 2023

التوقيع :

الاسم: أ.د. احمد حمد الله احمد

(عضواً)

التاريخ: / / 2023

التوقيع :

الاسم: أ.د. عادل كاظم سعود

(عضواً)

التاريخ: / / 2023

التوقيع :

الاسم : أ.م.د. حيدر حسين علي

(عضواً)

التاريخ : / / 2023

التوقيع :

الاسم : أ.د. عـــــلي حمزة عسل

(عضواً ومشرفاً)

التاريخ : / / 2023

صادق مجلس كلية القانون / جامعة كربلاء على قرار لجنة المناقشة

التوقيع:

أ.د. باسم خليل نايل السعيدي

عميد كلية القانون / جامعة كربلاء

التاريخ: / / 2023

((الإهداء))

إلى . . .

- بكل حب وفخر أهدي هذا الجهد إلى والدي ّ ووالدتي أمد الله في عمرهما . . .
- إلى زوجتي وأولادي (حفظهم الله)
- إلى من أرفع بهم رأسي أهلي وإخوتي ، وكل من يعز على قلبي .
- إلى بلدي العظيم والشامخ العراق .
- إلى كل عراقي كان همه العراق أولاً وضحى وسعى من أجل النهوض بوطننا الحبيب .

الباحث

شكر وتقدير

بسم الله خير الأسماء والذي بشكره تزيد نعمه على عباده، والحمد الله على عظيم نعمه وفضله ومنه علينا والصلاة والسلام على أشرف خلقه أجمعين السراج المنير نبينا محمد (صلى الله عليه والّه وصحبه وسلم).

أتقدم بجزيل الشكر والتقدير والامتنان إلى الأب والأستاذ الفاضل المشرف (الأستاذ الدكتور علي حمزة عسل) لقبوله الإشراف على كتابة الأطروحة وإبداء النصح والإرشاد والتوجيه السديد الذي لا إنقطاع له، والذي كان له الأثر الايجابي في إظهار الأطروحة على ما هي عليه .

كما يطيب لي ويسرني كثيرًا وأنا على يقين أنَ كلمات الشكر لا تفي بحقهم ولكن من باب رد الجميل والعرفان لهم اساتذتي في السنة التحضيرية سائلاً المولى أن يمن عليهم بتمام الصحة والعافية، ويحفظهم ذخراً للمسيرة العلمية .

كما وأتقدم بوافر الشكر والإمتنان والثناء الجميل الى كلية القانون – جامعة كربلاء عمادةً، وكادراً تدريسياً، وموظفين، لما يبذلونه من جهود، بغية تسهيل الصعوبات، وإزالة العقبات أمام الطلبة الباحثين والمساعدة لهم في كل ما يحتاجونه من أساسيات لإكمال البحث ومتطلباته، خدمة لبلدنا العظيم .

الباحث

الملخص

ان انتشار وتوسع إطار الجرائم الإلكترونية أصبح امراً واقعاً في ظل الثورة المعلوماتية والتطور الهائل في وسائل الاتصال الحديثة إلاّ ان هنالك مشكلات موضوعية واجرائية تثيرها الجرائم الإلكترونية على الصعيدين التشريعي والعملي.

وهذا البحث يهدف إلى معالجة مدى النقص التشريعي لمواجهة ومكافحة الجرائم الإلكترونية، فكانت الدراسة مقارنة مع بعض التشريعات العربية الحديثة وايضا مع التشريع الفرنسي والامريكي، فقد تناولنا في الباب الاول مدى الحماية الموضوعية المقررة في ظل التطور التكنولوجي والتقني الذي يعيشه العالم في الوقت الحاضر، ومن ثم تناولنا في أصل هذا الموضوع ماهية الجريمة الإلكترونية، فضلا عن اثر هذا التطور التكنولوجي وما نتج عنه من استخدام سلبي أثرّ بشكل خطير على السلامة الجسدية سواء من ناحية المساس المادي لسلامة الجسد أم على الصعيد المعنوي والنفسي والبيئي، إذ يعد الحق في السلامة الجسدية سبباً أساسيا يهدف إليه المشرع الجنائي لضمان حمايته، وقد تبين للباحث أن هنالك فرقاً كبيراً فيما بين الجرائم التقليدية والجرائم الإلكترونية، فالأخيرة تتميز بكونها جرائم ذات طبيعة خاصة، فهي من الجرائم الناعمة والتي يصعب إثبات دليل ارتكابها وتتبعها، وكذلك تمتاز بكونها من الجرائم التي ترتكب عبر الحدود وبسرعة وسهولة فائقة، ويصعب التفتيش عن أدلة تفيد إثبات الواقعة الاجرامية، وكذلك حاولنا دراسة وتوضيح أنماط ودوافع وأسباب ارتكاب الجريمة الإلكترونية، وتبين لنا أن أغلب مرتكبي هذه الجرائم هم من فئة الشباب المراهقين ويمتازون بالخبرة والذكاء في مجال الاجهزة التقنية الحديثة، ومن ثم تناولنا البحث في **الباب** الثاني عن الحماية الاجرائية وآليات التحقيق والتفتيش في الجرائم الإلكترونية في ظل التطور التكنولوجي، وكان موضوع البحث يتكلم عن آليات البحث والتحري عن الدليل الإلكتروني، وما هي الصعوبات التي تواجه الاجهزة المختصة في إثبات الجريمة الإلكترونية سواء على الصعيد المحلي أم الدولي، وكذلك بحثنا آليات التحقيق الابتدائي في هذه الجرائم، وما هي الوسائل الحديثة التي يمكن الاستعانة بها في مجال إثبات الجريمة الإلكترونية ومتابعة المتهم بواسطة الرقابة الإلكترونية ومدى الاختلاف فيما بين وسائل التحقيق في الجرائم التقليدية والجرائم الإلكترونية.

وقد خرج الباحث بعدد من النتائج ومن أهمها، أن النصوص التقليدية في القوانين الجزائية لا يمكن ان تعالج ظاهر تفشي الجرائم الإلكترونية في ظل هذا التطور التكنولوجي والتقني الواسع والسريع، وكذلك توصلنا إلى أن هذه الجرائم الناشئة عن إستخدام التكنولوجيا والإنترنت لها طبيعة من نوع خاص على خلاف الجرائم التقليدية. فضلا عن أن التطور التكنولوجي قد أسهم في تطوير السياسة الجنائية العمومية في بعض البلدان الأوربية والعربية بشكل متواضع تقريبا. وذلك من خلال تشريع سياسة قانونية تواكب التطور الذي يعيشه العالم، على الصعيد الاقتصادي والاجتماعي والسياسي .

قائمة المحتويات

الموضوع	رقم الصفحة
المقدمة	5 - 1
الباب الأول : السياسة الجنائية ومدى الحماية الجنائية الموضوعية في ظل التطور التكنولوجي	127 - 6
الفصل الأول : ماهية السياسة الجنائية وارتباطها التطور التكنولوجي	57 - 8
المبحث الأول : ماهية السياسة الجنائية	31 - 8
المطلب الأول : مفهوم السياسة الجنائية	22 - 9
الفرع الأول : تعريف السياسة الجنائية	12 -9
الفرع الثاني : السياسة الجنائية في ظل الاتفاقيات الدولية	22 - 12
المطلب الثاني : مدى ملائمة مبادئ التجريم والعقاب لمقتضيات السياسة الجنائية	31 - 22
الفرع الأول: أثر السياسة الجنائية في التجريم	27 - 24
الفرع الثاني : أثر السياسة الجنائية في العقاب	31 - 27
المبحث الثاني : الدور التكنولوجي واثره في السياسة الجنائية	57 - 32
المطلب الأول : التنظيم القانوني للتطور التكنولوجي	44 - 32
الفرع الأول : الطبيعة القانونية للتطور التكنولوجي	36 - 32
الفرع الثاني : الضوابط القانونية والأخلاقية للتطور التكنولوجي	40 - 36
الفرع الثالث : أثر التطور التكنولوجي في السياسة الجنائية	44 - 40
المطلب الثاني : دور السياسة الجنائية في مواجهة جرائم التكنولوجيا	57 - 44
الفرع الأول : مواجهة الجريمة المنظمة العابرة للحدود الوطنية	52 - 44
الفرع الثاني : تطور الجهود الجنائية التشريعية في مواجهة الجرائم الإلكترونية	57 - 52

الفصل الثاني : مظاهر الحماية الجنائية الموضوعية في ظل التطور التكنولوجي	127 - 58
المبحث الأول : تأثير التطور التكنولوجي على حق الانسان في السلامة الجسدية	88 - 58
المطلب الأول : ماهية حق الانسان في السلامة الجسدية	76 - 59
الفرع الأول : مفهوم حق الانسان في السلامة الجسدية	66 - 59
الفرع الثاني : حق الانسان في السلامة الجسدية في قانون العقوبات	71 - 66
الفرع الثالث : حق الانسان في السلامة الجسدية في قانون أصول المحاكمات الجزائية	76 - 71
المطلب الثاني : اثر التطور التكنولوجي على حق الانسان في سلامة جسده	88 - 76
الفرع الأول : الأثر السلبي للتكنولوجيا على حق الانسان في سلامة جسده	79 - 77
الفرع الثاني : دور السياسة الجنائية لحماية الانسان في ظل التطور التكنولوجي	88 - 79
المبحث الثاني : أثر التطور التكنولوجي في ظهور الجرائم الإلكترونية	127 - 89
المطلب الأول : ماهية الجرائم الالكترونية	98 -89
الفرع الأول مفهوم الجريمة الالكترونية	96 - 89
الفرع الثاني : خصائص الجريمة الالكترونية	98 -97
المطلب الثاني : دور السياسة الجنائية في حماية الانسان من الجرائم الناشئة عن التطور التكنولوجي	127 - 98
الفرع الأول : الجرائم الإلكترونية الماسة بالأمن الاسري	115 - 99
الفرع الثاني : جرائم الدخول غير القانوني للنظام الإلكتروني	127 - 115
الباب الثاني : مظاهر تأثير التطور التكنولوجي على السياسة الجنائية الإجرائية	232 - 128
الفصل الأول : الدور الإلكتروني في السياسة الجنائية	180 - 130
المبحث الأول : الوسائل الإلكترونية وأثرها في الإثبات الجنائي	162 - 131
المطلب الأول : مفهوم الوسائل الإلكترونية	139 - 131

الفرع الأول : التعريف بالوسائل الإلكترونية	137 - 132
الفرع الثاني : صعوبة فهم الدليل المتحصل من الوسائل الإلكترونية	139 - 137
المطلب الثاني : انواع الدليل الإلكتروني وإشكالية قبوله	162 - 140
الفرع الأول : انواع الأدلة المتحصلة من الوسائل الإلكترونية ووسائل اثباتها	150 - 140
الفرع الثاني : إشكالية قبول الأدلة المتحصلة من الوسائل الإلكترونية	162 - 151
المبحث الثاني : أثر التطور التكنولوجي على الإثبات الجنائي	180 - 162
المطلب الأول : أثر التطور التكنولوجي في المعاينة الإلكترونية	170 - 162
الفرع الأول : المعاينة في الجرائم الإلكترونية	164 - 163
الفرع الثاني : صعوبات إجراءات المعاينة الإلكترونية وتحصيل الدليل	170 - 164
المطلب الثاني : أثر التطور التكنولوجي في التفتيش الإلكتروني	180 - 171
الفرع الأول : مفهوم التفتيش وإسبابه	173 - 171
الفرع الثاني : مدى قابلية الأنظمة التكنولوجية والتقنية للتفتيش	180 - 174
الفصل الثاني : أثر التطور التكنولوجي على اجراءات التحقيق والمحاكمة	232 - 181
المبحث الأول : مظاهر تأثير التطور التكنولوجي على مرحلة التحقيق الابتدائي	208 - 181
المطلب الأول : مراقبة المتهم والتحقيق في الجريمة الإلكترونية	202 - 181
الفرع الأول : مفهوم المراقبة والتحقيق في الجرائم الإلكترونية	186 – 181
الفرع الثاني : طرق وآلية تطبيق المراقبة الإلكترونية اثناء التحقيق	202 - 186
المطلب الثاني : الوسائل التقنية الناتجة عن التطور التكنولوجي في مجال السمعيات والمرئيات	208 - 203
الفرع الأول : التنصت ومراقبة المكالمات وأجهزة الكمبيوتر	206 – 203
الفرع الثاني : الوسائل المرئية الإلكترونية	208 - 206

المبحث الثاني : مظاهر تأثير التطور التكنولوجي على مرحلة المحاكمة	232 - 209
المطلب الأول التنظيم القانوني لمرحلة المحاكمة الإلكترونية	224 - 209
الفرع الأول : متطلبات المحاكمة الجزائية الإلكترونية	212 -210
الفرع الثاني : القانون الواجب التطبيق في الجرائم الإلكترونية	222 - 212
الفرع الثالث : ضمانات المحاكمة الإلكترونية	224 - 222
المطلب الثاني : تقنيات التقاضي عن بعد في ظل التطور التكنولوجي	232 - 224
الفرع الأول : مفهوم التقاضي عن بُعد	227 - 225
الفرع الثاني : الأساس القانوني للتقاضي عن بُعد	232 - 227
الخاتمة :	239 - 233
المصادر	265 - 240
Abstract	i - ii

المقدمة

المقدمة

أولًا: التعريف بموضوع الدراسة :

يعيش العالم اليوم وسط أكبر عمليات النهضة في مجال التقنية عرفها الإنسان، وإذ تُعد جرائم التقنية العالية نتائج طبيعية لبيئة التطور العالمي، والتي يعيش فيها الإنسان المعاصر، ويشكل الحاسب الآلي أساس هذه البيئة الجديدة. ورغم المزايا الهائلة التي تحققت وتتحقق كل يوم بفضل التطور التكنولوجي على جميع الأصعدة، وفي شتى ميادين الحياة المعاصرة؛ فإن هذه الثورة التكنولوجية المتنامية صاحبتها في المقابل جملة من الانعكاسات السلبية الخطيرة جراء سوء استخدام هذه التقنية المتطورة، والانحراف عن الأغراض المتوخاة منها، أدت في تفشي طائفة من الظواهر الإجرامية المستحدثة، ألا وهي: ظاهرة الإجرام الإلكتروني.

فقد إرتبط ظهور الجرائم الإلكترونية كنوع جديد من الجرائم ذات الطبيعة الفنية والتقنية نتيجة التطور في مجال تكنولوجيا المعلومات والإتصالات، وإستخدام الوسائط الإلكترونية في شتي مجالات الحياة، على إعتبارها سلوكاً غير مشروع يتصل بالمعلومات المخزنة في جهاز الحاسب الآلي، أو بواسطة شبكة الإنترنت، والتلاعب بها، بقصد إلحاق الضرر بالمُجنى عليه، أو الحصول على ربح غير مشروع لصاحبه.

ولا شك أن تأثير التطور التكنولوجي قد شمل كل مناحي الحياة الإنسانية، إذ يُعد التطور التكنولوجي مقياس التقدم بين الدول لتلبية المصالح العامة للدولة والمصالح الخاصة للأفراد، ولتحقيق تلك المعادلة يتضح لنا جليًا أن حق الدولة في التطور التكنولوجي يقابله التزامها بحماية حقوق الإنسان؛ الحق في الحياة، والحق في الصحة، والحق في السلامة الجسدية،... إلخ. الأمر الذي يقتضي تدخل السياسة الجنائية بالتشريع لنسج الحماية القانونية اللازمة بمعالجة العجز عن التكييف القانوني لما ينتج من آثار سلبية للتكنولوجيا على حقوق الإنسان.

ومن ثمّ باتت الحاجةُ مُلحّةً وضروريةً إلى وضع سياسة جنائية رشيدة تستند على تدريب وتأهيل أجهزة العدالة الجنائية لمكافحة الظواهر المستحدثة، والحد قدر المستطاع من خطورتها. فضلًا عن ضرورة قيام الدول بتطوير تشريعاتها الجنائية أو التعديل عليها؛ لمواكبة التقدم والتطور التكنولوجي. إذ إن الجرائمَ الإلكترونية ليست مجردَ جرائمَ تقليديةٍ بثوبٍ جديدٍ؛ وانما لها طبيعتها الخاصّةِ المميّزةِ لها عن الجريمة التقليدية، نتيجة للتطوّر والاختلاف في وسائلها المستخدمة، فالجهات المُكلفة في البحث والتحري عن الجريمة والجناة اعتادت على التعامل مع الجرائم بصورتها التقليدية، ممّا أثارَ تحدّيًا أمامَ تلك الجهات في أنَّها في سباقٍ مستمرٍّ مع الزمن لمواكبة التطور، فضاقت النصوصُ العقابيّةُ التقليديّةُ عن استيعاب هذه الجرائم، ولم تكن النصوص الإجرائية أفضلَ حظًا منها، الأمر

الذي سهّل على مرتكبيها الإفلات من العقاب، فالجاني في هذا النوع من الجرائم شخصٌ يتمتّع بذكاء غير عادي، ويمتلك أدوات المعرفة التقنية التي تُمكّنه من استغلالها في إرتكاب الجرائم.

لذلك يأتي هذا البحث لكي يُبين أثر التطور التكنولوجي في السياسة الجنائية، وذلك من خلال إيضاح اتجاهات علم السياسة الجنائية التشريعية التي توجب على المشرع أن يرسم له الخطة التشريعية الجنائية في سبيل وضع قواعد خاصة لمواجهة التطور التكنولوجي.

ثانيًا: أهمية البحث، وأسباب اختياره:

إن لموضوع البحث أهمية متزايدة من الناحية العلمية والعملية، فالسياسة الجنائية في مقام الدراسة تعني مجموعة المبادئ التي توجه المشرع الجنائي في دولة ما حال وضعه التشريع الجنائي المتعلق بمكافحة الإجرام الإلكتروني، ومن ثم يثور التساؤل حول دور السياسة الجنائية إزاء الطبيعة القانونية المعقدة لتلك الجرائم، وما هي الخيارات المحددة لمواجهتها؟ وما هي الحلول لمواجهة القصور التشريعي؟.

فلا شك أن التكييف الجنائي التقليدي يعجز عن استيعاب بعض الجرائم؛ كجريمة ذاتية مستقلة، كالإيذاء المبهج، أو تعاطي المخدرات الرقمية التي تُحدث تأثيرًا على الحالة المزاجية يُحاكي تأثير ألمار جوانا وغيرها من المخدرات التقليدية، والتنمر الإلكتروني، وكذلك الابتزاز الإلكتروني في نصوص قانونية مستقلة أمرًا تستدعيه مقتضيات العدالة وطبيعتها القانونية الخاصة، فضلًا عن ضرورات المكافحة المثلى لهذه الظاهرة.

لذا بات على المشرع سرعة تجريم تلك الأفعال المُستجدة ووضع لها العقوبات الرادعة، كما أصبحت الدول مطالبة بالتفكير في إعادة النظر في سياساتها الجنائية المرتبطة بهذا التقدم التكنولوجي، وذلك بإيجاد خطط وأساليب تتجاوب وتطور الجريمة المرتبطة بالتقدم التكنولوجي. بل إن هذه الدول تُعد استراتيجيتها الجنائية المتطورة من خلال إيجاد وسائل جديدة للتعامل مع بعضها في إطار تتبع المجرمين وملاحقتهم أينما حلوا وارتحلوا، وأن توجد إطارًا جديدًا للتعاون المثمر في هذا المجال خصوصًا وأن آليات التعاون الدولي التقليدية أصبحت متجاوزة لما يكتنفها من تعقيد في الإجراءات وبطء في التنفيذ.

وفي المقابل فإن الطبيعة القانونية المُعقدة لمثل تلك الجرائم تضع السلطة التشريعية أمام خيارات محددة لمواجهتها، وذلك إما بتشريع "قانون خاص" يستوعب مختلف تلك الجرائم، أو تقنينها بشكل مناسب في قانون العقوبات وقانون أصول المحاكمات الجزائية.

ثالثًا: الدراسات السابقة :

لا شك أن موضوع التطور التكنولوجي والجرائم المتعلقة به يُعّد من المواضيع الحديثة كليًا، ومن ثم فإن البحث فيه لا يخلو من الصعوبات، وتتمثل الأخيرة بقلة البحوث العلمية التي لها علاقة مباشرة بموضع دراستنا، وقد وجدة بعض الجهود ذات الصلة بموضوع بحثنا، ومن أبرز هذه الدراسات ما يأتي:

1. حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت، دار النهضة العربية، القاهرة، 2009 .
2. خالد حسن أحمد لطفي، آليات التحقيق الجنائي في جرائم تقنية المعلومات، دار الفكر الجامعي، الاسكندرية، 2020 .
3. على عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الإبتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث، 2011.
4. أبراهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، اطروحة دكتوراه، جامعة مولود معمري – تيزي وزو، كلية الحقوق والعلوم السياسية، 2018
5. سعود علي عبدالله اللوغاني، السياسة الجنائية في مكافحة الجريمة الإلكترونية، أطروحة دكتوراه، جامعة الشارقة، كلية القانون، 2016 .

رابعًا: إشكالية البحث وتساؤلاته:

من المسلم به أن التطور التكنولوجي قد أفرز لنا ظواهر إجرامية جديدة مستجدة تقرع في جنباتها أجراس الخطر لتنبه مجتمعات العصر الراهن لحجم المخاطر وهول الخسائر الناجمة عن تلك الظواهر الإجرامية.

لذلك تبرز إشكالية هذا البحث من خلال تحقيق الموازنة بين متطلبات التكنولوجيا ومقتضيات الحفاظ على حقوق الإنسان، من خلال تدخل السياسة الجنائية لتشريع نصوص التجريم وفرض العقوبات اللازمة للحماية من آثارها السلبية، وذلك على النحو الآتي بيانه:

1- تحديد الآثار السلبية للتكنولوجيا الحديثة وما ينتج عنها من جرائم.
2- تقييم الجهود الوطنية والدولية للسياسة الجنائية في قدرتها على الحماية من الآثار السلبية للتطور التكنولوجي.
3- مدى نجاح السياسة الجنائية الحديثة في التصدي لتلك الظواهر الناتجة عن التطور التكنولوجي.؟ وهل من الممكن الاكتفاء بالقوانين التقليدية ؟
4- عدم وجود قانون في التشريع العراقي ينظم الجرائم الالكترونية .
5- صعوبة التفتيش الالكتروني لما يمثل تعدي على الخصوصية الفكرية وحماية الحق في الحياة الخاصة، بالإضافة إلى صعوبة إثبات الدليل الالكتروني عند ارتكاب الجريمة.

خامسًا: منهج البحث:

نعتمد في هذا البحث على المنهج التحليلي الاستقرائي، وذلك من خلال جمع المعلومات المتعلقة بموضوع البحث ودراستها وتكييفها من الناحية الفقهية وفقًا للقواعد الجزائية مع تحليل النصوص التشريعية لمجوعة من القوانين المقارنة المعنية بموضوع البحث، وذلك بالتركيز على النصوص الخاصة والتي تمثل أثر التطور التكنولوجي في السياسة الجنائية في القانون العراقي وبعض قوانين الدول العربية وكذلك كل من القانون الفرنسي والامريكي، وكذلك الوقوف على أحكام واجتهادات القضاء من خلال القرارات القضائية المعززة للجوانب الفقهية والنظرية فيه، مع الاستعانة بأحكام القضاء الجزائي العراقي والمصري والفرنسي، ومن ثم تحقيق أهداف البحث.

سادسا : خطة البحث:

لدراسة موضوع البحث، من جوانبه المتعددة؛ فإنه من الضروري ابتداءً بيان مفهوم السياسة الجنائية وتوجهاتها بصدد جرائم تكنولوجيا المعلومات، وكذلك التعرف على أنماط تلك الجرائم المستحدثة، مع إيضاح أثر ذلك التطور على السياسة الجنائية. لذا يتطلب الأمر تقسيم هذا البحث، وذلك من خلال خطة هيكلية تألفت من بابين، وذلك على النحو الآتي:

نبحث في الباب الأول: السياسة الجنائية ومدى الحماية الجنائية الموضوعية في ظل التطور التكنولوجي، وقد قسمنا دراستنا في هذا الباب لفصلين، بحثنا في الفصل الأول ماهية السياسة الجنائية وارتباطها التطور التكنولوجي، وخصصنا الفصل الثاني لدراسة مظاهر الحماية الجنائية الموضوعية في ظل التطور التكنولوجي. **أما في الباب الثاني:** سنحاول أن نبين مظاهر تأثير التطور التكنولوجي على الحماية الجنائية الإجرائية، وكذلك نقسم الباب الثاني لفصلين على النحو الاتي، نبحث في الفصل الأول الدور الإلكتروني في السياسة الجنائية، وندرس في الفصل الثاني أثر التطور التكنولوجي على إجراءات التحقيق والمحاكمة، ثم خاتمة البحث التي ستتضمن أهم الإستنتاجات والمقترحات التي سنتوصل اليها بعون الله تعالى ومنه التوفيق والسداد.

الباب الأول

السياسة الجنائية ومدى الحماية الجنائية الموضوعية في ظل التطور التكنولوجي

الباب الأول

السياسة الجنائية ومدى الحماية الجنائية الموضوعية في ظل التطور التكنولوجي

السياسة الجنائية يمكن عدّها الخريطة المرسومة من قبل المؤسسات التشريعية والقضائية والتنفيذية في الدولة والتي تظهر فيها رأي الشعب والجماعة بصورة عامة في تحديد السلوك المخالف والعقوبات المقررة بالقانون، ومنها تحقيق أقصى غايات العدالة، فإن حماية المجتمع يجب أن تعطي تصوراً شاملاً من أجل تحقيق الأمن للمواطن والسلامة والإستقرار، فالسياسة الجنائية تعني في صورتها النهائية تحديد الأساليب والوسائل والمنهجية المؤدية إلى تحقيق الاستقرار الاجتماعي من خلال إصلاح الجاني وإعادة تأهيله وتوازنه للعودة إلى المجتمع سالما ليكون فرداً مقبولاً .

ويعيش العالم في الوقت الحالي تطوراً سريعاً، يتمثل بوجود التكنولوجيا الحديثة المتمثلة بالأنترنت، وأجهزة الحاسب الآلي، والذي يتطور كل يوم ليصبح إستعماله أسرع وأدق وسهل الاستخدام، ومن خلال هذا التطور التكنولوجي فقد اصبح المجتمع العالمي بصورة عامة يمكنه التواصل مع بعض من ابعد نقطة في العالم وفي أي ظرف كان، بواسطة التكنولوجيا الحديثة والانترنت، وهذا ما يشكل عاملاً ايجابيا بفضل التطور التكنولوجي، ولكن في الوقت نفسه توجد أثار سلبية خطيرة، تتمثل بسوء إستخدام هذه التكنولوجيا وما ينتج عنها من ارتكاب لبعض الجرائم بواسطة إستخدام الانترنت، ولهذه الجرائم خصائص تميزها عن غيرها من الجرائم التي نص عليها قانون العقوبات في أغلب دول العالم قبل ظهور التكنولوجيا الحديثة (الانترنت).

ولهذا سنحاول تقسيم موضوع بحثنا في الباب الاول إلى فصلين، نوضح في الفصل الاول ماهية السياسية الجنائية وإرتباطها بالتطور التكنولوجي، ونخصص الفصل الثاني لبحث مظاهر الحماية الجنائية الموضوعية في ظل التطور التكنولوجي.

الفصل الأول

ماهية السياسة الجنائية وارتباطها التطور التكنولوجي

إن جميع النشاطات المبذولة لوقاية المجتمع من الجريمة ومعالجة الوضع الاجرامي بشكل عام يمكن عدها سياسة جنائية، وبهذا فأن الجريمة خروج عن الضوابط السلوكية التي اختطها المجتمع لتأمين سلامة وأستقرار وأمان أفراده، وما يهمنا في هذا المقام أن المشرع يجب أن يعي مرحلة التخطيط لوضع سياسة جنائية وقائية وعلاجية تتضمن تدابير وإستراتيجيات تقوم بتحقيق الاهداف التي ترسمها السياسة الجنائية عبر وسائلها القانونية المتاحة، أو التي يقتضي توفيرها فيما بعد. إذ أن التقدم العلمي والتكنولوجي السريع جعل الإنسان قادراً على تسخير التقنيات والتطبيقات التكنولوجية في تحقيق مصالحه المختلفة، بما يسهل أمور حياته، إلا أنه ومع هذا فقد جعل الإنسان التعامل مع التطور التكنولوجي كوسيلة للتعدي على حقوق الإنسان إلى حد بعيد، مما يوجب إعادة النظر في الإستخدامات البشرية لبعض الأدوات العلمية والتكنولوجية التي تؤثر بشكل أو بآخر على حقوق الإنسان، لا سيما حقه في حياته الخاصة، أو سلامة جسمه، وكذلك لا يمكن أن يترك الجسم البشري يعاني من عدم التكييف مع التكنولوجيا لما تحمله من خصائص وطبيعة ذات أثر ضار عليه، دون النظر في وضع حماية وطرق ضبط استخدام هذه التكنولوجيا بضوابط قانونية؛ من أجل ضمان الحماية من آثارها الضارة.

وفي هذا الخصوص يتوجب علينا في البدء إيضاح ماهية السياسة الجنائية في المبحث الاول، وسنتناول دراسة الدور التكنولوجي وأثره على السياسة الجنائية في مبحث ثان.

المبحث الأول

ماهية السياسة الجنائية

مفهوم السياسة الجنائية ظل يتأرجح ما بين التجريم والعقاب من جهة وما يتعلق بالتدابير والإجراءات الجنائية، إذ لا يخلو الأمر من معالجة ظاهرة الإجرام على المستويين الموضوعي والشكلي. فكلما يتعلق الأمر بتجريم فعل أو تركه وتحديد العقاب المناسب له كان موضوع ذلك القانون الجنائي، وكلما تعلق بإجراءات البحث والمتابعة والمحاكمة والتنفيذ كان ذلك من مواضيع الاجراءات وأصول المحاكمات الجنائية. أما السياسة الجنائية الحديثة والمعاصرة، فأنها لا تقتصر على المفهوم التقليدي وإنما تجاوز الأمر إلى الأهتمام بالأسباب المؤدية إلى إيجاد الظاهرة الاجرامية. ويمكن القوال أن المفهوم المعاصر للسياسة الجنائية هو مفهوم حديث، وقد تضمن هذا المفهوم سياسة تجريم وعقاب

متكاملة ومتطورة؛ وذلك بقصد تقويم المجرم وإعادة تأهيله، ومن المعلوم أن هذا التطور في السياسة العقابية وطابعها ونطاقها جاء نتيجة لتطور وظيفة القانون الجنائي ذاته وفكرة العقاب الذي كان محصوراً في كونه رد فعل لمن إرتكب جريمة، وأن الجريمة مجرد حادثة فردية أقبل عليها مرتكبها بإرادته، فالسياسة الجنائية عموماً تعكس المصالح الواجب حمايتها.

المطلب الأول

مفهوم السياسة الجنائية

يمكننا القول بأن جميع النشاطات المبذولة لوقاية المجتمع من الجريمة ومعالجة الوضع الاجرامي بشكل عام يمكن عَدّها سياسة جنائية، وبهذا فأن أي فعل مكون للجريمة يُعّد خروجاً عن الضوابط السلوكية التي اختطها المشرع لتأمين سلامة واستقرار وأمان أفراده. فهدف السياسة الجنائية هو الاهتمام بشأن الافراد والمجتمع، في سبيل الحد من الجريمة والوقاية منها، بمعنى حماية المصالح المعتبرة، وتوفير الأمن اللازم، وهذا يعني أن السياسة الجنائية تدخل في ميادين الحياة جميعاً، فهي عبارة عن مجموعة من الإجراءات والتدابير والوسائل، ينبغي على المشرع الجنائي دراستها ورسم خطة تهدف إلى حماية المجتمع وضمان حرية عيش الانسان بكرامة من خلال عدم المساس بالحقوق والحريات الدستورية.

وعلى ضوء ذلك سنحاول بيان تعريف السياسة الجنائية من خلال بيان التعريف اللغوي والاصطلاحي وفي الشريعة الاسلامية .

الفرع الأول

تعريف السياسة الجنائية

أولا : تعريف السياسة الجنائية لغة :

1- السياسة لغة : هي القيام على الشيء بما يصلحه، والسياسة فعل السائس، ويقال هو يسوس الدواب اذا قام عليها وراضها، والولي يسوس رعيته[1]. وقيل أيضاً في بيانها: سياسة (أسم) مصدر ساس، مبادئ معتمدة تتخذ الاجراءات بناءً عليها، والتنظيم السياسي هو مجموعة من الناس ذوي الاتجاه الواحد فيما

(1) - ينظر: أبن منظور ، لسان العرب ، 1997 ، ص 376

يتعلق بالبرامج والمبادئ السياسية وفقاً لقواعد تنظيمية مقبولة من جانبهم، وتحدد علاقاتهم وأسلوبهم في العمل والنشاط.[1]

2- الجناية لغة : جني : جنى الذنب عليه جناية – الجناية الذنب والجرم وما يفعله الانسان، مما يوجب عليه القصاص أو العقاب في الدنيا والآخرة، وتجنى فلان على فلان ذنباً إذا تقوله عليه وهو بريء، والتجني مثل التجرم وهو يدعي عليك ذنباً لم تفعله[2].

ثانيا : تعريف السياسة الجنائية في الفقه والقانون

لم يكن مصطلح (السياسة الجنائية) معروفا أوائل القرن التاسع عشر، اذ يعد الفقيه الالماني (فيورباخ) من أوائل من استعمل هذا التعبير. إذ عرفها بأنها " هي مجموعة الاجراءات العقابية المتخذة من قبل الدولة ضد المجرم "[3] أما العالم الالماني (فرانز فون ليست) فعرفها بأنها "مجموعة المبادئ القائمة على أساس من الفحص العلمي لأصول الجريمة وجذورها وآثار العقاب التي على الدولة أن تكافح بمقتضاها الاجرام بالعقوبات وغيرها من التدابير المشابهة[4]. وعرفها (كراماتيكا) بأنها النشاط الذي يستهدف تأهيل كل شخص إنحرف سلوكه وهي مسؤولية وإلتزام يقع أيضاً على عاتق المجتمع باعتباره هو المسؤول عن السلوك المنحرف ، أو هي اتجاه فكري جديد يرسم سياسة عقابية على أسس حديثة في فن مكافحة الإجرام[5] . ويعرفها (مارك أنسل) بالقول: هي السياسة التي تهدف إلى الوصول لأفضل صيغة لقواعد القانون الوضعي، وتوجيه كل من المشرع الذي يضع القانون والقاضي الذي يقوم بتطبيقه والإدارة المكلفة بتنفيذ ما يقضي به هذا القاضي. ويعرفها الفقيه النرويجي (اندیناس) على أنها: تخطيط سياسة تدابير المجتمع ضد المجرم[6] . وعرفها بعض الفقه على أنها : علم ينصب على المستقبل فيرسم خطوطه وتطلعاته القانونية وطموحاته، ويلزم المشرع الجنائي ويقوده نحو مكافحة الجريمة سواء عن طريق تدابير وقائية من الجريمة، أم عن طريق تجريم

(1) - د. معالي حميد الشمري، السياسة الجنائية التشريعية في قوانين الاحزاب السياسية ، مجلة كلية التربية، العدد التاسع والثلاثون، الجزء الثاني، 2020،ص 465 .

(2) - أبن منظور، لسان العرب، محمد بن ابي بكر ،ص 476 . وكذلك : المعجم الوسيط ، الجزء 1 و 2، دار احياء التراث العربي، بيروت، 2008، ص 159 . وكذلك ينظر: المنجد في اللغة. لويس المعلوف، الطبعة الرابعة، انتشارات ذوي القربى، 1429 هـ، ص 88 .

(3) - د. واثبة داود السعدي، الأسس النظرية لعلمي الاجرام والسياسة الجنائية، مكتبة الرسالة ، من غير سنة نشر، ص 112 . وكذلك : د. براء منذر عبداللطيف، المرجع السابق، ص 7 .

(4) - د. حميد عبد حمادي ضاحي، سياسة المشرع العراقي في مكافحة الفساد الاداري ، بحث منشور، مجلة جامعة الانبار للعلوم القانونية، العدد الخامس ، سنة 2018 ، ص 244 .

(5) - د. صلاح حسن احمد ، الدفاع الاجتماعي ضد الجريمة بين الشريعة الاسلامية والقانون الوضعي ، بحث منشور ، مجلة كلية العلوم والسياسة ، جامعة كركوك ، 2011 ، ص 114.

(6) - سعداوي محمد صغير ، السياسة الجزائية لمكافحة الجريمة ، اطروحة دكتوراه ، جامعة ابو بكر بلقايد ، كلية الآداب والعلوم الاجتماعية ، الجزائر ، 2010 ، ص12.

أنماط سلوك معين مستحدث، وتقدير عقوبات رادعة [1]. وأيضاً يمكن تعريف السياسة الجنائية على أنها: (اسم للأحكام والتصرفات التي تدار بها شؤون الامة في حكوماتها وتشريعاتها وقضائها، وفي جميع سلطاتها التنفيذية والإدارية، وفي علاقاتها الخارجية التي تربطها بغيرها من الأمم)[2] .

وهناك من عرفها على أساس المفهوم الضيق بأنها: مجموعة من الوسائل والتدابير التي ينبغي على الدولة اتخاذها لمكافحة الجريمة[3]. أما المفهوم الواسع للسياسة الجنائية فهي: دراسة الاسباب والعوامل المهمة للوصول إلى الوسيلة المناسبة في سبيل التصدي للسلوك الاجرامي والوقاية منه[4]. ومن خلال هذه المجموعة من التعاريف، والتي قد تتفق جميعها في مضمونها، إذ إن السياسة الجنائية هي علم وتخطيط ودراسة، يتناسب مع فكر وعادات وتقاليد المجتمع.

ثالثا : تعريف السياسة الجنائية في الشريعة

في الحقيقة أن فقهاء الشريعة لم يتطرقوا إلى تعريف السياسة الجنائية في السابق، إلا أنه حديثا ازدادت الأهمية إلى توجيه دراستهم لهذا المفهوم والذي يدخل ضمن نطاق مفهوم (السياسة الشرعية).

وفي هذا الصدد فقد أورد الفقهاء المسلمون بعض التعريفات للسياسة الشرعية، فعرفها بعضهم على أنها: " تدبير الامور، وحسن رعايتها وإصلاحها، وتأتي في معنى آخر وهي تدبير شؤون الدولة" فالساسة هم قادة الأمم لتدبير شؤونها العامة، وأجمع معاني السياسة هو إستصلاح الخلق بإرشادهم إلى الطريق الصحيح في العاجل والأجل[5]، والسياسة بالكسر تعني القيام على الشيء بما يصلحه، وتدبير الامة والجري بها وفق سنن العدل والإستقامة؛ لإستصلاح شؤونها الداخلية والخارجية[6]، وجاء تعريف السياسة الجنائية في الشريعة الاسلامية بانها: هي السياسة الشرعية المعمول بها في الشرع الحكيم، والتي تعني كما يقول الامام ابن القيم الجوزي في مرجعة (الطرق الحكيمة في السياسة الشرعية) نقلا عن الامام ابن العقيد في الفنون : (فعل ما يكون الناس مع أقرب إلى الاصلاح ، أبعد

(1) - حيدر راجي علي ، السياسة الجنائية في قانون مكافحة الإرهاب ، رسالة ماجستير ، جامعة كربلاء ، كلية القانون ، 2018 ، ص8.

(2) - خالد بن عبدالله الشافي ، دور السياسة الجنائية في تحقيق الأمن الأخلاقي في ضوء الشريعة الاسلامية ، المصدر السابق ، ص 11.

(3) - د. منذر كمال الشاوي، السياسة الجنائية في قانون العقوبات العراقي، الرسالة للطباعة، بغداد، 1978، ص11 وما بعدها.

(4) - د. احمد فتحي سرور، أصول السياسة الجنائية، دار النهضة العربية، مصر، 1972، ص 13 وما بعدها.

(5) - محمد بن المدني بوساق، اتجاهات السياسة الجنائية المعاصرة والشريعة الاسلامية، مركز الدراسات والبحوث ، اكاديمية نايف العربي للعلوم الامنية، الرياض، 2002، ص 75.

(6) - حيدر راجي علي ، السياسة الجنائية في قانون مكافحة الارهاب ،المصدر السابق ، ص6.

عن الفساد وإن لم يقم به الرسول، ولا نزل به الوحي). وهناك من وصف السياسة الجنائية بأنها: إدارة الشؤون العامة للدولة الإسلامية، بما يكفل تحقيق المصالح ودفع المضار بما لا يتعدى حدود الشريعة في أصوله الكلية. وجاء أيضاً تعريفها على أنها : رعاية شؤون الأمة على الصعيد الداخلي والخارجي وفق الشريعة الإسلامية[1].

ويرى الباحث أن تعريف السياسة الجنائية هي : مجموعة من المبادئ والأسس النظرية والفلسفية تمثل إيدلوجية النظام القابض على السلطة، والتي تضع النموذج العام الذي تعتمده التشريعات الجنائية في تجريم الأفعال وسلوك الأفراد. فالسياسة الجنائية تهتم في معالجة ومكافحة الخطورة الإجتماعية (الجريمة) والتي تمس الأمن والنظام العام للدولة ومؤسساتها، أي أنها خطة لوضع مجموعة من الإجراءات الرادعة والتي بموجبها تكفل الدولة مكافحة الجرائم والافعال غير المباحة، فهي رسم وتكوين القواعد القانونية، بناءً على معطيات علم الإجرام الذي يواكب التطور الذي يعيشه كل مجتمع وفق ظرف وزمان معين، فهي دليل المشرع إلى ما يجب أن تكون عليه نصوص الوقاية والتجريم والعقاب، وكيفية تنفيذ الجزاء.

الفرع الثاني

السياسة الجنائية في ظل الاتفاقيات الدولية

أهتمت التشريعات الدولية المعاصرة بموضوع مكافحة الجريمة، وأصبحت أحد الاهتمامات الرئيسة للدول والحكومات وذلك لما لهذا الموضوع من أهمية في حفظ أمن وإستقرار الحياة العامة ولنمو وتطور النظام الإجتماعي والأقتصادي، وكل هذا مرهون بسلامة الإنسان، ومدى اطمئنانه على حياته وكرامته[2]، لهذا أصبح الإستقرار الأمني لكل دولة هو الأساس في تطورها على جميع الاصعدة وبالأخص التطور الاقتصادي، ونمو الاستثمار وجذب السياحة والاستثمار، لهذا نجد أن أغلب الدول أعطت الاهمية الكبرى لمكافحة الجريمة على جميع الأصعدة مما دفعها لعقد اتفاقيات ومعاهدات دولية من أجل مكافحة الجريمة، وذلك من خلال وضع سياسة وقائية قائمة على التخطيط والسياسة الجنائية من خلال الإعتماد على معطيات علمية وفرض العلوم الاجتماعية والإنسانية والإستراتيجية ومواكبة جميع التحولات التي تطرأ على المجتمع من خلال التطور التكنولوجي والأقتصادي وغيرها، سواء

(1) - هدام إبراهيم أبو كاس. السياسة الجنائية بين الفقه التقليدي والإتجاه الحديث، رسالة ماجستير، جامعة د.الطاهر موالاي ، كلية الحقوق والعلوم السياسة ، الجزائر، 2016 ، ص 14 .

(2) - د. واثبة داود السعدي ، المرجع السابق، ص 119.

على الصعيد الوطني، أم على المستوى الدولي والمنظمات الدولية، مما أدى إلى تظافر الجهود الدولية فيما بينها، ومن ثم أدى إلى ظهور نماذج وأنماط عديده لهذا التعاون والذي كان له الدور الكبير في إنجاح السياسة الجنائية على صعيد التعاون الدولي، فقد لعبت المعاهدات والاتفاقيات الدولية بشان القانون الجنائي الدولي دورا مهماً في هذا المجال، وبالأخص الدور الفعال لمنظمة الأمم المتحدة والمنظمات المتخصصة في مجال مكافحة الجريمة ومنها (منظمة الشرطة الدولية الجنائية)، والتي قدمت التعاون الدولي من أجل مكافحة الجريمة، وكذلك ساعدت الباحثين من أجل وضع سياسة جنائية مواكبة للتطور الذي تعيشه أغلب المجتمعات الدولية على صعيد السياسات الوطنية والاقليمية والدولية للوقاية من مخاطر الجريمة[1].

وقد أهتمت المنظمة الدولية المتمثلة بـ (الأمم المتحدة) بفكرة مكافحة الجريمة، وإصلاح المجرمين اهتماما كبيرا، من خلال إدراك المخاطر التي تهدد العالم من جراء إنتشار الجريمة بصورة عامة، وما ينتج عنها من تفاقم خطر الجريمة المنظمة العابرة للحدود وغيرها من الجرائم الخاصة[2]، وعلى أساس ذلك ظهر أهتمام الهيئة الدولية واضحاً في البحث عن طرق وأساليب ناجعة لمواجهة ظاهرة الاجرام المنظم، وقد أكد (الدكتور بطرس غالي) الأمين العام لهيئة الأمم المتحدة في ذلك الوقت، على تبينه في التصدي للجريمة في ذلك الوقت، من خلال إلتزامه بالحفاظ على القيم الإنسانية الأساسية التي تضمنها ميثاق الامم المتحدة، وسعية لمحاربة قوى الظلام المتمثلة في انتشار الجريمة المنظمة كظاهرة عالمية انتشرت في كل مكان من العالم[3]، والتي قد انتهكت القواعد الاساسية للقانون في الدول الغنية والفقيرة واتخذت العنف والتهديد وسائل أساسية لها، الأمر الذي جعل منها جريمة بغير هوية تعمل في عدة دول بهدف كسب الأرباح مستعملة في ذلك تلويث مناخ العمل في مجال رأس المال وافساد الزعامات السياسية والتأثير السلبي على حقوق الإنسان، مما يتوجب ضرورة الاسترشاد في المبادئ التوجيهية التي أقرتها الامم المتحدة، ولهذه الأسباب إتجهت الأمم المتحدة إلى تشكيل لجان تختص في متابعة ظاهرة الجريمة المنظمة والعابرة للحدود من خلال البحث عن اليات لمواجهتها . ومن هذه اللجان:

1- لجنة الجريمة والعدالة الجنائية .
2- لجنة مخصصة دولية حكومية.

---

(1) - أمير فرج يوسف. الجريمة الالكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والإنترنت، مكتبة الوفاء، الإسكندرية، 2011، ص 419 .

(2) - د. أكرم نشأت ابراهيم ، السياسة الجنائية، دار الثقافة ، ط 1، عمان، 2008، ص 44.

(3) - د. زيباري الشاذلي، إتجاهات السياسة الجنائية الدولية كآلية قانونية لمواجهة الجريمة المنظمة العابرة للحدود، بحث منشور، مجلة البحوث القانونية والاقتصادية ، مجلد 2، العدد 2، 2020، ص 265 .

3- فريق كبار الخبراء .

كما جاء في الاتفاقية الاوربية لحماية حقوق الإنسان عام 1950 ضابط الضرورة، ووضعت المواد (11 ، إلى 18) أن ممارسة الحقوق والحريات يمكن أن تخضع لشروط أو قيود التجريم، أو العقاب التي ينص عليها القانون مما يعد تدابير ضرورية في مجتمع ديمقراطي لحماية الامن الوطني ووحدة الكيان الإقليمي للدولة أو المحافظة على الأمن العام. أو الدفاع عن النظام، أو منع الجريمة، أو حماية الصحة أو الأخلاق أو حماية حقوق الغير في مواجهة إفشاء الأسرار الخاصة أو لضمان إستقلال سمعة وحيدة القضاء. وجميع هذه الجهود هي من أجل مكافحة الجريمة بأفضل الوسائل والطرق الحديثة، وذلك لمواكبة التطور الذي تعيشه أغلب المجتمعات، وكذلك للإحاطة الوقائية للجريمة قبل وقوعها كسياسة وقائية منعية تواكب تطور الجريمة المنظمة[1].

أولاً : السياسة الجنائية في التشريعات الغربية

اهتم المجتمع الدولي بظاهرة تفشي الجريمة وإنتشارها، وذلك لما تشكله من خطر، يصيب المجتمعات من الناحية الإجتماعية والأقتصادية والسياسية، مما يؤدي إلى زعزعة الأمن الدولي والوطني، وهذا مما أدى إلى تظافر الجهود الدولية والإقليمية لمكافحة الجريمة، ووضع سياسة جنائية دولية واقليمية ووطنية، تتناسب مع التطور الذي يعيشه العالم في ظل العولمة والتكنولوجيا[2]. وسوف نتطرق إلى هذه السياسات الدولية على الصعيد الدولي والاقليمي ومنها:

1- موقف السياسة الجنائية في فرنسا : المشرع الفرنسي لم يشرع قانوناً خاصاً لمعالجة الجريمة المنظمة بصورة عامة، ولكنه أقر ظروفاً مشددة كلما أقترن بإرتكاب موضوع الجريمة التقليدية من قبل جماعة منظمة، وعلى الرغم من أنه ليس بالأسلوب الأمثل للتصدي لهذه الظاهرة، ولكن سياسة التشريع في فرنسا إستهدفت من وراء ذلك تجريم الواقعة الأكثر خطورة، المتمثلة في تنظيم عصابة اجرامية مهما كان نشاطها، وعلى ضوء ذلك فأن تجريم مجرد تكوين عصابة منظمة هو في حد ذاته شكل من أشكال الجريمة المنظمة، كما جرم المشرع الفرنسي جريمة تبييض الأموال لتشمل كافة الاموال التي مصدرها جريمة خطيرة، بعد ان كانت مقصورة على الاموال المتحصلة من الإتجار بالمخدرات فقط[3].

---

(1) - عبدالصمد الكنا، ضوابط التجريم والعقاب ضمانه للحقوق والحريات، بحث منشور ، مجلة المنار للدراسات القانونية والادارية، العدد (5) ، 2017 ، ص 22 .

(2) - احمد عبدالمجيد الحاج، المسؤولية الجنائية لجرائم النشر الالكتروني في ضوء قانون مكافحة جرائم تقنية المعلومات الاماراتي، بحث منشور، مجلة المنهل، وزارة الداخلية، ابو ظبي، 2012، ص 10.

(3) - د. عبدالفتاح بيومي حجازي، علم الجريمة والمجرم المعلوماتي، الطبعة الاولى، منشأة المعارف، الاسكندرية، 2009، ص125 .

وبعد ذلك صدر قانون رقم (6 /يناير/ 1978) الخاص بالمعالجة الإلكترونية للبيانات الاسمية، وكان مطروحاً للنظر امام مجلس الشيوخ مشروع قانون أعد لتعديل قانون حرية الاتصالات الصادر 1986 ليتفق مع التوجهات الأوربية الجديدة، تقدمت الحكومة الفرنسية بتعديل لهذا المشروع يتعلق بإضافة مواد جديدة للقانون المذكور بشأن الإذاعة والتلفزيون، مستهدفا بذلك التعديل الحكومة، وكذلك صدر قانون رقم (19) لسنة 1992 الخاص ببعض الجرائم المعلوماتية، بعد أن فشلت فرنسا تنظيم استعمال الانترنت عام 1988، وبعد ذلك صدر قانون رقم 230 لسنة 2000 في شأن الاثبات والمتعلق بالتوقيع الالكتروني[1].

2- موقف السياسة الجنائية في أمريكا : اهتم المشرع الأمريكي بمكافحة الجريمة المنظمة من خلال تشريع سياسة جنائية، تتضمن قانونا خاصا عرف بقانون (المنظمات المتأثرة بالإبتزاز والفساد) لسنة 1970 ، والذي يختص بمكافحة طائفة من جرائم الولايات والإتحادية، بالإضافة إلى الجريمة المنظمة، ونجد المشرع الأمريكي استخدم لفظ (مؤسسة غير شرعية) بدل جماعة إجرامية منظمة لتركيزه على طبيعة ما تمارسه تلك المؤسسة أو المنظمة من انشطه ذات طابع اقتصادي ومالي، وفي إطار مكافحة جريمة تبييض الأموال بوصفها أحدى صور الجريمة المنظمة، فقد تم تجريمها؛ كونها تمثل نشاطا غير قانوني، وخطرها لم يقتصر على متحصلات الجرائم المخدرات، بل شمل كافة الأنشطة الإجرامية الاخرى[2].

أن السياسة الجنائية للولايات المتحدة الأمريكية تختلف من الصعيد الاتحادي منه على الصعيد المحلي، ويعود ذلك لتبني الولايات المتحدة الأمريكية تشريعات على المستوى الولايات أي تلك التي تخص الولاية بذاتها فقط وعلى المستوى الاتحادي أي تلك التي تخص جميع الولايات الأمريكية ضمن سياستها الجنائية لمواجهة الجرائم الالكترونية، فالدستور الأمريكي قد سمح بالتشريع على مستويين:

المستوى الأول: المستوى الإتحادي والذي لا يكون إلا بالقدر الضروري من التداخل.

المستوى الثاني: من التشريع يكون بإذن من الحكومة الإتحادية للحكومات المحلية في موضوع معين، وليس من الاعتيادي للقوانين الجنائية الاتحادية أن تتدخل مع القوانين المحلية في مسائل جوهرية.

---

(1) - سعود علي عبدالله اللوغاني، السياسة الجنائية في مكافحة الجريمة الالكترونية، أطروحة دكتوراه، جامعة الشارقة، كلية القانون، 2016 ، ص 176. وكذلك: د. عبدالفتاح بيومي حجازي، علم الجريمة والمجرم المعلوماتي ، المصدر السابق، ص 126.

(2) – د. مدحت رمضان، جرائم الاعتداء على الاشخاص والانترنت، دار النهضة العربية، القاهرة، 2000، ص 17 وما بعدها.

وتتعامل التشريعات الجنائية في الولايات المتحدة الامريكية مع جرائم الكترونية عديدة، ومن ضمنها (قانون الإحتيال الالكتروني وإساءة استخدام الحاسوب) (**18 U.S. Code § 1030**)، والذي يجرم الأفعال التي ترتكب ضد المؤسسات المالية أو ضد الحكومة الفدرالية أو الجرائم التي تؤثر على التجارة بين الولايات، أو التجارة الدولية أو الجرائم الالكترونية ضد الأفراد[1]، ومن هذه الجرائم:

أ- الحصول على معلومات من حاسوب حكومي والتي من المفترض أن تبقى سرية بشكل غير قانوني.

ب- الوصول إلى حاسوب بشكل مشروع، لكن يستخدم هذا الوصول للحاسوب لارتكاب جرائم أو الوصول لمعلومات لا يجوز له الوصول إليها.

ج- الوصول لمعلومات وإرتكاب جرائم احتيال من خلالها.

د- تهديد بتسبيب ضررً للحاسوب؛ من أجل الحصول على أموال، أو ممتلكات شخص من الأشخاص.

ه- التسبب بضرر للحاسوب من خلال الدخول غير المشروع للحاسوب أو من خلال إدخال رموز أو معلومات ضارة للحاسوب [2].

وأيضا تضمن القانون (**18 U.S 2251**) تجريم بعض الافعال ومن ضمنها قانون استيراد أو نقل المواد الفاحشة والذي يحظر استخدام الحاسوب لتوريد المواد الفاحشة للولايات المتحدة فيما بين الولايات أو بالتجارة الأجنبية، ومن ضمنها ما يأتي:

1- قانون حظر استغلال الأطفال والذي يمنع من أدخال، أو إستغلال القصر في المواد الإباحية، لو تم صناعة الفلم من مواد تم استيرادها للولايات المتحدة الأمريكية وبما في الحاسوب.

2- ويحظر هذا القانون إستخدام الحواسيب لتجارة أو نقل المواد الإباحية التي يوجد فيها قُصر.

3- ويحظر كذلك صناعة الأفلام الإباحية للأطفال[3].

ونجد أن السياسة الجنائية للمشرع الأمريكي تحاول مواكبة التطور التكنولوجي والتقني، من خلال إصدار مجموعة كبيرة من القوانين لتنظيم التعاملات الإلكترونية، وقد شرع قانون آخر هو قانون

(1)- Susan W. Brenner, State Cybercrime Legislation in the United States of America: A Survey, Richmond Journal of Law and Technology, Volume 7, Issue 3, page 3.

(2)- Xiobang LI & Yongfeng Qin, Research on Criminal Jurisdiction of Computer cybercrime, 8th International Congress of Information and Communication Technology, 2018, page 30.

(3)- Susan W. Brenner, Op.Cit, page3.

الاحتيال في الملفات الإلكترونية والمعلومات **18 U.S 1028**، يعد جريمة حيازة ملفات أو معلومات بما فيها تلك التي تستخدم لتزوير البيانات. وأما القانون الاتحادي الأخير في هذه المسألة هو قانون الإنتهاك الجنائي لحقوق الملكية الفكرية رقم (**18 U.S.C. § 2319**)، والذي يحظر إنتهاك حقوق الملكية الفكرية[1].

أما على صعيد الولايات فلا توجد آلية موحدة لا على المستوى الإتحادي، ولا على المستوى التشريعي لوضع تشريعات داخلية للولايات لمواجهة الجرائم الإلكترونية، ولكن توجد بعض الأنماط المشتركة بين الولايات ومن ضمنها قوانين موحدة جزائية للجرائم الإلكترونية وقوانين استرداد وتعويض.

ويمكن القول أن السياسة الجنائية في الجرائم الالكترونية تقسم القواعد على ثماني فئات وهي قواعد إجرائية، وجرائم غير جنسية، وهي جرائم الاحتيال والسرقة الالكترونية، وجرائم تتسبب بأضرار للحاسوب، وجرائم التزييف، وجرائم المقامرة وجرائم التي تخالف الأخلاق العامة، وجرائم ضد الحكومة[2]، والتي سنتناولها كما يأتي:

أ- قواعد إجرائية: وضعت معظم الولايات قواعد إجرائية للمحاكمة عن ارتكاب الجرائم الإلكترونية، ووضعت بعض منها جزاءات وعقوبات على الجرائم ووضعت ألمدد التي يجب أن يتم من خلالها إقامة الدعوى وإنهائها، وضمانات المتهم الجنائية.

ب- جرائم غير جنسية ضد الشخص: وضعت بعض الولايات قوانين تتكلم عن الجرائم غير الجنسية التي ترتكب ضد الأشخاص، مثلاً وضعت بعض الولايات نصوصاً لجرائم القتل باستخدام الحاسوب، وذلك عن طريق أختراق حاسوب والتسبب بقتل شخص أو عدة أشخاص أو تعريض حياتهم للخطر. وبين قانون (ولاية فرجينيا) يُعّد جريمة إستخدام حاسوب لتسبب بإصابة جسدية للفرد بشكل عمدي، وجرمت بعض القوانين ملاحقة الشخص على الانترنيت، وبعضاً منها إشترطت وجود تهديد خطير لحياة الفرد لاعتبارها جريمة[3].

ت- الجرائم الجنسية: تحاسب معظم قوانين الولايات على الجرائم الجنسية المتعلقة بتجارة المواد الإباحية للأطفال، وبعض منها يعاقب على إستخدام القاصر بأفعال جنسية على الانترنيت، وبشكل عام تحظر كل الولايات إستخدام الأطفال للتجارة الجنسية بهم أو لاستغلالهم بشكل جنسي، وبشكل عام تَعد

(1)- Sophie Victoria Ann Richardson and Nicholas Gilmour, Cyber Crime and National Security: A New Zealand Perspective, Studying Group on Organised Crime, page 14
(2)- Ibid, page4.
(3)- Ibid, page4.

الولايات الجرائم الجنسية ضد الأطفال من بين الجرائم الخطرة والتي تقتضي مواجهة وفرض عقوبات عليها[1].

ث- جرائم الإضرار والأختراق: إن معظم قوانين الولايات في أمريكا تتضمن قوانين تتعلق بجرائم الاختراق والتسبب بأضرار للحاسوب، وتنقسهم هذه القوانين إلى عدة فئات من بينها، الفئة الأولى هي عملية اختراق الحواسيب والتي يكون فعلها الإجرامي من الدخول للحاسوب من دون رخصة، تضيف بعض الولايات نصوص تتعلق بإساءة إستخدام الحاسوب والتي تتعلق بحظر النسخ أو إستقبال أو إستخدام معلومات تم الحصول عليها بأختراق أو إنتهاك حاسوب. وتمنع بعض النصوص عملية نقل الفيروسات والبرامج الخبيثة الأخرى، وتجرم بعض الولايات عملية نقل المعلومات التي تتسبب بأضرار لسمعة الشخص ويمنع بعض منها عملية إضرار بخدمات الحاسوب[2].

ج- جرائم الإحتيال والسرقة الإلكترونية: تمنع العديد من الولايات استخدام الحاسوب لإرتكاب جرائم الاحتيال، أي إستخدام الحاسوب، أو الشبكة لغرض خداع، أو من أجل الحصول على الأموال أو الممتلكات أو الخدامات، ومن هذه الجرائم جرائم اختلاس الأموال الرقمية، وكذلك جرائم السرقة الرقمية، والتي من ضمن جرائمها هي سرقة البرمجيات وسرقة المعلومات وسرقة معدات الحاسوب، وسرقة خدمات الحاسوب، وكذلك إستخدام الحاسوب لإرتكاب جرائم السرقة الاعتيادية، أي سرقة الممتلكات فيما عدا خدمات الحاسوب، أو برمجياتها أو معداتها[3].

ح- جرائم التزوير الرقمي: تجرم بعض الولايات جرائم التزوير، والتي تعرف بأنها جرائم ترتكب من أي شخص يقوم بخلق بيانات أو تعديلها أو محوها، أي تلك البيانات في الحاسوب، أو برامج الحاسوب، والتي بقيام الشخص بمحوها أو تعديلها يكون قد إرتكب جريمة التزوير الالكتروني. وضعت بعض من الولايات نصوصاً تتعلق بأجهزة التزوير من برمجيات ومعدات حاسوب والتي تستخدم لهذه الأغراض[4].

خ- المقامرة وجرائم ضد الأخلاق الأخرى: منعت ولاية واحدة جرائم المقامرة وهي (ولاية لوزيانا) والتي وضعت نصاً لجرائم المقامرة بإستخدام الحاسوب والتي تتكون من ارتكاب أو مساهمة في "لعبة أو مسابقة أو قرعة أو أي مسابقة قد يخسر فيها الشخص ما يملك.... لحصول على أموال على الإنترنيت أو الشبكة العنكبوتية العالمية أو بأي حاسوب أخر. أي يشترط في هذه الجريمة إستخدام الإنترنيت لكسب المال من مسابقة أو قرعة والتي يشترط أن يمكن خسارتها في نفس الآن أي توجد مقامرة على

(1)- Jonathan Clough, Principles of Cybercrime, Cambridge Univesity Press, United States, page 30.
(2)- Ibid, page6.
(3)- Ibid, page7.
(4)- Ibid, page8.

الأموال، وجرمت بعض الولايات شراء الكحول بإستخدام الإنترنيت وبعض منها منعت بيع السكائر باستخدام الإنترنيت[1].

د-الجرائم ضد الحكومة: جرمت بعض الولايات معاقبة الأشخاص عن الجرائم المرتكبة ضد الحكومة مثل (ولاية إيلينوي)[2].

ثانيا : السياسة الجنائية في تشريعات الدول العربية

يتضح لنا جليا أن أغلب الدول العربية من خلال تشريعاتها الجنائية، إلى انها تُسهم في مكافحة الجريمة، من خلال تشريع سياسة جنائية متناسقة ومتطورة تهدف إلى وضع حلول وآليات تتناسب مع التطور الذي يحصل في المجتمعات كافة في ظل العولمة الجديدة التي تعيشها أغلب دول العالم، وتطور التكنولوجيا، والتعامل الاقتصادي والدولي[3].

1- موقف المشرع المصري

تُعد حركة التشريع في مصر حركة نشيطة ومتجددة، تتأثر بإتجاهات التشريع الدولية بشكل مباشر، وقد يرجع عدم إتخاذ موقف صريح في مواجهة الجريمة المنظمة، إلى الإعتقاد السائد أن مصر لا تعاني أي اشكالية فيما يتعلق بظاهرة الإجرام المنظم بأبعاده الجديدة ولا تتواجد على أرضها منظمات إجرامية من نوع المافيا وغيرها، إذ إن الغالب هو طابع الإجرام الفردي أو التشكيل العصابي (الداخلي) إلاّ أنه تم تفنيد هذا الإعتقاد من خلال الدراسات والأحصائيات العلمية التي كشفت أن مصر هي منطقة عبور للمنظمات الاجرامية والمتخصصة في التعامل غير المشروع في جرائم المخدرات والمؤثرات العقلية، وممارسة بعض الانشطة الاجرامية الاخرى كتبييض الاموال بمختلف أشكاله[4].

2- موقف المشرع المغربي :

سعى المشرع المغربي لمكافحة الجريمة وذلك من خلال إعداد مشروع قانون رقم (10.16) الذي صادق عليه المجلس الحكومي بتاريخ (8 /يونيو/ 2016) وأحيل إلى مجلس النواب بتاريخ (14/ يونيو/ 2016) إذ شرعت لجنة العدل والتشريع في مناقشة يوم 13 يوليوز 2016 . وقد تضمن هذا المشروع عدداً من المواضيع والتدابير التي استهدفت مراجعة سياسة التجريم علما أن أطر وزارة

(1)- Sahira Jati Pratiwi, Steven Adinda Destaloka and Putri Permatasar, The Application of e-Court as an Effort to Modernize the Justice Administration in Indonesia: Challenges & Problems, Indonesian Journal of Advocacy and Legal Services, Vol. 2, No. 1, 2020, page 13.

(2)- Ibid, page 15.

(3) - د. اكرم نشأت ابراهيم، المرجع السابق، ص 45.

(4) - د. زيباري الشاذلي ، المرجع السابق، ص 270.

العدل وبعض القضاة ذوي الكفاءة والتجربة في المجال الجنائي لا زالوا بصدد تنقيح مسودة المشروع الجزائي للقانون الجنائي.

وقد ظهرت الحاجة إلى تجريم أفعال جديده نشأت اساساً من مقتضيات الدستور، ومن الإتفاقيات الدولية التي صادق عليها المغرب[1].

ومن هذه المواضيع المهمة التي تخص السياسة الجنائية الحديثة لدولة المغرب هي ، وضع سياسة جنائية فيما يخص جرائم القانون الدولي الانساني، وكذلك تشريع قانون جرائم القانون الدولي لحقوق الانسان، وسعت السياسة الجنائية في دولة المغرب إلى بذل الجهود في مجال مراجعة السياسة الجنائية فيما يخص السياسة العقابية ومدى فاعلية العقوبات البديلة والعدالة التصالحية، والتخفيف التلقائي للعقوبات، بالإضافة إلى السعي في مجال محاربة الجريمة المعلوماتية . ومن خلال ذلك نرى أن السياسة الجنائية في دولة المغرب العربي تتماشى مع التطور الإجتماعي والتكنولوجي والأقتصادي وغيرها من مجالات الحياة [2].

3- موقف المشرع العراقي :

نصت التشريعات الجزائية في ورقة أصلاح النظام القانوني في العراق على ما يلي (تحديد المسؤولية الجزائية في ضوء العلاقات الجديدة بين الفرد والمجتمع واذا كانت النظرة التقليدية تحدد المسؤولية الجزائية على أساس مبدأ الاختيار فان النظرة الاصلاحية الجديدة تأخذ بنظر الإعتبار العوامل الموضوعية والشخصية في آن واحد. ويلزم أن تلعب النظرة العلمية إلى المجرم والجريمة والمجنى عليه دورها في تحديد مفهوم جديد لموانع المسؤولية الجزائية، وفي رسم طرق وحلول اصلاح المجرم وحماية المجتمع منه)[3].

ونصت السياسة الجنائية في القانون ذاته على بعض المضامين وهي: (لكي يكون الشخص مسؤولاً جزائياً، لا بد من أن يكون قادرا ذاتياً وموضوعياً، على أختيار الفعل (العلم والارادة) أو الإمتناع الذي يكون جريمة، وفي حال تأكد مبدأ المسؤولية الجزائية فأن نطاقها يتحدد، تشديدا أو تخفيفا، على أساس

(1) - ينظر: توصيات مؤتمر الامم المتحدة الثالثة عشر حول الجريمة والعدالة الجنائية، بعنوان (الجهود السياسة الجنائية المغربية في التصدي للجريمة)، سلسلة دراسات وابحاث جنائية، صدرة عن مركز الدراسات وابحاث السياسة الجنائية، المملكة المغربية، وزارة العدل ، العدد 3 ، 2020، ص 77 وما بعدها .

(2) - محمد، ورضوان العنبي، السياسة الجنائية بالمغرب وانواع العقوبات البديلة لمكافحة الجريمة، بحث منشور، مجلة المنار للدراسات القانونية والادارية، العدد الخاص، 2017، ص 134 و135.

(3) - د. كاظم عبدالله الشمري، زينة عبدالجليل عبد، سياسة التجريم في القوانين الخاصة، بحث منشور ، مجلة العلوم القانونية، جامعة بغداد، كلية القانون، العدد الخاص، المجلد 36، 2021، ص 183.

الظروف التي تسهم في تحقق ارادة الفاعل وأختياره)[1].

ومن خلال تحليلنا للنصوص الواردة في السياسة الجزائية المرسومة في العراق في بعض القوانين الجنائية نجد أن واضعي السياسة الجنائية قد إعتمدوا المذهب الوسطي، فمن خلال هذه النصوص نجد أن السياسة الجنائية الحديثة تتمثل ببعض المبادئ :

أ- لا تلغى مبدأ حرية الأختيار، وإنما تلغى اعتماده كأساس وحيد لتحقق المسؤولية الجزائية وتدعوا إلى الأخذ بنظر الإعتبار للعوامل الموضوعية والشخصية في آن واحد.

ب- تعتمد لتحقق المسؤولية الجزائية القدرة الذاتية والموضوعية للفاعل على اختيار الفعل والامتناع الذي يكون الجريمة.

ت- تحدد نطاق المسؤولية تشديداً وتخفيفاً في ضوء الظروف التي تَسهم في تكوين إرادة الفاعل واختياره.

ث- تعتمد النظرة العلمية إلى المجرم والجريمة والمجني عليه في تحديد موانع المسؤولية الجزائية وفي رسم سبل إصلاح المجرم وحماية المجتمع من الخطورة الاجرامية [2].

ونلاحظ أن المشرع الجنائي في العراق قد واكب التطور الذي يعيشه البلاد وخاصة بعد عام 2003 بعد أن تغير نظام الحكم فيه، فقد تغيرت السياسة الجنائية لتواكب التطور على الصعيد الإجتماعي والأقتصادي والسياسي، إذ تضمنت السياسة الجنائية الجديدة في العراق عدة قوانين لمكافحة الجريمة، ومن هذه القوانين، قانون مكافحة الارهاب رقم (13) لسنة 2005 وقانون جهاز مكافحة الارهاب رقم (31) لسنة 2016 وقانون هيئة النزاهة، وجميع هذه القوانين تعد سياسة جنائية مواكبة للتطور الذي يعيشه البلد.

وقد إتخذ المشرع الجنائي في العراق سياسة جنائية تحوطية عند تشريع نصوص التجريم الاساسية، بمعنى أنه لا يعاقب المشرع الجزائي إلا على النشاط الخارجي المحسوس الذي يتجلى بأفعال مادية تحدث اضطراباً اجتماعياً، لذا فلا عقوبة على التفكير في الجرائم أو العزم على إرتكابها، ولا على التحضير والتهيئة له. وما لم يتعدى الفاعل هذه المرحلة ويصل إلى مرحلة الشروع اي البدء بالتنفيذ فلا عقاب يترتب عليه. لأن المشرع الوضعي لا سلطان له على الضمائر ولان الفكرة ما دامت كامنه في نفس صاحبها ولم يعمل على تحقيقها بفعل خارجي مادي فهي حتى ذلك الوقت لا تؤذي أحدا وليس فيها إخلال بنظام المجتمع، وقد أخذ المشرع العراقي بنهج التجريم التحوطي من خلال فهم نصوص

(1) - د، حيدر علي نوري، سياسة التجريم دراسة مقارنة، رسالة ماجستير، جامعة النهرين، كلية القانون، 1999، ص 58.

(2) - د. واثبة داود السعدي، المرجع السابق ، ص 160.

مواد قانون مكافحة الإرهاب لكونه قد حذر وحدد الأفعال التي من الممكن أن ترتقي إلى فعل إرهابي يعاقب علية الشخص[1] .

المطلب الثاني

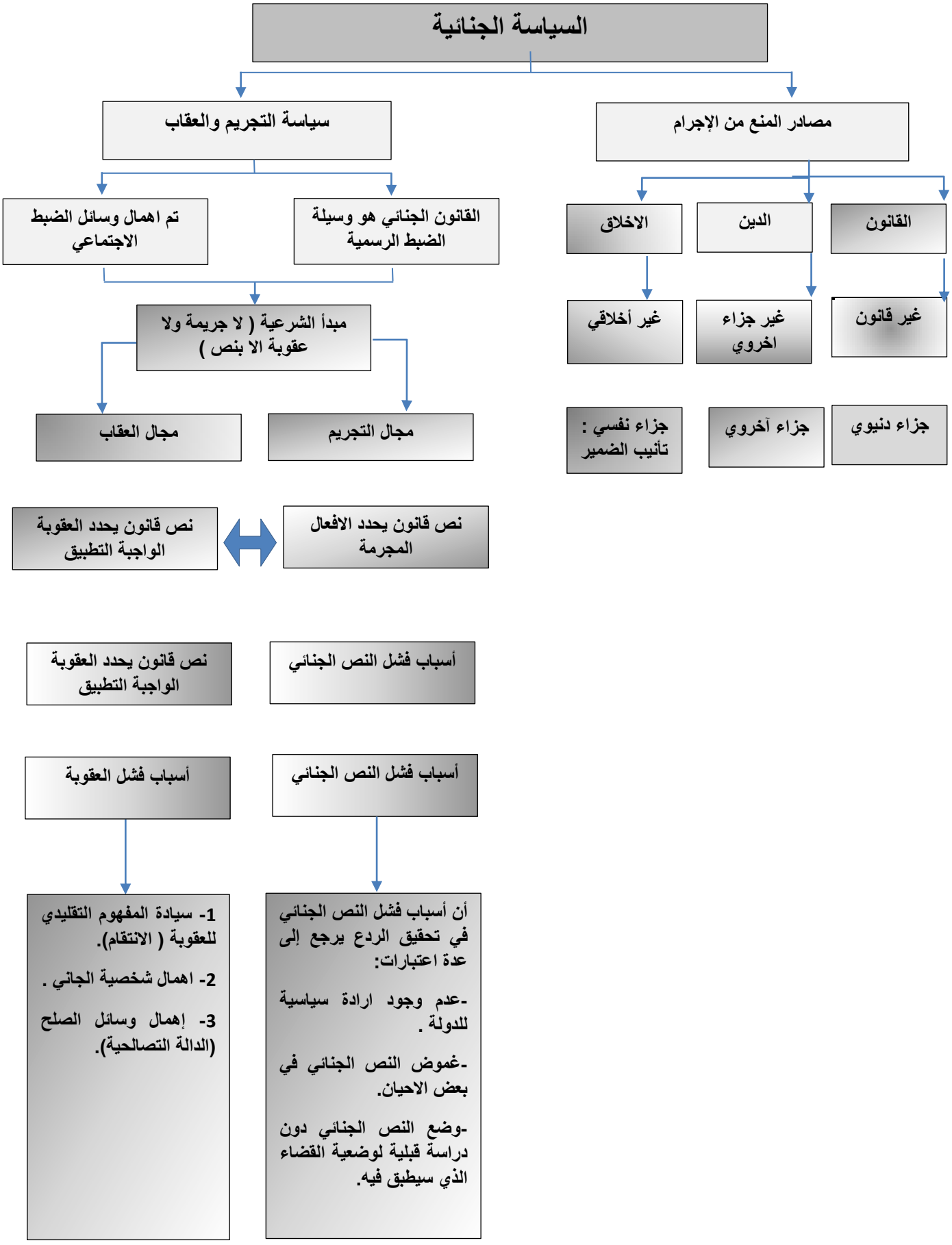
مدى ملاءمة مبادئ التجريم والعقاب لمقتضيات السياسة الجنائية

تتخذ سياسة التجريم مجموعة من المبادئ والأسس النظرية والفلسفية التي تضع النموذج العام الذي تعتمده التشريعات الجنائية في تجريم الأفعال وسلوك الأفراد والجماعات. وقد عرفت هذه الافكار والنظريات تطورات متلاحقة منذ ظهور القانون الجنائي مع التجمعات القديمة التي كانت وراء ظهور فكر جنائي جديد تمثل في بروز مجموعة من المدارس الفقهية. وهو ما أعطاها صبغة متميزة عن غيرها من التشريعات الجنائية الوضعية.

وعلى أساس ذلك سنقسم هذا الموضوع إلى فرعين، نتكلم في الاول عن اثر السياسة الجنائية في التجريم، ونخصص الفرع الثاني لدراسة أثر السياسة الجنائية في العقاب.

وقبل الشروع في دراسة وتوضيح مدى ملاءمة وأثر السياسة الجنائية في كل من التجريم والعقاب، سنوضح بشكل مخطط مدى تأثر السياسة الجنائية في التجريم والعقاب وما هي العوامل الإجتماعية، والأقتصادية، والدينية، والسياسية، في وضع السياسة الجنائية، وما هي أسباب فشل النص الجنائي والعقابي في بعض الاحيان.

(1) - د. اردلان نور الدين محمود ، سياسة التجريم والعقاب في قانون مكافحة الارهاب ، بحث منشور ، جامعة سوران ، سليمانية، العراق، 2013 ، ص7.


السياسة الجنائية
سياسة التجريم والعقاب
مصادر المنع من الإجرام
تم اهمال وسائل الضبط الاجتماعي
القانون الجنائي هو وسيلة الضبط الرسمية
الاخلاق
الدين
القانون
مبدأ الشرعية (لا جريمة ولا عقوبة الا بنص)
غير أخلاقي
غير جزاء اخروي
غير قانون
مجال العقاب
مجال التجريم
جزاء نفسي : تأنيب الضمير
جزاء آخروي
جزاء دنيوي
نص قانون يحدد العقوبة الواجبة التطبيق
نص قانون يحدد الافعال المجرمة
نص قانون يحدد العقوبة الواجبة التطبيق
أسباب فشل النص الجنائي
أسباب فشل العقوبة
أسباب فشل النص الجنائي
1- سيادة المفهوم التقليدي للعقوبة (الانتقام).
2- اهمال شخصية الجاني .
3- إهمال وسائل الصلح (الدالة التصالحية).
أن أسباب فشل النص الجنائي في تحقيق الردع يرجع إلى عدة اعتبارات:
-عدم وجود ارادة سياسية للدولة .
-غموض النص الجنائي في بعض الاحيان.
-وضع النص الجنائي دون دراسة قبلية لوضعية القضاء الذي سيطبق فيه.

الفرع الأول

أثر السياسة الجنائية في التجريم

تتخذ الدولة السياسة الجنائية كوسيلة لحماية المصالح التي تمثل الحياة الإجتماعية والأقتصادية والسياسية، وعلى أساس ذلك ترسم السياسة الجنائية، إذ تتلاءم مع واقع المجتمع والنظام السياسي القابض على السلطة[1]، ومن خلال ذلك فإذا رأت الدولة أن المصالح تستوجب أقصى مراتب الحماية القانونية عبرت عن ذلك بالعقوبة. وتتحدد المصالح الجديرة بالحماية الجنائية وفقا لظروف وأحتياجات كل مجتمع وتتأثر بتقاليده ونظامه الاقتصادي والاجتماعي والسياسي. وإذ يُعد التجريم هو وسيلة لتحقيق غاية، وهذه الغاية تتمثل بحماية النظام العام سواء على الصعيد المحلي أم الدولي.

ويتمثّل الأساس الفكري للسياسة الجنائية بمجموعة النظريات والأفكار والآراء التي جاء بها الفلاسفة والمفكرون والفقهاء، وبما أن السياسة الجنائية هي سياسة فلسفية وتشريعية، فلا بد من تأثرها بالأفكار الفلسفية والسياسية ، وللسياسة الجنائية صورتان نظرية وعملية، أما الصورة النظرية فتتمثل بالنظريات الفلسفية التي إستمدت السياسة الجنائية وجودها التي تحدد أو ترسم اتجاهاتها العامة، أما الصورة العملية فتعبّر عن الإيديولوجية التي يتبناها النظام السياسي داخل الدولة، والتي تختلف بحسب طبيعة النظام الحاكم[2].

ويجدر الاشارة إلى أن هناك علاقة وثيقة بين كل من سياسة التجريم والسياسة العقابية، فالقاعدة العقابية تتضمن شقين: التكليف بسلوك اجتماعي معين، فضلا عن ذلك يوجد جزاء جنائي يترتب على مخالفة هذا التكليف، وهو العقوبة. وهذا يدل على مدى العلاقة الوثيقة بين كل من سياسة التجريم والسياسة العقابية[3].

وعرفت سياسة التجريم بأنها: سياسة تشريعية تتحكم فيها الدولة تهدف إلى أختيار صورة السلوك الانساني التي تنتهك مصالح وقيم المجتمع الجديرة بالحماية، ومن ثم تستحق اللوم والعقاب، فالتجريم هو (إضفاء عدم المشروعية على سلوك معين يشكل إعتداءً أو خطراً على المصالح ، والقيم الأساسية التي يتوقف عليها إستمرار المجتمع واستقراره)، إذ محل التجريم هو السلوك، ومناطة المصلحة، وهذا

---

(1) - د. نورس أحمد كاظم الموسوي، السياسة الجنائية في حماية الامن الفكري، المركز الديمقراطي العربي، المانيا، برلين، 2022، ص 63.

(2) - د. خالد مجيد عبدالحميد الجبوري ، النظرية العامة للتجريم الوقائي ، المركز العربي للنشر ، الطبعة الاولى ، 2018، ص11.

(3) - د. احمد فتحي سرور ، المرجع السابق، ص 18 .

يقتضي تحديد مصالح المجتمع، والقيم والمبادئ التي رسخت في ضمير الجماعة، ومن ثم نزع الشرعية عن كل فعل أو قول ينتهك هذه المصالح[1].

وتتعدد المصالح الجديرة بالحماية الجنائية وفقا لظروف واحتياجات كل مجتمع، وتتأثر بتقاليده ونظمه الاقتصادية والاجتماعية والسياسية، وعليه يُعد التجريم وفق سياسة جنائية هو أقصى مراتب الحماية التي يضيفها التشريع على نوع معين من المصالح التي تهم المجتمع ولما كانت المجتمعات بنظمها السياسية والاقتصادية والإجتماعية تتفاوت فيما بينها في تحديد هذه المصالح، فانه ولا بد تبعا لذلك من اختلاف سياسة التجريم فيما بين هذه المجتمعات والنظم.

وفي هذا الاطار تباشر الدولة وظيفتها الجنائية لحماية المصالح الاجتماعية التي تهم المجتمع فتختار الجزاء الانسب والاصلح والاقرب للتعبير عن مدى تقدير المجتمع لأهمية هذه المصالح.

فاذا قدرت الدولة ان المصلحة تستحق اقصى مراتب الحماية القانونية عبرت عن ذلك بتوجيه العقوبة المناسبة، واذا راجعنا التطور التاريخي للمصالح التي يحميها القانون، سوف يتضح لنا مدى تأثرها بنظام المجتمعات البشرية ومقومات حياتها، فالتغيرات الاجتماعية تعكس بصورة عامة التحولات التي تلحق بهيكل القيم الإجتماعية وتعكس بوجه عام التحولات التي تلحق القيم الإجتماعية وهذه القيم تمثل في جوهرها مجموعة من المعتقدات وأنواع السلوك التي يقبلها المواطنون في بلد معين[2].

وعلى أساس ذلك فإن معيار التجريم في أغلب الأنظمة، هو الخطورة الإجتماعية[3]، وأن سياسة التجريم تتوجه بشكل رئيس على الأفعال ذات الخطورة الاجتماعية كالتي تتعرض إلى نظام الدولة وأمنها ومؤسساتها وإلى شخص المواطنين وحرياتهم وحقوقهم المضمونة في الدستور وفي القانونين وعلى الافعال التي تمس الاقتصاد الوطني وتمثل نوعاً من إستغلال النفوذ وسوء إستعمال الصلاحيات الممنوحة[4]. وإن هذا المفهوم يتناسب ويتكامل مع طبيعة النظام لكل دولة وأهدافه على أنه الهدف الأساس للنظام وهو ما يشكل مفهوم الخطورة الاجتماعية والاقتصادي[5].

---

(1) - حازم زياد طالب دغمش، دور السياسة الجنائية في مواجهة الانحراف الفكري، رسالة ماجستير، الجامعة الإسلامية بغزة، كلية الشريعة والقانون، 2018، ص 15 .

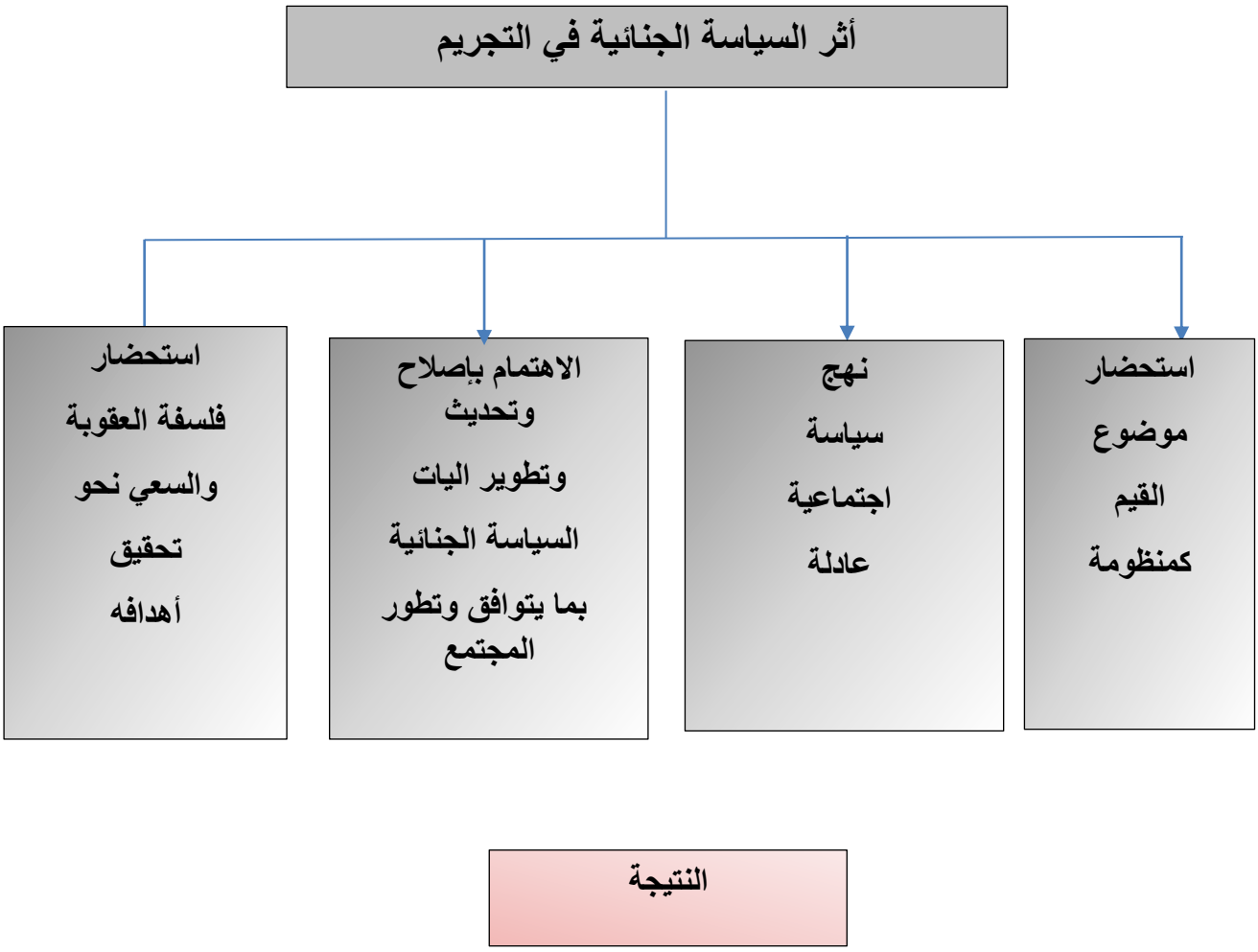
(2) - د. احمد فتحي سرور، أصول السياسة الجنائية، دار النهضة العربية، القاهرة، 1972 ص 18 وما بعدها .

(3) - د. محمد الرازقي، علم الاجرام والسياسة الجنائية، دار الكتاب الجديد، الطبعة الثالثة، بيروت، 2004، ص128.

(4) - د. علي حمزة عسل، د. خالد مجيد ، التجريم الوقائي في قانون حماية المستهلك العراقي، بحث منشور، مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد الاول، السنة التاسعة، 2017، ص 306 و 307.

(5) - د. واثبه داود السعدي، المرجع السابق، ص 174 .

ويمكن إيضاح أثر السياسة الجنائية في التجريم، على شكل مرتسم ومخطط، وما هي العوامل والمرتكزات الرئيسة التي يعتمدها المشرع الجنائي عند التجريم[1].



تقتضي السياسة الجنائية التركيز على الجانب الوقائي للحد من الظواهر الاجرامية قبل التفكير في وضع نصوص تجريميه وعقابية على كل مخالف لنص قانوني من منطلق ان السياسة الاستباقية لها دور مهم في منع العديد ن الجرائم إذ انها تتدخل قبل وقوع الجريمة والحال أنه في بعض الأحيان يكون القانون نفسة عاملا رئيسيا للأجرام .

ونخلص إلى أن أثر السياسة الجنائية يتركز في معالجة ومكافحة الخطورة الاجتماعية (الجريمة) والتي تمس الأمن والنظام العام للدولة ومؤسساتها، وكذلك نلاحظ أن أثر السياسة الجنائية تتبنى حماية الاسرة وتقوية روابطها الإجتماعية التي لا تتعارض مع مقومات وعادات المجتمع، وأيضا حماية حرية وامن

(1)- عماد أكضيض ، إشكالية السياسة الجنائية والعقابية ودور التوجهات الحديثة في مكافحة ومنع الجريمة، بحث منشور، على الموقع، https://lm.facebook.com/l.php?u=https%3A%2F%2Fdrive.google.com، تم زيارة الموقع بتاريخ 2021/10/17، ص 17 .

وكرامة المواطنين من خطر التجاوزات المجرمة، وضمانة تطبيق بعض الأحكام التي وردت في الدستور، كحظر النشاط الذي يستهدف تفتيت الوحدة الوطنية أو إثارة النعرات العنصرية والطائفية. لذا على المشرع الجنائي العراقي الأخذ بمعيار الخطورة عند تشريعه لأي قانون، ونخص بالذكر عند تشريع قانون مكافحة الجرائم الالكترونية والمعلوماتية، وايضا عند إجراء أي تعديل للقوانين الجزائية لسد النقص التشريعي الذي بدأ يظهر لنا جليا بسبب التطور التكنولوجي والتقني السريع الذي يعيشه العالم، وبدأت الجرائم الإلكترونية تنتشر في شتئ تفاصيل الحياة، وهذه الأخيرة تختلف اختلافا كبيراً عن الجرائم التقليدية، ومن الصعب ان تنطبق عليها القوانين التقليدية.

الفرع الثاني

أثر السياسة الجنائية في العقاب

الأصل في الإنسان هو الحرية في العيش، ولكن غاية المشرع والمجتمع بصورة عامة بالنسبة لمرتكب الجريمة إذا ثبتت مسؤوليته الجنائية هو توقيع الجزاء الجنائي عليه، ولا يكون ذلك إلا وفقاً لمبدأ الشرعية في التجريم والعقاب، ولا يأتي ذلك إلاّ بعد أن يتم تحريك الدعوى الجزائية ومباشرتها من طرف الإدعاء العام والتي يصدر من جهة الحكم بعد إتباع الإجراءات حكماً جزائياً قابلاً للتنفيذ، وجميع هذه الاجراءات تُعد ضمانات لكرامة الانسان، ويقع على عاتق الدولة تنفيذ هذه الحكم لأنه لا يمكن توقيع عقوبة إلاّ بوجود حكم أو قرار صادر عن هيئة قضائية مختصة[1].

فالتجريم يعني إضفاء الحماية الجزائية على مصلحة معتبرة، من المصالح الاجتماعية التي تهم المجتمع، ومنع أي مساس يصيبها يؤدي إلى إهدارها أو تدميرها أو الإضرار بها، كليا أو جزئياً، ففعل الضرر الذي يهدد المصالح ما هو إلاّ نشاط مخل بالحياة الإجتماعية، وعلى ضوء ذلك تباشر الدولة وظيفتها من خلال تشريع نصوص جزائية لحماية هذه المصالح الاجتماعية والاقتصادية والسياسية وغيرها، فيتم تشديد وتخفيف العقوبة على أساس مدى تقدير تلك المصالح وقيمتها لكل مجتمع وبيئة. فهناك علاقة وثيقة ومباشرة بين كل من سياسة لتجريم والعقاب، فالقاعدة الجزائية تتكون من شقين، الاول: التكليف بسلوك اجتماعي معين، والثاني: جزاء يترتب على مخالفة هذا التكليف وهو العقاب[2].

---

(1) - د. أزاوا عبدالقادر، د. دهيمي نجاة، السياسة الجنائية في جرائم الأعمال، بحث منشور ، المجلة الأفريقية للدراسات القانونية والسياسية، جامعة أحمد دراية، ادرار، الجزائر، مجلد، 3، العدد، 2، 2019 ، ص 129.

(2) - د. علي حمزة عسل، د. خالد مجيد ، التجريم الوقائي في قانون حماية المستهلك العراقي، المصدر السابق، ص304.

فالسياسة الجنائية هي التي تحكم الجزاء المترتب على وقوع الجريمة فتحدد أنواعها، وأهدافها، وأسلوب تطبيقها وتنفيذها، بمعنى هي التي تهدف إلى بيان رد الفعل الاجتماعي في مواجهة الجريمة، أي نوع ومقدار الجزاء الجنائي الذي يُعد الأكثر فعالية في حماية المصالح الاجتماعية الجديرة بالحماية ضد أي سلوك يشكل خطرا واعتداء عليها[1].

وبالنظر إلى سياسة العقاب والتي تُعد أداة لتنفيذ السياسة الجنائية، نجد أن هذه السياسة قد مرت بمراحل عدة تعكس كل منها درجة تطور المجتمعات البشرية ذاتها، إذ بدأت سياسة العقاب في العصور القديمة بفكرة الإنتقام من الجاني، وذلك بتعذيبه وفرض اقسى العقوبات عليه، ولأن الهدف من سياسة العقاب هو الإنتقام فلم يكن ينظر إلى تحقيق اصلاح الجاني أو تقويمه[2].

ويذهب بعضهم إلى أن أساس حق العقاب ومدى مشروعية الجرائم والعقوبات، يقول الاستاذ (بكاريا): إلى أنه " ينبغي أن تتوزع المصالح الموجودة في المجتمع على أساس التوزيع العادل والمتساوي، على الرغم أنه يلاحظ وجود عدد من هؤلاء الافراد الذين تتولد لديهم الرغبة العارمة في أن يستحوذ من جانبه على أكبر قدر من الامتيازات والنفوذ، وفي المقابل يترك جانب آخر وهم غالبية المجتمع في الضعف والشقاء، ولا يتم إيقاف ذلك إلا عن طريق سن تشريعات عادلة، بموجبها يتنازل الافراد بشكل مباشر عن بعض مصالحهم الخاصة، من أجل تحقيق المصالح الاكثر أهمية في المجتمع، أو يتركون للقوانين تنظيم تلك المصالح على اساس المفاضل والاولوية في حماية المصالح الجديرة بالحماية.

ومن هذا المنطلق يرى استاذنا الدكتور(أكرم نشأت ابراهيم) إلى أنه يجب أن تؤسس السياسة الجنائية، سواء في صياغتها، أو في تطبيقها على الحقائق العلمية، ويجب أن تتبنى السياسة الجنائية أفكار حرة وعلمية ترتكز على المصالح الإجتماعية والأقتصادية والسياسية الجديرة بالحماية، وعدم المساس بحرية وكرامة الأفراد، وعدم إنكار القيم الاخلاقية الراسخة في ضمير المجتمع، وضمان حقوقهم الدستورية[3].

وفي العصر الحديث وبالتحديد منذ أوائل القرن الثامن عشر تطورت سياسة العقاب تطورا ملحوظاً إذ إنصب أهتمام السياسة العقابية على شخصية الجاني، بوصفه إنسانا كسائر البشر، إذ اتجهت السياسة العقابية إلى الإعتماد على إصلاح الجاني وتقويمه، والعمل على إصلاح المؤسسات العقابية لتحقيق هذا الهدف، وثم تطورت السياسة العقابية وذلك بظهور ازدواجية الجزاء الجنائي تبعاً لفلسفة المدرسة الوسطية، والتي حاولت التوفيق بين المدرستين التقليدية والوضعية، وذهب رواد هذه المدرسة بأن

(1) - د. احمد فتحي سرور ، المرجع السابق، ص 96 .
(2) - د. نورس أحمد كاظم الموسوي، السياسة الجنائية في حماية الامن الفكري ، المصدر السابق، ص 68.
(3) - د. أكرم نشأت ابراهيم، المرجع السابق، ص 135.

العقوبة وحدها لا تكفي بل لا بد من تكميلها واسنادها بتدابير أخرى، لتجميد الخطورة المتوقعة التي تدل عليها ارتكاب الشخص للفعل الاجرامي [1].

ويلعب التشريع العقابي دوراً مهماً في الوقاية من الإجرام وذلك عندما يحقق التشريع التوازن بين حماية المجتمع وبين حماية حقوق الإنسان وحرياته داخل المجتمع، إذ إن السياسة العقابية تكون ناجحة عندما ينبثق عنها تشريع جنائي جيّد يوفّق بين مصلحة المجتمع وبين مصلحة الأفراد في إطار العلاقات الإجتماعية؛ لأن الإنسان هو أساس المجتمع وعلى المشرّع أن يضمن للإنسان حقوقه وحريته، إذ إن ضمانها كفيل على ضمان تجاوبه الفعلي مع المجتمع وعدم خرقه للأوامر والنواهي التي يتضمنها التشريع، ومن ثمّ عدم إقباله على ارتكاب الجريمة التي تهدد أمن المجتمع وسلامته الذي يعيش فيه، كما يعد التشريع الأداة الفاعلة في الوقاية من الإجرام وذلك من خلال إصدار العديد من القوانين التي تسهم بصورة مباشرة أو غير مباشرة في الوقاية مثل قانون التعليم الإلزامي وقانون الرعاية الاجتماعية وغيرها الكثير من القوانين التي تلعب دوراً بارزاً في الوقاية من الإجرام[2].

وعلى أساس ذلك فإن أثر السياسة الجنائية في العقاب يمكن أن نشاهدها في الوقاية المتمثلة في تلافي إرتكاب جرائم جديدة من المحكوم عليهم، أو من الاخرين. وكذلك يتمثل اثر السياسة الجنائية في العقاب من خلال إصلاح واعادة تربية المحكوم عليهم وتعويدهم على احترام قواعد الحياة الإجتماعية. وأيضا نرى اثرها في الردع " الخاص والعام" المتمثل بإيقاع العقاب المناسب لإصلاح المحكوم عليه، ولتلافي إرتكاب جرائم أخرى من قبله ومن الآخرين[3].

وتمتاز السياسة العقابية على أنها وقائية، تتمثل مهمتها الرئيسة في مواجهة الخطورة الاجتماعية للفرد ويكون ذلك عن طريق إتخاذ التدابير اللازمة من أجل منع إرتكاب الجريمة، فالسياسة العقابية هي بمعنى تناسب العقوبة مع الجرم المقترف، فالقانون الجنائي في كل زمان ومكان يهدف إلى تحقيق العدالة ، فالقانون يقف إلى جانب العدالة ومن ثم اذا تحقق احدهما دون الاخر فإن ذلك لا يجدي نفعاً[4]. فلكي تتحقق العدالة لابد من وجود مبادئ لتحقيقها، ومن اهم المبادئ التي جاءت بها السياسة العقابية الحديثة هو مبدأ التناسب، ويتوجه مضمون هذا المبدأ إلى المشرع، وينبه على ضرورة مراعاة التناسب بين ايلام العقوبة الجنائية والجريمة التي تقررت لها هذه العقوبة فإنه من الواجبات التي تقع على عاتق المشرع عند تحديده لشق الجزاء العقابي من القاعدة الجنائية[5].

---

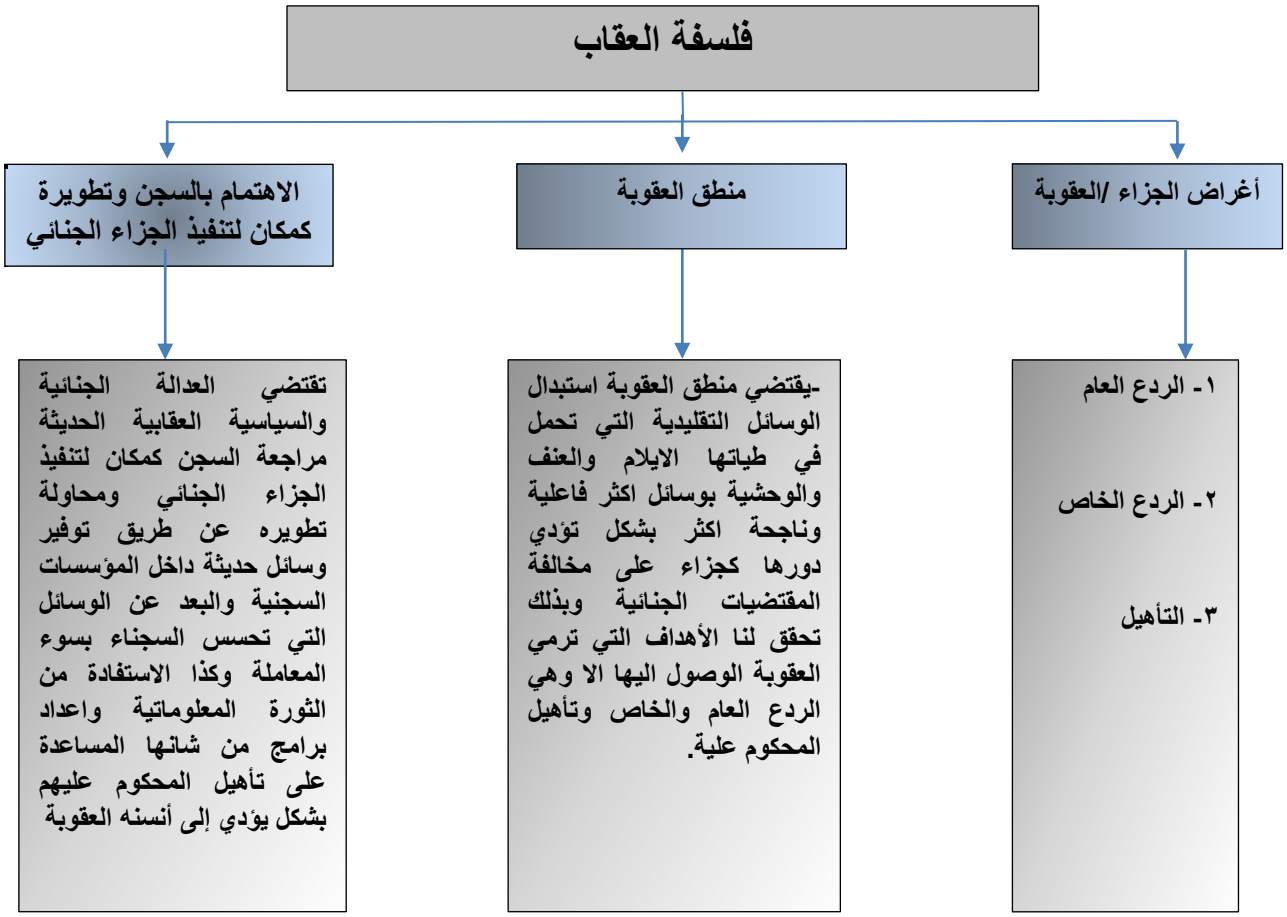
(1) - حازم زياد طالب دغمش، المرجع السابق، ص 17 .
(2) - سعداوي محمد صغير، السياسة الجزائية لمكافحة الجريمة ، المصدر السابق، ص 243.
(3) - د. واثبة داود السعدي، المرجع السابق، ص 181 .
(4) - فاضل عباس الملا ، اصول التشريع الجنائي الاسلامي ، الطبعة الاولى ، 2005، ص83.
(5) - محمود نجيب حسيني، علم العقاب، دار النهضة العربية، طبعة 3 ، القاهرة ، 1973، ص 64.

ونخلص إلى أن السياسة الجنائية ومدى ملائمتها لسياسة التجريم والعقاب يمكن أن تتمثل ببعض النقاط التالية[1]:

1- في السياسة الجنائية الحديثة لا بد من مراعاة حقيقة، وهي أن الجريمة هي حالة اجتماعية وليست مشكلة قانونية، لذلك يتطلب في السياسة الجنائية دوراً فعالاً من خلال الأهتمام بالوقاية من الجريمة قبل وقوعها، ومعالجة الجريمة بعد وقوعها.
2- على المشرع الجنائي ومن خلال السياسة الجنائية تجاوز جميع الخلافات العقائدية في الفكر الجنائي، وتحتضن مختلف التيارات الفكرية في مواجهة ظاهرة الاجرام.
3- يجب إعطاء الاولوية لسياسة المنع (منع الجريمة) وتغليبها على سياسة التجريم والعقاب.
4- من ضمانات وأولوية السياسة الجنائية هو احترام الحقوق والحريات لجميع الامم والمجتمعات، وفقا لشرائع الديانات السماوية والقوانين الوضعية، وذلك لضمان استقرار وتقبل القوانين وحيادتها.
5- نرى أثر السياسة الجنائية في العقاب من خلال اعتماد معيار تصنيف العقوبات المقررة لكل فعل غير مباح وحسب جسامة الفعل، فالسياسة الجنائية تلجأ إلى المعيار الموضوعي لتضيف جسامة وخطورة الافعال التي تمس المصلحة المعتبرة، وعلى أساس ذلك تم تقسيم الجرائم إلى (جناية وجنح ومخالفات) وكذلك تم تقسيم العقوبات من الإعدام نزولاً إلى العقوبات التكميلية والتبعية والغرامات إلخ. وجميع هذه التصنيفات والتي هي نتاج وثمرة السياسة الجنائية للمشرع الجنائي لكل نظام قانوني متكامل، له الاثر المباشر اتجاه الجرائم الالكترونية، من خلال مدى مطابقة القوانين والتشريعات الحديثة التي تشرع لمواكبة ومكافحة الجرائم التكنولوجية والتقنية الحديثة[2].

ومن خلال دراستنا لأثر السياسة الجنائية في العقاب، يمكن أن نوضح بشكل مرتسم يبين مدى فلسفة السياسة الجنائية وأثرها في العقاب[3].

(1) - عبدالوهاب عبدالرزاق التحافي، اتجاهات السياسة الجنائية لمواجهة الجرائم الاجتماعية، مقالة منشورة، مجلة الزمان 24 الدولية ، العدد 1764 ، 2016، ص 5 .
(2) - د. أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دار هومه، 2019، ص 32.
(3) - عماد أكضيض ، إشكالية السياسة الجنائية والعقابية، المصدر السابق، ص 9.


فلسفة العقاب
أغراض الجزاء /العقوبة
منطق العقوبة
الاهتمام بالسجن وتطويرة كمكان لتنفيذ الجزاء الجنائي
١- الردع العام
٢- الردع الخاص
٣- التأهيل
-يقتضي منطق العقوبة استبدال الوسائل التقليدية التي تحمل في طياتها الايلام والعنف والوحشية بوسائل اكثر فاعلية وناجحة اكثر بشكل تؤدي دورها كجزاء على مخالفة المقتضيات الجنائية وبذلك تحقق لنا الأهداف التي ترمي العقوبة الوصول اليها الا وهي الردع العام والخاص وتأهيل المحكوم علية.
تقتضي العدالة الجنائية والسياسية العقابية الحديثة مراجعة السجن كمكان لتنفيذ الجزاء الجنائي ومحاولة تطويره عن طريق توفير وسائل حديثة داخل المؤسسات السجنية والبعد عن الوسائل التي تحسس السجناء بسوء المعاملة وكذا الاستفادة من الثورة المعلوماتية واعداد برامج من شانها المساعدة على تأهيل المحكوم عليهم بشكل يؤدي إلى أنسنه العقوبة

المبحث الثاني

الدور التكنولوجي وأثره في السياسة الجنائية

إن الحديث عن الدور التكنولوجي وأثره في السياسة الجنائية، يتطلب منا في البدء تتبع المسار التاريخي لطبيعة هذا التطور، ومدى تأثيره في فروع القانون بصورة عامة، ومدى الحاجة لهذه التكنولوجيا في شتى تفاصيل الحياة وما هي الحماية المقررة لها ، وعلى ضوء ذلك سنتناول في هذا المبحث التنظيم القانوني للتطور التكنولوجي في مطلب أول، ونخصص دراستنا في المطلب الثاني لدور السياسة الجنائية في مواجهة الجرائم التكنولوجيا.

المطلب الأول

التنظيم القانوني للتطور التكنولوجي

ظهرت الحاجة إلى إستعمال التكنولوجيا الحديثة الحاسب الآلي وجميع البرامج الإلكترونية في ظل التطور الذي يعيشه العالم من عولمة فكرية وأقتصادية وإجتماعية وسياسية، في السنوات الأخيرة، ولغاية يومنا هذا، ومع هذا التطور التكنولوجي، ومدى الحاجة الفعلية للتعامل والتواصل بين جميع المجتمعات على الصعيد الدولي والمحلي، فقد رافق قلق حول مدى أمن هذا التطور الالكتروني، مما أدى إلى الأهتمام بدراسة التنظيم القانوني لهذا التطور التكنولوجي والتقني من قبل الباحثين والقانونيين، لضرورة سد الفراغ التشريعي في هذا الشأن، ووضع تنظيم قانوني لاستخدام هذا التطور التقني، من خلال تشريع قوانين تحكم الضوابط الاخلاقية والقانونية للتعامل مع هذا التطور. ومن أجل الإحاطة بهذا التنظيم سنقسم هذا المطلب على ثلاثة فروع، نتناول في الفرع الاول دراسة الطبيعة القانونية للتطور التكنولوجي، ونخصص دراستنا في الفرع الثاني لبحث الضوابط القانونية والاخلاقية للتطور التكنولوجي، اما الفرع الثالث نخصصه لدراسة أثر التطور التكنولوجي في السياسة الجنائية.

الفرع الاول

الطبيعة القانونية للتطور التكنولوجي

للتطور التكنولوجي إيجابيات كثيرة ومتنوعة، ومن خلالها بدأ العالم يجني ثمار هذا التطور وعلى جميع الأصعدة (الإجتماعية والأقتصادية والسياسية والصحية والتقنية)، عن طريق شبكات الإنترنت، وهذه الاخيرة أدت إلى أن ربط العالم والشعوب بعضها ببعض وأصبح التواصل عن بعد سهل وممكن،

وقربت المسافات بين جميع الشعوب وألغت الحدود [1]. مما أدى هذا التعامل إلى تسارع الأحداث، وقد تطور مفهوم التطور التكنولوجي إلى التعامل مع عدة أنواع من الأجهزة الحديثة، ولا يقتصر الأمر على جهاز الكمبيوتر فقط، وإنما شمل استخدام جميع التقنيات الحديثة وعلى أساس ذلك يُعد الانترنت هو أكبر بوابه عالمية تم اكتشافها إلى الآن، وذلك لان الشخص يستطيع ان يقوم بالأعمال والتصرفات والتواصل مع الجميع وهو في مكانه[2].

وقد انقسم الفقه الجنائي إلى ثلاثة اتجاهات في تحديد الطبيعة القانونية للتطور التكنولوجي، إذ ذهب **الاتجاه الاول** : بالقول إلى أن المعلومات والبيانات الرقمية بأنواعها، والتي هي تمثل جوهر التطور التكنولوجي، هي ذات طبيعة معنوية لا يمكن الاستئثار بها، فأنها لا تدخل ضمن طائفة القيم المشمولة بالحماية ما لم تكن تنتمي إلى مجموعة من الاشياء المادية الفنية أو الافكار الادبية والتي يحميها القانون، كالحقوق الفكرية والادبية والفنية والاقتصادية، وهذا ما أدى ببعضهم إلى عدّ هذا التطور من طائفة المنافع والخدمات . **أما الاتجاه الثاني:** فقد كان رأيه مغايراً وذلك من خلال اعطاء القيمة المعنوية والمالية والاقتصادية لهذا التطور والتقنية الحديثة المتمثلة بجميع تفاصيل التطور التكنولوجي وشبهوا هذه القيمة كغيرها من القيم الاخرى التي تعد من قبيل الحقوق المالية والمادية والمعنوية، ومن المؤيدين لهذا الإتجاه هما الفقيهان الفرنسيان (vivant و catala). فالفقيه (catala) يرى ان المعلومات التقنية وما ينتج عنها هي بحد ذاتها قيمة مالية ومعنوية ويمكن أن تكون لها قيمة قابلة للتملك في ذاتها، بغض النظر عن الوسيط المادي الذي يحتويها، وقد شبهت هذه المعلومات بالسلع من حيث أن كليهما نتاج العمل البشري وتدخل ضمن حيازة الشي للمالك بصورة مشروعة وتصلح للتعامل بها؛ كونها تمثل قيمة معنوية لصاحبها بالإضافة إلى القيمة الإقتصادية والمالية [3].

وهناك من قال أن طبيعة التطور التكنولوجي تمتاز بكونها ذات طبيعة خاصة[4]، إذ أنه يكون نظاماً علمياً وفنياً متسارعاً ومتطوراً، ومصطلح تكنولوجيا (technologie)هو مصطلح مشتق من كلمتين (techno) و (logie) وأول ظهور لهذا المصطلح كان في ألمانيا عام 1770 ، مهنة الفن أو صناعة يدوية، وأيضا تعني المعرفة النظامية، فالتكنولوجيا هي نظام فكري وعلمي، ومنهم من وصف

(1) - سليمان نبيل زعرب، الحماية الشرعية للحق في الخصوصية الالكترونية في الفقه الاسلامي، رسالة ماجستير، الجامعة الاسلامية بغزة، كلية الشريعة والقانون، 2020 ، ص 20.

(2) - د. علي هاشم عبدالحسن، الحماية الجزائية للأمن الاسري من التطور التكنولوجي (دراسة مقارنة) ، ط 1، دار مصر للنشر، القاهرة، 2021، ص 38.

(3) - محمد كمال محمود السوقي، الحماية الجنائية لسرية المعلومات الالكترونية (دراسة مقارنة)، دار الفكر والقانون، المنصورة، 2021، ص 45.

وكذلك: محمد علي سالم. حسون عبيد، الجريمة المعلوماتية، بحث منشور، مجلة جامعة بابل، العلوم الانسانية، مجلد 14، العدد 2، 2007، ص 92.

(4) - طوني ميشيل عيسى، التنظيم القانوني لشبكة الانترنت، من دون دار نشر، 2001، ص 373.

التطور التكنولوجي بأنه: جميع الوسائل المستخدمة في تشغيل ونقل وتخزين البيانات والمعلومات بشكل الكتروني وما ينتج عنها من برامج وأجهزة[1]. ومنهم من عبر عن التكنولوجيا على أنها ليست مجرد علم أو تطبيق العلم، أو مجرد أجهزة ، بل هي أعم وأشمل من ذلك بكثير فهي نشاط يشمل الجانب العلمي والتطبيقي[2].

أما تعريف التطور التكنولوجي فقد ذهب بعض الفقهاء إلى تعريف هذا التطور وقالوا بأنه" العلم الذي يمثل التعامل عن طريق الاجهزة الحديثة ويكون هذا التعامل في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تحميلها وتحليلها باستخدام برامج وتطبيقات تكنولوجية حديثة بشكل معلومات رقمية دقيقة جداً[3]. وعرفه بعضهم بأنه " مجموعة من البيانات الرقمية التي يمكن أن يتم التعامل بها بواسطة اجهزة الكمبيوتر والآلات متطورة، وهذه المعلومات والبيانات يمكن التعامل بها عن بعد وبسهولة وتخضع لإجراءات واحكام قانونية وعلمية[4]" وهناك من يعرف هذا التطور التكنولوجي على أنه " علم البيانات الرقمية المخزن بشكل رموز وارقام بواسطة جهاز الحاسوب لإنجاز مهمة ما"[5].

ويمكن القول ان الطبيعة القانونية للتطور التكنولوجي تتمثل بكونها ذات صفة متجددة ومستمرة في التطور في مجال المعلومات والتقنيات، أي أن هذا التطور والتكنولوجيا يرتبط ارتباطاً مباشراً بمجموعة من الأجهزة ذات التقنيات الحديثة والدقيقة والحساسة والتي تمتاز بالسرعة وسهولة الإستعمال والتشغيل والإخفاء والتخزين، ونقل البيانات الدقيقة، وجميع هذه الصفات والمميزات تَعد مميزات ذات طبيعة خاصة، لكونها غير مادية وفي الوقت نفسه ذات طابع له قيمة معنوية ومالية وقانونية[6].

فقد ظهرت نتيجة لذلك التطور التكنولوجي ونتيجة للتعامل عن بعد بواسطة الوسائل الالكترونية الحديثة والإنترنت، فقد ظهرت أيضاً مجموعة كبيرة من الجرائم الناشئة عن استعمال التكنولوجيا

---

(1) - مراد رايس، أثر تكنولوجيا المعلومات على الموارد البشرية في المؤسسة، رسالة ماجستير ، جامعة الجزائر، فرع الادارة، 2006، ص 28.

(2) - د. نور الدين زمام، أ. صباح سليماني، تطور مفهوم التكنولوجيا واستخداماته العلمية، بحث منشور، مجلة العلوم الانسانية والاجتماعية، جامعة محمد خيضر بسكرة، الجزائر، العدد الحادي عشر ، 2013، ص 165.

(3) - سعاد بومايله وفارس بوباكور، أثر التكنولوجيا الحديثة للإعلام والاتصال في المؤسسة الاقتصادية، مجلة الاقتصاد المناجمت، العدد 3، 2004، ص 205.

(4) - مراد رايس، أثر تكنولوجيا المعلومات على الموارد البشرية في المؤسسة، المصدر السابق، ص 29.

(5)- امير فرج يوسف، الاثبات الجنائي للجريمة الالكترونية، مكتبة الوفاء القانونية، الاسكندرية، ط1 ، 2011، ص63 .

(6)- د. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، 2007، ص 20 .

والانترنت ولأسباب كثيرة بدأت هذه الجرائم بالإزدياد[1]، وسبب ذلك هو لعدم وجود تشريعات قانونية دولية ومحلية كافية تلم وتحيط بهذه الجرائم الحديثة والمعقدة والتي تُعد هي وليدة التطور التكنولوجي، وكذلك لكون هذه الجرائم تمتاز بعدة خصائص تميزها عن الجرائم العادية والتي قد تكون أغلبها مقننه في قوانين العقوبات وغيرها من القوانين[2] .

ولدراسة الطبيعة القانونية للتطور التكنولوجي أهمية بالغة، لبيان الأحكام الموضوعية والاجرائية، وذلك لوجود اختلاف فيما اذا كانت ذات طبيعة خاصة على أساس أعتبار جرائمها تُعد ذات طبيعة خاصة أم أنها يمكن عدّها من الجرائم التقليدية. بمعنى أن البحث في التنظيم القانونية للتطور التكنولوجي، الغاية منه التحري عن النظام القانوني الذي تخضع له تلك الجرائم، بالإضافة إلى معرفة التنظيم القانوني للمسؤولية الجنائية[3].

فالتطور التكنولوجي يمكن القول إنه قد ظهر منذ عام (1860) عندما تمت أول محاولة ناجحة للاتصالات الهاتفية على يد العالم الالماني (فيليب رايز) ، وبعدها العالم الامريكي (جراهام بل) والذي يُعد أول من أنشأ نظام الهاتف في العالم في عام (1876) عندما سجل العالم (جراهام بل) براءة أختراعه والتي غيرت الكثير من نظام هذه الحياة، وتعد طفرة تكنولوجية نحو مستقبل التعامل عن بعد، وبعدها إنتشرت التجارب العلمية نحو اكتشافات عده للتطور في الاجهزة الذكية والحاسوب والإنترنت[4].

وظهر أول مصطلح لشبكات التواصل الإجتماعي عام (1954) من قبل (جون بارنز) والذي كان باحثا في العلوم الإنسانية في جامعة لندن، وظهرت في السبعينات من القرن العشرين بعض الوسائل الإلكترونية والإجتماعية والتي كانت بدائية في تصميمها، وقد سهلت التعاون والتفاعل الاجتماعي، مما

---

(1)- فايز احمد خليفة احمد بن يعروف، المواجهة التشريعية والامنية للجرائم المتصلة بمواقع التواصل الاجتماعي، أدارة مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، 2019، ص 37 .

وكذلك: نداء نائل فايز، خصوصية الجرائم المعلوماتية، رسالة ماجستير، جامعة النجاح الوطنية، كلية القانون، فلسطين، 2017 ، ص 9.

وكذلك: أشرف علي عقلة القواقزة، دور التشريع الاردني في مواجهة الجريمة الالكترونية وأثرها في أمن معلومات المكتبات، بحث منشور، مجلة دراسات علوم الشريعة والقانون، المجلد 47، العدد 1 و 2019، ص617 .

(2) - لينا محمد الاسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، ط1، دار الحامد للنشر، الاردن 1 ، 2015، ص 66 .

(3) - د. سعد معن ابراهيم، حسام حازم احمد، التحريض في وسائل النشر وكيفية مواجهته أمنيا، مكتبة القانون المقارن، بغداد، 2021 ، ص 85.

(4) - د. أحمد حمد الله أحمد، المسؤولية الجنائية الناشئة عن الاستعمال غير المشروع لخدمة الهاتف النقال، دار السنهوري، بيروت، 2017، ص 24 .

أدى هذا التفاعل إلى تطور العلاقات والسعي إلى تطوير مثل هذه البرامج[1].وقد كان أول ظهور لتطور المواقع الإلكترونية في عام 1983 عندما تم تأسيس شبكتين، الاولى باسم (arpane) وكان تخصص هذه الشبكة للإستخدامات العسكرية، أما الشبكة الثانية للإنترنت باسم (milnet) وخصصت للإستخدام المدني والتي تستعمل لتبادل المعلومات وتوصيل البريد الالكتروني[2]. وفي بداية التسعينيات، ففي عام (1995) ظهر أول موقع للتواصل وهو (classmates.com) والذي صممه (راندي كونرادز)، وكان الهدف من هذا البرنامج هو لتواصل مجموعة من الطلبة والاصدقاء الذين جمعتهم الدراسة في الماضي من أجل التواصل والصداقة[3].

الفرع الثاني

الضوابط القانونية والأخلاقية للتطور التكنولوجي

القانون الجنائي يمكن وصفة هو قانون القيم الإجتماعية، وهذه القيم تتمثل بمجموعة من الأفكار والمبادئ والتي تمثل المصلحة العامة (المصلحة المحمية) في كل زمان ومكان، ومن هذا المنطلق فأن القانون الجنائي هو الاجدر بحماية هذه المصالح، من الخطر والضرر الذي قد يصيب هذه القيم والمصالح العامة والخاصة، ومعيار الحماية والضوابط القانونية والاخلاقية التي على اساسها يعتمدها المشرع الجنائي في رسم وتشريع السياسة الجنائية، وهذه الأخيرة تسهم في تعزيز السياسة العمومية، من خلال توظيف العديد من أدواتها، سواء التشريعية عن طريق تضمين العديد من النصوص القانونية المنظمة لمجالات معينة، كالنصوص المنظمة لمجال حماية الآداب العامة، أو تعزيز القانون الجنائي بتشريع نصوص تسهم في الحد من جرائم السرقة[4].

ويمكننا القول أن انتشار المواقع الإلكترونية، وسهولة الوصول اليها، وتزايد وتطور برامج التواصل الإجتماعي (السوشيال ميديا) وما تتضمنها هذه المواقع الالكترونية من فعالية وجاذبية، ونشر لمحتويات اصبحت تسبب خللاً اجتماعياً واخلاقياً، ما يؤثر سلبا على المجتمع بصورة عامة، وعلى الاسرة بصورة خاصة، إذ أصبح الإرتياد لهذه المواقع سهلا ودون عناء، مما أدى هذا الأمر إلى خلق

(1) - شرحبيل غالب حميد ابو سويلم، اعتماد طلبة الجامعة الاردنية على شبكات التواصل الاجتماعي للحصول على الاخبار والمعلومات، رسالة ماجستير، جامعة الشرق الاوسط، كلية الاعلام، 2015، ص 35.

(2) - د. صدام حسين ياسين العبيدي، جرائم الانترنت وعقوباتها في الشريعة الاسلامية والقوانين الوضعية، المركز العربي للنشر، ط 1 ، 2019 ، ص 33 .

(3) - رشيدة فاريش ، نورة قاوش، تأثير مواقع التواصل الاجتماعي في أنتشار الجريمة الالكترونية في وسط المراهقين، رسالة ماجستير، جامعة أكلي محند والحاج البويرة، كلية العلوم الانسانية والاجتماعية، 2018 ، ص29 .

(4) - ملاطي هشام، السياسة الجنائية في علاقتها مع السياسات العمومية للدولة، بحث منشور، المجلة المغربية للسياسات العمومية، المجلد 12، العدد 22، 2017، ص 154.

مشاكل عديده، منها الإنحلال المجتمعي والأخلاقي ومنها ما يؤدي إلى التشجيع على ممارسة الجرائم والابتزاز الالكتروني وسرقة للأموال[1]، وقد تطور الامر إلى أن وصل ببعضهم إلى الانتحار بسبب هذه المواقع الالكترونية وما ينتج عنها من محتوى أصبح يشكل خطرا أكبر من الجرائم العادية وذلك لكون الجرائم العادية تطلب مجهودا بدنيا وأيام من اجل تحقيق الجريم، أما الجرائم الالكترونية فإنها تمتاز بكونها سهلة جدا ولا تتطلب أي مجهود بدني وتمتاز بسرعة انجازها وسهولة إخفاء هوية المجرم دون أن يترك أي أثرٍ له [2].

ويعتمد المشرع الجنائي في بعض الاحيان عند وضع السياسة الجنائية، الاخذ بمعيار أو الضابط التشريعي والقضائي في تجريم بعض الافعال، ففي أغلب التشريعات الوضعية يحاول المشرع الجنائي إلغاء بعض النصوص، أو تعديلها وفقا لظروف كل بلد ومجتمع، وعليه الأخذ بنظر الإعتبار مواكبة التطور الذي يعيشه المجتمع في كل مجالات الحياة، وإذ إن هذه الأسس هي التي يهتم لها المشرع الجنائي عند دراسته لعلم الإجرام، وهذه الدراسة تكون ذات مضمون مختلف ومتفاوت من مجتمع لآخر، ولكل بيئة ثقافية تشريعها الخاص، وهذا ما يؤدي إلى استحالة وضع معيار ثابت لتجريم بعض الأفعال [3].

وهناك من يعتمد المعيار الشعبي ضمن الضوابط القانونية والأخلاقية لمواكبة التطور التكنولوجي، ويتمثل هذه المعيار بالأخذ بفكرة التصور القانوني والاخلاقي للفعل الذي يشكل رفضاً شعبياً وعدم تقبل لمثل هذه الأفعال، فقد يرى المجتمع ضرورة معاقبة بعض أنماط الحياة والتي تمثل سلوكاً وتصرفاً غير مقبول، قد تمس، أو تضايق، أو تجرح الشعور. وهذا ما نلاحظه في بعض المجتمعات التي تحرم تشريعاتها الزنا أو الأجهاض أو الدعاية ضد منع الحمل على سبيل المثال، ولكن هذه الافعال اصبحت لدى بعض المجتمعات من الامور التي تدعو إلى السخرية، مما يضطر المشرع إلى إلغائها أو التعديل على احكامها، وهناك بعض القوانين والتشريعات التي تجرم بعض المنشورات التي تجرح الشعور والكرامة، فقد أصبحت هذه الأفعال مرفوضة وغير مقبولة من قبل الطبقة المثقفة، في حين أنها لا تشكل فعل محظوراً في السابق[4].

ولقد نتج عن هذا التطور التكنولوجي مجموعة كبيرة من المواقع المشبوهة والتي هدفها هو الإخلال بالآداب العامة، وذلك من خلال نشر الفساد والإنحلال وهدم المبادئ العامة والاخلاق والقيم الاجتماعية

(1) - سحر فؤاد مجيد، جريمة التحرش الجنسي بالأطفال عبر الانترنيت، بحث منشور، المجلة الاكاديمية للبحث القانوني، العدد الخاص، 2017، ص 308.
(2) - نادر عبدالكريم الغزواني، الحماية الجنائية من جرائم الانترنت، دون دار نشر ، ص 60.
(3) - د. عبدالفتاح بيومي حجازي، المصدر السابق، ص 339.
(4) - د. محمد الرازقي، علم الاجرام والسياسة الجنائية، دار الكتاب الجديد، ط 3، لبنان، 2004 ، ص 26 .

وبالأخص القيم العربية والاسلامية، ونتيجة لانتشار هذه المواقع وبعض وسائل الانترنت وهو نتائج التطور التكنولوجي، فلقد وفرت هذه التكنولوجيا بيئة مناسبة لانتشار الفساد الاخلاقي والتشجيع على إنتهاك الآداب والأخلاق العامة، وهنا يظهر الدور الكبير للمشرع الجنائي عند وضع السياسة الجنائية والتي يجب أن تكون هذه الأخيرة مواكبة للتطور التكنولوجي وتؤسس على أساس حماية المصالح العامة، ووضع التدابير اللازمة للوقاية من الجرائم الناشئة عن التطور التكنولوجي وما يمس الأخلاق والآداب العامة[1].

وعلى ضوء ذلك فقد انقسم الفقه في تحديد الضوابط القانونية والأخلاقية للتطور التكنولوجي إلى اتجاهين: **الاتجاه الاول:** ويرى أن تتمثل الضوابط القانونية والأخلاقية للتطور التكنولوجي بأنها قواعد عامة، بمعنى ان التعامل مع هذا التطور يكون تعاملاً معنوياً وليس مادياً، وذلك على أن التطور التكنولوجي يُعد من قبيل الملكية الفكرية والتعامل بمعلومات ليست مادية وانما فكرية، ومثال على ذلك عندما يتم سرقة مال معلوماتي غير مادي، أو في حال الاستعمال غير المشروع للبيانات أو المعطيات المخزنة داخل نظام الحاسوب أو الاجهزة التقنية الحديثة الاخرى، فهذا الأمر ينطوي ضمن الأحكام الخاصة بسرقة المعلومات والتي ليس لها وجود مادي[2].

أما الاتجاه الثاني: فقد ذهب هذا الإتجاه إلى تحديد الضوابط القانونية والأخلاقية على أنها مجموعة من القيم قابلة لاستحواذ مستقلة عن قيمتها المادية، أي أن هذه المعلومات لها قيمة اقتصادية ومعنوية قابلة لآن تحاز حيازة مشروعة، وأنها ترتبط بمؤلفها عن طريق علاقة التبني، أو ما يسمى (براءة الإختراع). كما أنه توجد علاقة قانونية تتمثل في علاقة المالك بالشيء الذي يملكه، أو يخترعه أو الذي ينشره. وإن هذا الشيء يستحق الحماية القانونية ومعاملته معاملة المال. ويذهب بعضهم إلى أنه يجب التفرقة بان هناك مالاً معلوماتياً مادياً فقط ولا يمكن أن يخرج عن هذه الطبيعة، وهي الآلات وأدوات الحاسوب الالي، وإن هناك من المال المعلوماتي المادي والذي يحتوي على مضمون وقيمة معنوية حقيقية، وهو المال المادي مثل ، الذاكرة أو الأسطوانة الممغنطة أو الأسلاك التي تنتقل منها الإشارات عن بعد. كما هو الحال في جرائم التجسس عن بعد[3].

وتأسيسا على ما تقدم فهناك من صنف الحدود الأخلاقية للتطور التقني على النحو الاتي:

---

(1) - هروال هبة نبيلة، جرائم الانترنت (دراسة مقارنة) أطروحة دكتوراه، جامعة أبي بكر بلقايد، كلية الحقوق والعلوم السياسية، الجزائر، 2014، ص 143 .

(2) - م. لينا محمد الاسدي ، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، دار حامد للنشر، الاردن، 2015 ، ص 30.

(3) - براهيمي جمال ، الجرائم المعلوماتية في القانون الجزائري واليمني، أطروحة دكتوراه، جامعة تيزي وزو، كلية الحقوق، 2018، ص 118. وكذلك ينظر: عبدالله دغش العجمي، المشكلات العملية والقانونية للجرائم الالكترونية (دراسة مقارنة) رسالة ماجستير ، جامعة الشرق الاوسط، كلية القانون، 2014، ص 14.

1- المعلومات الشخصية: أسفر التطور التقني في السنوات العشر الأخيرة عن معضلة المعلومات الشخصية وكبرى الشركات، بتعبير آخر كيف ستستغل كبرى الشركات المعلومات التي تتوفر لها عن الأشخاص، إذ تسعى هذه الشركات بشكل مستمر أن تجمع معلومات خاصة على الأفراد، من أجل تلبية احتياجاتهم عن طريق تقديم الخدمات أو البضائع وذلك من خلال معرفة البضائع التي يبحث عنها الزبائن، يحتاج السياسيون كذلك لمعلومات عن المسائل العامة والخاصة التي تخص الشأن السياسي من قبل الناخبين، بهذا تثار مشكلة كبرى حول متى تتجاوز الشركات حدود ونطاق المعلومات الشخصية للأفراد [1].

2- المعلومات الخاطئة وغير الدقيقة: استخدم السياسيون في الولايات المتحدة الأمريكية بين الأعوام 2016 و2020 منصات التواصل الإجتماعي للتمرير معلومات كاذبة من أجل استقطاب الجماهير لهم في المشهد السياسي، ولا يقتصر الحال على السياسيون فمنصات التواصل الاجتماعي تفتقر لأي معايير، أو أدوات للتحقق من صحة المعلومات المنشورة، ومن ثم ان نشر المعلومات الكاذبة والتضليل على الإنترنيت يُعد من قبيل تجاوز حدود قواعد الأخلاق[2].

3- غياب الرقابة والمسؤولية[3]: أن السؤال الذي يثار في هذا الشأن أن معظم الشركات تعمل بلإستخدام بيانات شخصية مهمة مثل أرقام بطاقات الإئتمان ومعلومات خاصة ودقيقة عن الأفراد، فكيف تضمن الشركات الحفاظ على هذه المعلومات؟، إذ خلقت هذه المسألة الحاجة الماسة لوجود مسؤولية أخلاقية عن حفظ المعلومات الشخصية والخاصة بالأفراد من الضياع أو السرقة[4].

4- التطور والذكاء الصناعي: خلق تطور الذكاء الصناعي العديد من المشاكل الأخلاقية والتي تتطلب أن يتم وضع حدودٍ للتطور التقني واضحة ودقيقة فيها:

أ- إستبدال العاملين: أن تطور تقنيات الذكاء الصناعي يعني زيادة الاتمتة في مجال الأعمال، ومن ثم فستثار مسألة بل ربما أزمة حول مكانة العاملين بعد إستبدالهم من قبل الآلات؟

ب- تعقب الحالة الصحية للأفراد: منذ بداية جائحة كورونا، وقد أثيرت مسألة مهمة وهي، هل من الممكن أخلاقياً فحص صحة الناس والتأكد منها بشكل مستمر؟

---

(1)- Ashley Watters, 5 Ethical Issues in Technology to Watch for in 2021, CompTIA, 2021, the link: (https://connect.comptia.org/blog/ethical-issues-in-technology)), Accessed at (03-07-2022).

(2)- Cyber threats to family offices How a resilient approach in the family office can thwart today's cyber threats, Deloitte private, page 5.

(3) - نسرين عبدالحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف، الاسكندرية، 2008، ص246 .

(4)- Barbara A. Hudson, Penal Policy and Social Justice, THE Macmillan Press LTD 1993, USA, page 14.

ت- إن تقنيات الذكاء الصناعي يتم تطويرها من قبل بشر لهم تحيزات أخلاقية وتفضيلات، مما يعني إنتقال هذه التحيزات لهم، بهذا ستثار مشكلة مهمة وهي هل من الواجب أخلاقياً إبعاد التحيزات التي لدى البشر من الآلات[1].

5- التنظيم القانوني للتقنيات: أن تطورات التقنيات مثل الروبوتات، والسيارات الكهربائية وإستخدام الروبوتات بالقتال لم يعد خيالاً، بل أصبح واقعاً. وان الشركات الكبرى والحكومات بدأت تستثمر هذه الآليات بشكل مستمر مما يخلق مشاكل أخلاقية كبرى، هل بالإمكان استخدامها في المجال العسكري؟ ما تأثيراتها على الأناس العزل في الحروب والعمليات العسكرية؟ هل توجد حدود أخلاقية حول متى يجوز أو لا يجوز استعمالها؟ ما هي أثارها على البيئة، أي هل لها تأثيرات خطرة على البيئة؟ أم لا، وإذا كان لها خطرً على البيئة، هل يمكن وضع حدود لإستخدامها أم لا؟ كل هذه الأسئلة تثير مشاكل أخلاقية عدة وتبين وجوب ترسيم حدود حول الإستخدام التقنيات هذه في المجالات العسكرية[2].

الفرع الثالث

أثر التطور التكنولوجي في السياسة الجنائية

من أساسيات السياسة الجنائية هو الاهتمام بالحماية الخاصة للأفراد من خلال الضمانة الدستورية والقانونية، في مختلف تشريعات الدول المتقدمة، وذلك لكون هذه الحماية هي المصلحة المعنية الأجدر بالحماية لما تمثله لضمانة كرامة وحرية الشخص في العيش بحياة كريمة. والحق في الخصوصية هو أحد الحقوق اللصيقة التي تثبت للإنسان، والتي غالباً ما يصعب حصر الجوانب المختلفة لها، والتميز بين ما يعد من الحياة الخاصة، وما يعد من الحياة العامة[3].

والحقيقة أن الحياة في الوقت الحالي في ظل التطور التكنولوجي، تتمثل في مجموعة من المعلومات الخاصة، والتي تمثل كرامة وحرية الشخص من خلال التعامل مع الحياة والمجتمع الدولي والمحلي من خلال ظهور العديد من الأجهزة الحديثة وشبكات الإنترنت وبرامج التواصل الاجتماعي، وهناك من يحاول أن يعبث بهذه الحياة الخاصة من خلال إرتكاب جرائم الإنترنت والتعدي على المعلومات الخاصة والابتزاز، والتهديد، وسرقة الأموال وغيرها العديد من الجرائم التي ترتكب بواسطة أحدث الاجهزة والتقنيات عن بعد وبسهولة وسرعة[4].

---

(1)- Ashley Watters, Ibid.

(2)- Ashley Watters, Ibid.

(3) - د. احمد فتحي سرور، القانون الجنائي الدستوري، الطبعة الثانية، دار الشروق، 2002 ، ص 7.

(4) - د. عبدالفتاح بيومي حجازي، المصدر السابق ، ص 117 .

فالسياسة الجنائية يمكن وصفها على أنها تمثل الخطوط العامة التي تحدد إتجاه المشرع والسلطات التي تقوم على تطبيق القانون وتنفيذه بشكل يحقق الأمن الإجتماعي، فهي من تحدد ما يجب ان يكون عليه التشريع، وذلك فيما يتعلق بعنصر الإلزام في القاعدة العقابية المتمثل في الجزاء الجنائي الملائم لكل فعل مجرم ، كما أنها تحدد ما يجب أن يتخذ من تدابير تحول دون وقوع الجريمة، ويمكن تقسيم السياسة الجنائية إلى ثلاثة أنواع، وهي أما ان تكون سياسة جنائية، أو قضائية، أو تنفيذية، فالسياسة الجنائية هي التي تحدد الافعال غير مباحة والجزاء الجنائي يقابل كل من إرتكب فعلا يمس المصلحة المحمية وفقا لهذه السياسية التشريعية، أما السياسة القضائية هي التي تحدد إجراءات الخصومة والتحقيق اثناء المحاكمة، إستنادا إلى قانون الاجراءات الجزائية، وأخيراً السياسة التنفيذية، والتي بدورها تحدد سلطة الإدارة العقابية المكلفة بتنفيذ الجزاءات الجنائية والتدابير العامة، وتحديد القواعد العامة التي تتضمن التنفيذ سواء بأنواع السجون أو الاجراءات التي تتخذ بداخلها، وهو ما يسمى سياسة المنشأة العقابية وغيرها.

فالسياسة الجنائية بمفهومها الحديث، هي رسم وتكوين القواعد القانونية، بناء على معطيات علم الإجرام الذي يواكب التطور الذي يعيشه كل مجتمع وفق ظرف وزمان معين، فهي دليل المشرع إلى ما يجب أن تكون عليه نصوص التجريم والعقاب، وكيفية تنفيذ الجزاء الجنائي [1].

وعلى أساس ذلك يمكن القول إلى أن أساس التجريم في السياسة الجنائية هو (المصلحة المعتبرة)، أو المحل القانوني الأجدر بالحماية، والذي قد يتمثل، بالأخلاق والآداب العامة، وحماية الإقتصاد العام للدولة، والامن العام للدولة، والعلاقات الدولية بصورة عامة الخ. وجميع هذه التفاصيل التي ذكرناها هي التي تستهدفها السياسة الجنائية في ظل التطور التكنولوجي، وما ينتج عن هذه التكنولوجيا الحديثة[2]، أي بمعنى أن السياسة الجنائية تتأثر وتواكب التطور التكنولوجي وما ينتج عنه من جرائم لكون قانون العقوبات لا يستطيع احتواء جميع الجرائم، لأن المجتمع بدأ يتعامل مع التطور التكنولوجي بكل تفاصيل الحياة، ومن خلال هذه التكنولوجيا بدأت الجرائم بالتطور وأغلب الجرائم التي ترتكب بواسطة التكنولوجيا الحديثة وشبكات الإنترنت، هناك نقص تشريعي لم يستطع أحتوائها أو توقعها، وذلك بسبب أن التكنولوجيا الحديثة وما ينتج عنها من تطور سريع ، يستوجب على المشرع الجنائي أن

---

(1) - احمد فاروق زاهر، مبادئ علمي الاجرام والعقاب، الطبعة الاولى، جامعة الشارقة، 2013 ، ص 183 . وكذلك: عبدالكريم نصار، اساسيات علم الاجرام والعقاب، منشورات جامعة جيهان، اربيل، 2011، ص 44.

(2) - عبدالفتاح مصطفى الصيفي، المطابقة في مجال التجريم (محاولة فقهية لوضع نظرية عامة للمطابقة) بحث منشور، مجلة كلية الحقوق للبحوث القانونية والاقتصادية، جامعة الاسكندرية، كلية الحقوق، المجلد 13، العدد الخاص، 2018 ص 143 .

يواكب هذا التطور، والا أصبحنا أمام عجز تشريعي يسبب خللاً أمنياً في الإستقرار الإجتماعي والأقتصادي والسياسي والدولي.

ومن هذا المنطلق نجد أن للتطور التكنولوجي أثراً واضحاً وكبيراً في تطور السياسة الجنائية، وهذا ما نلاحظه من وجود عدة إتفاقيات ومعاهدات دولية وإقليمية من أجل التعاون وبذل الجهود، لمكافحة الجرائم الناشئة عن التطور التكنولوجي.

وبعد أن شهدنا تطور أشكال الجريمة بوجود التطور التكنولوجي والتقني، ومع استخدام جهاز الحاسب الآلي والإنترنت، وإستهداف هذه الجرائم لكافة المصالح والحقوق، وأصبحت الجرائم الإلكترونية تقع على الأشخاص والأموال والمعلومات، سواء القتل أو التحريض على الانتحار، والتسبب في الأضرار والمضايقات غير الأخلاقية، وإنتهاك سرية البيانات الشخصية، وتحريض القاصرين على الأنشطة الجنسية غير المشروعة، بالإضافة إلى جرائم التحرش الجنسي والابتزاز والتنمر ونشر الإرهاب والعديد من الجرائم التي ترتكب بواسطة الوسائل الإلكترونية، كان لا بد من تفعيل المواجهة التشريعية الجنائية لمواكبة ومكافحة مثل هذه الجرائم، لأن التشريع الجنائي يمثل الإطار الوقائي والردعي الذي يحيط بالجريمة من جميع نواحيها، فالتشريع الجنائي يمثل سياسة وإيدلوجية النظام القابض على السلطة ، فلا يمكن أن يستمر أي نظام من دون نظام تشريعي جنائي، وهذا يعني لا يمكن ترك الفراغ التشريعي أو النقص التشريعي في ظل التطور التكنولوجي الذي تعيشه أغلب المجتمعات في العالم[1].

وتأسيسا على ذلك نجد أن السياسة الجنائية، تختلف في مجال مكافحة الجريمة الإلكترونية فيما بين الدول، ويرجع هذا لأختلاف الأنظمة والقوانين وطبيعة العادات والتقاليد في المجتمعات، وقد أخذت الدول أحد الإتجاهين في رسم السياسة التشريعية الجنائية لمكافحة الجرائم الالكترونية[2] .

الاتجاه الاول: سياسة تطبيق نصوص القوانين التقليدية على الجرائم الالكترونية، يرى هذه الاتجاه إلى انه بسبب التعقيدات والاشكالية التي احدثتها الثورة التكنولوجية وما نتج عنها من جرائم الكترونية، جعل مهمة القضاء صعبة في مواجهة مثل هذه الجرائم المعقدة، والتي بدأت خطورتها تفتك بالأمن والمصالح العامة، بسبب عدم وجود نصوص جنائية تشريعية كفيلة لمكافحة هذه الجرائم، وعلى ضوء ذلك فأن مؤيدي هذا الإتجاه يرون أن محاولة تطبيق النصوص الجنائية التقليدية على الجرائم الالكترونية يمثل أحد الحلول في مجال السياسة الجنائية، ويستندون في ذلك أنه في ظل عدم تدخل المشرع الجنائي بإصدار تشريعات جنائية خاصة لمواجهة هذه الجرائم أو حتى مراجعة نصوصها

(1) - يونس عرب، جرائم الكمبيوتر والانترنت، بحث مقدم إلى مؤتمر الامن العربي، المركز العربي للدراسات والبحوث الجنائية، ابو ظبي، 2002، ص 159.

(2) - سعود علي عبدالله اللوغاني، السياسة الجنائية في مكافحة الجريمة الالكترونية، المصدر السابق، ص139.

العقابية الحالية ومدى توافقها مع هذه الأنماط المستحدثة من الجرائم حتى تكون كفيلة لمواجهتها، فانه في تلك الحالة لا مناص من تطبيق القضاء للنصوص العقابية التقليدية، لكي لا يقال أن هذه الأفعال مباحة وغير مجرمة ولا يرتب المشرع عليها أي عقاب، ويذهب اصحاب هذا الإتجاه إلى عدّ الجرائم الالكترونية بمثابة جرائم تقليدية لا تختلف عن غيرها، وإنما الذي يختلف فيها هو الوسيلة التي نفذت بها الجرائم الالكترونية وهي الاجهزة التقنية الحديثة[1].

اما اصحاب الاتجاه الثاني: سياسة تشريع قوانين خاصة لمكافحة الجرائم الإلكترونية، بسبب الإنتشار الكبير لإستخدام الاجهزة التقنية الحديثة والإنترنت، في أغلب تفاصيل تعاملات الحياة، فقد يرى أصحاب هذا الإتجاه إلى ضرورة الحاجة لإستحداث تشريعات جديدة لمكافحة الجريمة الإلكترونية، وذلك بسبب تزايد أصحاب النفوس الضعيفة والنفعية ليستغلوا هذا التقنيات الحديثة والإنترنت لأغراض غير مشروعة، واصبح هذا النظام ومعلوماته محلا للعديد من الإعتداءات التي تهدد وتعرض المصالح المحمية للخطر، ونجد أن مثل هذه الجرائم قد إنتشرت بصورة سريعة وتزايدت بشكل واسع بعد ظهور شبكة الإنترنت، مما أوجب على المشرع الجنائي ، بالإسراع لتشريع قوانين جديدة لتواكب هذا التطور التكنولوجي ولسد النقص التشريعي، خشية إفلات المجرمين من المساءلة الجزائية والعقاب، وأيضا ما يسبب تعرض المصالح والأمن المجتمعي والدولي بفقدان الثقة بالتعامل بهذه التكنولوجية والتي لها العديد من الإيجابيات وتسهيل التعاملات الأقتصادية والسياسية والدولية، مما يسبب خسائر كبيرة قد تؤثر على الإستقرار المحلي والدولي، وذلك بسبب عجز القوانين التقليدية في مكافحة الجرائم الإلكترونية وهذا ما لاحظناه في أغلب الدول المتأخرة والنامية، والتي لم تشرع لغاية اليوم قوانين خاصة لمواجهة مثل هذه الجرائم[2]. وقد أوصت العديد من الإتفاقيات والمؤتمرات الدولية في ديباجتها على الدول الأعضاء الإسراع وتشريع قوانين لمواجهة الجرائم الإلكترونية، وقد صادق العراق على مثل هذه الاتفاقيات [3].

ونجد أن الأثر المباشر للتطور التكنولوجي في السياسة الجنائية قد إنعكس من خلال اتساع نطاق التجريم والعقاب مع تطور المجتمع وزيادة التوسع العمراني والتقني ، مما أدى بالمشرع بتجريم صور وسلوك تعبر عن مراحل التطور التكنولوجي الحديث الذي يعيشه المجتمع، فالانتقال من مجتمع بدائي يعتمد على الزراعة، إلى مجتمع متمدن يعتمد على الصناعة والتكنولوجيا الحديثة، جعل من الضرورة

(1) - شمسان ناجي صالح الخيلي، الجرائم المستخدمة بطرق غير مشروعة لشبكة الانترنت، دار النهضة العربية، القاهرة، 2009، ص 48.

(2) - سعود علي عبدالله اللوغاني، السياسة الجنائية في مكافحة الجريمة الالكترونية، المصدر السابق، ص 162 وما بعدها.

(3) - ينظر: قانون تصديق الاتفاقية العربية العراقي لمكافحة جرائم تقنية المعلومات رقم (31) لسنة 2013 .

الحتمية، ظهور جرائم جديدة كالجرائم الإلكترونية وغيرها، مما جعل المشرع الجنائي يستجيب إلى التطور الذي يعيشه العالم، وظهور التكنولوجيا وتشعب دورها في أغلب تعاملات الحياة، لذا كان من الطبيعي تشريع قوانين جديدة تجرم الافعال الماسة بأمن الدولة والمجتمع، سواء على الصعيد الخارجي أو الداخلي، فعلى الصعيد الخارجي فقد صدرت بعض المبادئ الإرشادية والتوجيهية في مجال تجريم الأفعال التي تنتهك الخصوصية والحماية المقررة لها، ومن هذه المبادئ والتوصيات ما تضمنه القرار الصادر عن مؤتمر الأمم المتحدة (الثامن) لمنع الجريمة ومعاملة السجناء، بالإضافة إلى صدور قرار بشأن الجرائم ذات الصلة بأجهزة الحاسب الالي، وأكد القرار على ضرورة مكافحة جرائم الكمبيوتر، وكذلك ما تضمنته مقررات وتوصيات المؤتمر (الخامس عشر) للجمعية الدولية لقانون العقوبات عام (1994) المنعقد في البرازيل بشأن جرائم الكمبيوتر والذي نادى بضرورة تبني المؤتمر تجريم بعض الأفعال المرتبطة بإستخدام الكمبيوتر[1].

المطلب الثاني

دور السياسة الجنائية في مواجهة جرائم التكنولوجيا

أن الحديث عن الضوابط القانونية والأخلاقية للتطور التكنولوجي له قيمة قانونية، تتمثل في مدى إستعمال المجتمع لهذا التطور التكنولوجي ومدى تأثير السياسة الجنائية في وضع قيود لحرية الفرد الشخصية في التعامل مع هذا التطور، وكذلك مدى تأثر السياسة الجنائية بهذه التكنولوجيا الحديثة، وذلك لظهور جرائم تنشأ عن الإستعمال السلبي لهذه التكنولوجيا.

الفرع الأول

مواجهة الجريمة المنظمة العابرة للحدود الوطنية

لكي يكون هناك استقرار أمني ودولي على الصعيد العالمي، فإن هذا الأمر يحتاج إلى قدر من التعاون الدولي، لمواجهة الجريمة كإحدى القضايا الرئيسة التي تؤثر سلباً بشكل كبير على الامن والسلم الدوليين، إذ إن مكافحة هذه الجرائم المنظمة والعابرة للحدود وجرائم الإنترنت، أصبحت تشغل أهتمام الباحثين والمختصين في الشأن الدولي على حد سواء، وهذا ما ثبت إلى أن أي دولة - لا تستطيع بجهودها المفردة القضاء على الجريمة المنظمة، مع هذا التطور التكنولوجي السريع والمذهل الذي

(1) - سعود علي عبدالله اللوغاني، السياسة الجنائية في مكافحة الجريمة الالكترونية، المصدر السابق ، ص 168 وما بعدها .

يعيشه العالم، وظهور أنواع عديده من الجرائم غير التقليدية ، والتي ترتكب بكل سهولة، ولا تتقيد بحدود ووقت، وأصبح هذا الامر يشكل خطراً كبيراً على الأمن والسلم الدوليين دون إستثناء، وهذا الأمر يتطلب تعاون دولي لمكافحة هذه الجرائم العابرة للحدود[1].

وفي ظل التطور الذي يعيشه العالم بأسره، نلاحظ أن المجتمع الدولي أخذ على عاتقة ببذل الجهود من خلال عقد مجموعة من الإتفاقيات والمؤتمرات الدولية والإقليمية، بغية مواجهة الجريمة المنظمة والجرائم الإلكترونية، وذلك لكون القوانين التقليدية لا تكفي لمواجهة الجريمة المنظمة العابرة للحدود وجرائم الانترنت، في ظل هذا التطور التكنولوجي والمتسارع بشكل لا يمكن توقع ما سيؤول الية هذا التطور من أبعاد تقنية في المستقبل القريب، وقد رافق هذا التطور مجموعة من الجرائم، وهذا ما يسبب مشكلة أمنية ومشاكل اجتماعية واقتصادية وسياسية، ونتيجة لذلك أهتم المجتمع الدولي، من دول وحكومات ومنظمات دولية واقليمية، لهذه الظاهرة التي تواكب التطور التكنولوجي، وبروز العديد من الجرائم، والنظر في سبل معالجتها ووضع الحلول الناجعة لمكافحتها [2].

إذ جاء في ميثاق الامم المتحدة الصادر عام (2002) تعريف الجريمة المنظمة العابرة للحدود هي " مجموعة من الافعال أو العمليات الإجرامية التي تقوم بها جماعة تتألف من ثلاثة أشخاص فأكثر، تكون منظمة ومرتكبة خلال حيز زمني متصل وطويل من أجل جني منافع مالية أو مادية بشكل مباشر أو غير مباشر". وعرفها بعضهم بانها " الجرائم التي ترتكب من منظمة إجرامية وتتشكل هذه المنظمة من ثلاثة أفراد على الاقل يسود على هذه المنظمة طابع الإستمرارية، وتقوم غالباً بإرتكاب هذه الجريمة وغالبا ما ترتكب هذه الجريمة في اكثر من دولة"[3].

اولا : دور المنظمات الدولية

1- منظمة الامم المتحدة

بذلت الأمم المتحدة جهوداً كبيرة ودوراً فعالاً في مجال مكافحة الجريمة المنظمة وقد نظمت في عام (1975) مؤتمرها الخامس والذي تضمن طرق وإساليب لمكافحة الجريمة المنظمة، وكذلك تشكل في عام (1995) المؤتمر الدولي الذي عقد في دولة مصر العربية، الخاص بالحد من إنتشار الجريمة، للحد من جرائم الإتجار بالنساء وخطف الاطفال والاتجار بالأسلحة وغيرها من الجرائم العابرة

(1) - د. حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، دار النهضة العربية، القاهرة، 2009، ص 636 .

(2) - نسرين عبدالحميد نبيه، المصدر السابق ، ص 211.

(3) - جغدم محمد الامين، جرائم الارهاب الالكتروني والجرائم المنظمة ، بحث منشور ، مجلة كلية الحقوق ، جامعة عبدالحميد ابن باديس، الجزائر، ص 139 .

للحدود. بالإضافة إلى المؤتمر الدولي الذي عقد عام (2000) برعاية الأمم المتحدة [1]، إذ شارك فيه ما يقارب (124) دولة ، لتوقيع ما تضمنته المعاهدة الدولية من تجريم بعض الأفعال من جرائم غسل الأموال وعرقلة عمل العدالة وكذلك تضمنت الاتفاقية آلية لمصادرة عائدات الجريمة المنظمة، من ممتلكات ومعدات تدخل في الجريمة المنظمة[2].

وقد توصلت منظمة الأمم المتحدة في مؤتمرها الثامن حول منع الجريمة ومعاملة المجرمين، إلى إصدار قرار خاص بالجرائم المتعلقة بالتكنولوجيا والإنترنت، وإشار القرار إلى أن الاجراء الدولي لمواجهة جرائم الإنترنت يتطلب من الدول الاعضاء التعاون وإتخاذ مجموعة من الإجراءات وهي [3]:

أ- تحديث القوانين الجنائية بما في ذلك التدابير المتخذة من أجل ضمان تطبيق القوانين الجنائية الراهنة.

ب- إتخاذ تدابير أمنية تعتمد على إستراتيجية متطورة، مع مراعاة خصوصية الأفراد واحترام حقوق الانسان.

ت- مصادرة كل ما يدخل في اعداد وصنع في الجريمة والانشطة غير المشروعة.

ث- التعاون مع المنظمات الدولية والإقليمية في مجال مكافحة جرائم الإنترنت والجرائم المنظمة، ووضع منهج للتدريس منهج الآداب والأخلاق في مجال إستخدام الحاسوب والانترنت [4].

ج- نشر الوعي لدى الشعوب والقضاء والأجهزة العاملة على مكافحة هذا النوع من الجرائم والتثقيف على أهمية محاكمة مرتكبيها.

وتزايد أهتمام منظمة الأمم المتحدة في مجال مكافحة الجريمة، وقد دعت إلى عقد إتفاقية لمكافحة الجريمة المنظمة العابرة للحدود، في فيينا في اكتوبر عام (2010) إذ تضمن فهرست الاتفاقية مجموعة من القرارات تتعلق بتسليم المجرمين وتبادل المساعدة القانونية وبعض الامور التي تدعوا إلى التعاون الدولي[5].

2- الشرطة الجنائية الدولية (الإنتربول)

كانت البدايات الاولية للتعاون الدولي بدأت عام 1904 م عندما تم ابرام الاتفاقية الدولية الخاصة بمكافحة الرقيق الابيض بتاريخ (1904/5/18) والتي جاء بنص المادة (الاولى) منها على أن "تتعهد

---

(1) - علي عدنان الفيل، الاجرام الالكتروني، دراسة مقارنة، ط1، منشورات زين الحقوقية، 2011، ص 330.

(2) - لخضر رابحي، ابراهيم سويسي ، مجابهة جريمة التحريض الالكتروني في ضوء مبدأ مسؤولية الحماية، بحث منشور، مجلة الدراسات القانونية والسياسية، المجلد 6، العدد 2، 2020، ص 57.

(3) - د. محمد ممدوح بدير، مكافحة الجريمة المعلوماتية عبر شبكات الانترنت، ط1، مركز الدراسات العربية، مصر ، 2019 ، ص 135 وما بعدها .

(4) - د. أسامه بن غانم العبيدي، الجهود الدولية في مكافحة الجرائم المعلوماتية، بحث منشور ، مجلة الحقوق، العدد 4، السنة 39، 2015، ص 138.

(5) - د. محمد ممدوح بدير، المصدر السابق، ص 138 .

كل الحكومات المتعاقدة بإنشاء أو تعين سلطة لجمع المعلومات الخاصة باستخدام النساء والفتيات لغرض الدعارة في الخارج ...."[1]، وجاء بعد هذه الاتفاقية تأسيس منظمة الشرطة الجنائية الدولية عام (1923)، ومركزها مدينة (ليون) في فرنسا، وتوجد لهذه المنظمة عدة فروع ومكاتب في دول عديدة ما يقارب (177) دولة من دول الاعضاء، وقد أسهمت هذه المنظمة (الانتربول) في مكافحة الجريمة المنظمة [2]، وكان لها دور كبير في تزويد الدول الاعضاء بمعلومات مهمة عن المجرمين المطلوبين للعدالة وتبادل المعلومات. وقد تطور دور (الإنتربول) في عام 1993 عندما أنشات قسماً خاصاً بتحليل المعلومات الجنائية والتي كانت ترتبط بالأمانة العامة للمنظمة، ومهمتها تحليل واستخلاص المعلومات عن بعض المنظمات الاجرامية عن طريق التتبع الالكتروني والاتصالات بواسطة أجهزة متطورة من خلال نقل المعلومات المهمة بين الدول[3].

ومن الامثلة على دور (الإنتربول) فيما يتعلق بالجرائم المنظمة، وهو ما حصل في دولة الامارات العربية، المتحدة عندما قام أحد الاشخاص بنشر صورة ذات طبيعة جنسية لاحد الاطفال القصر من خلال موقعة على شبكة الانترنت، وعلى أثر ذلك تم توقيف المتهم من قبل النيابة العامة في دبي بتهمة نشر صور ذات طبيعة جنسية وانتهاك للخصوصية، وكان توقيف المتهم من قبل النيابة العامة في الإمارات العربية المتحدة إستنادا لتلقيهم برقية من الإنتربول الدولية في بريطانيا بهذا الخصوص[4].

ثانيا : دور المنظمات الاقليمية

لقد أسهمت المنظمات الاقليمية في مجال مكافحة والحد من الجريمة المنظمة العابرة للحدود، وذلك من خلال تضافر الجهود الدولية وانعقاد العديد من المؤتمرات الدولية على المستوى الإقليمي والمحلي، وعلى النحو الأتي :

1- المجلس الاوربي

يسعى الإتحاد الاوروبي إلى بذل جهود كبيرة وعلى مدى سنوات إلى وضع حلول ناجعة للحد من إنتشار الجريمة المنظمة، والجرائم التي تنشأ عن التطور التكنولوجي، وقد توجت هذه الجهود بصدور (اتفاقية بودابست)، والتي خصصت لمكافحة الجرائم المنظمة وجرائم الإنترنت، وسميت هذه الإتفاقية بالإتفاقية الأوربية لمكافحة جرائم المعلوماتية[5].

---

(1) - د. حسين بن سعيد الغافري، المصدر السابق، ص 637 .
(2) - د. أسامه بن غانم العبيدي، الجهود الدولية في مكافحة الجرائم المعلوماتية، المصدر السابق، ص 123.
(3) - د. حسين بن سعيد الغافري، المصدر السابق ، ص 640.
(4) - د. أسامه بن غانم العبيدي، الجهود الدولية في مكافحة الجرائم المعلوماتية، المصدر السابق، ص 124.
(5) - ينظر: هلالي عبد اللاه أحمد، جرائم المعلوماتية عابرة الحدود، دار النهضة العربية، القاهرة، 2007، ص63.

وتتمثل مبادئ وأهداف هذه الإتفاقية في السعي لتحقيق وحدة التدابير التشريعية بين الدول الأوروبية والدول المنضمة للاتفاقية، من غير الدول الاوربية وكان التأكيد على أهمية التعاون الدولي والاقليمي في مجال مكافحة الجرائم المنظمة والمعلوماتية عبر شبكات الإنترنت، وأكدت الإتفاقية على تحقيق التوازن بين الحرية الخاصة والتي يكفلها الدستور، في مجال إستخدام الإنترنت، وبين التجريم والعقاب عند تشريع القوانين بغية مكافحة الجريمة المنظمة والجرائم الإلكترونية، وقد جاء في مضمون الإتفاقية بيان تعريف وتحديد العقوبات التي توقع على من يرتكب الجرائم المعلوماتية، وتكون هذه العقوبات في إطار القوانين المحلية. وقد نضم هذه الإتفاقية كل من مجلس الاتحاد الأوروبي بالتعاون مع كندا واليابان وجنوب افريقيا والولايات المتحدة الامريكية، وتم التوقيع عليها في عام (2001) ودخلت حيز التنفيذ في عام (2004) وبعدها انضم لهذه الإتفاقية عددً من الدول من مختلف الإقاليم. وقد بذل الاتحاد الاوروبي جهودا من اجل مكافحة الجريمة وكان اخرها في عام (2006) [1].

وقد أصدر مركز العدل الأوروبي ومركز الشرطة الأوروبية للجرائم الإلكترونية ورقة حدد فيها التحديات التي تواجه الدول في مواجهة الجرائم الإلكترونية عبر الحدود والتي بتخطيها يمكن مواجهة الجرائم الإلكترونية بشكل أفضل، وقد بنيت المعلومات التي تحصلها المركز على الخبرات العملية المشتركة، والنقاشات بين الدول، وكذلك تقارير للإجتماعات الأستراتيجية مع الخبراء الوطنين وحاملي الأسهم وتقارير إستراتيجية وتقييمات من الشرطة الأوروبية مثل تقرير خطر الجرائم المنظمة الأوروبية كذلك مصادر أخرى متنوعة. وحدد هذا التقرير المشاكل التالية التي تواجه الدول في مواجهة الجرائم الالكترونية وسنسعى للتركيز على مشكلة غياب التنسيق والتعاون الدولي من بين هذه المشاكل[2]، واما هذه المشاكل فهي:

(ا) فقدان البيانات.

(ب) فقدان المواقع.

(ت) مشاكل متعلقة بالإطار القانوني الوطني.

(ث) مشاكل متعلقة بغياب التنسيق الدولي.

(ج) مشاكل تتعلق بغياب الشراكات العامة والخاصة.

---

(1) - د. محمد ممدوح بدير، المصدر السابق، ص 144 .

(2)- Eurojust and Europol, Common challenges in combating cybercrime, OINT REPORT Europol and Eurojust Public Information, 2019, page 4 &5.

(ث) مشاكل متعلقة بغياب التعاون الدولي في مواجهة الجرائم الالكترونية المنظمة: أن العوائق التي تواجه التعاون الدولي هي[1]:

1- في السياق الدولي لا يوجد أي إطار قانوني لمشاركة الأدلة ولحفظها، تعني هذه الحالة بأن الأدلة لن تحفظ لمدة طويلة قبل أن تنقل لدولة التي تطلب هذا الدليل، وخاصة أن مشكلة حفظ الأدلة في الجرائم الإلكترونية المنظمة العابرة للحدود هي مشاكل ذات حساسية تتطلب دقة في توقيت نقل الأدلة. فالأختلاف في القوانين بين الدول يتطلب تنسيقاً قضائياً مع وضع جداول لنقل الأدلة في الجرائم الإلكترونية المنظمة العابرة للحدود، بغياب القواعد القانونية الكافية لمواجهة الجرائم الإلكترونية المنظمة يتطلب التنسيق بين الدول بالقواعد القانونية القائمة لمواجهتها بشكل أفضل. ومن ثم يجب ان توجد آلية عابرة للحدود للتواصل وتبادل المعلومات لأغراض التحقيق والرد والوقاية من الجرائم الالكترونية المنظمة، ومن المسائل الأخرى التي يتعين وجود التنسيق بها هي مسألة ضرورة حصول تعاون دولي بين السلطات المختصة بالتحقيق فيما يتعلق بالأدلة والمعلومات المتعلقة بالجرائم بشكل يسهل التحقيق الجرائم الالكترونية المنظمة العابرة للحدود- ويجب ان تضع الدول بالإعتبار إطاراً قانونياً مشتركاً للتحقيق فيما بينها فيما يخص الجرائم الإلكترونية المنظمة العابرة للحدود، ومن ثم يسهل إيجاد مرتكبي هذه الجرائم والقبض عليهم ومعاقبتهم[2].

2- ضعف التنسيق الدولي لمواجهة الهجمات الإلكترونية ذات نطاق واسع: أن الهجمات الإلكترونية المنظمة ذات النطاق الواسع تشكل تهديداً للتعاون الدولي، وأن نطاق ردود الدول وتنسيقها لمواجهة هذه الجرائم الإلكترونية ليس كافياً لمواجهة الهجمات الإلكترونية المنظمة ذات النطاق الواسع، فحصلت هجمة إلكترونية منظمة في العام (2017) والتي استهدفت العديد من الصناعات الأوروبية في وقت متقارب وفي العديد من الدول والقطاعات وكانت هذه الهجمات سريعة وفعالة، ان ضعف الأمن السيبراني والرقابة الرقمية ورافقها ترابط الشبكات الرقمية عبر الحدود وبسهولة وعلى نطاق واسع، وبترافق هذه العوامل معا سنحت الفرصة للمنظمات الإجرامية من إرتكاب جرائم إلكترونية ذات نطاق واسع ومنظم في آن واحد . أن هذا الهجوم قد بين مسألة مهمة وهي غياب التنسيق الجماعي لمواجهة الجرائم الإلكترونية المنظمة الكبرى مما يعني ضعف النظام الدفاعي الإلكتروني. إن هذه

(1)- Eurojust and Europol, Common challenges in combating cybercrime, Op,Cit, page6.
(2)- Rob van den Hoven van Genderen, Cybercrime investigation

and the protection of personal data and privacy, Economic Crime Division

Directorate General of Human Rights and Legal Affairs Strasbourg, France, 2008, page 24.

الهجمات لها عواقب سيئة على أرض الواقع ويمكنها أن تمتد للمناطق عديدة حول العالم مما يعني الحاجة لتنسيق دولي أفضل لمواجهة الجرائم الإلكترونية المنظمة ذات النطاق الواسع ووضع قواعد تحدد الإجراءات وتقييم المسؤولية على الأفراد أو المنظمات التي ترتكب هذه الجرائم[1].

2- منظمة التعاون والتنمية الاقتصادية

أمام قلة الإتفاقيات الدولية والإقليمية التي تهتم بتنظيم ومكافحة الجرائم المنظمة والجرائم الإلكترونية، وعدم كفاية الإتفاقيات القديمة ذات الصلة بهذه الجرائم، فقد أصبح المجتمع الدولي أمام نقص تشريعي دولي وإقليمي امام هذا التطور التكنولوجي وما ينتج عنه من جرائم، أصبحت القوانين لا تتسع لمكافحة هذه الجرائم المنظمة والسريعة، مما ادى بالمجتمع الدولي والإقليمي على تبني مجموعة من الإتفاقيات من اجل وضع الحلول المناسبة والناجعة لمكافحة الجرائم المنظمة وجرائم الإنترنت في سبيل توفير الحماية للأمن والسلم الدوليين وتوفير الحماية القانونية الكافية لمستخدمي شبكات الإنترنت، فقد أصدرت منظمة التعاون والتنمية الأقتصادية في عام (1980) مجموعة من التوجيهات والقرارات الإرشادية، لتنظيم حماية الحياة الخاصة والمعلومات ذات الطابع الشخصي، وأصدرت المنظمة تقريرا في عام (1983) بعنوان (الجرائم المرتبطة بالحاسوب وتحليل السياسة القانونية الجنائية)، وقد تضمن هذا التقرير مجموعة من المبادئ التي تحدد السياسة الجنائية والمقترحات الخاصة في عدد من الدول الاعضاء، ومن هذه المبادئ هو الحد الأدنى لأفعال سوء إستخدام الحاسوب والإنترنت، والتي يتوجب على الدول الاعضاء تجريم هذه الافعال وتحدد لها عقوبات ضمن القوانين الوطنية، وأوصت اللجنة المكلفة من قبل منظمة التعاون والتنمية الأقتصادية، مجموعة من الإرشادات والحماية المقررة لضحايا جرائم الإنترنت والإتجار في الأسرار والأختراق غير المأذون فيه للحاسب أو لأنظمته، ومن هذه الإرشادات هي [2]:

أ- تجريم التلاعب في البيانات المعالجة ألياً بما في ذلك محوها.

ب- التجسس المعلوماتي بكل اشكاله .

ت- التخريب المعلوماتي بما فيه من سرقة بعض البيانات أو الاستخدام غير المشروع.

ث- قرصنة البرامج.

ج- إعتراض إستخدام المعطيات أو نقلها.

وكذلك اهتم فريق من الخبراء في إعداد مجموعة من المبادئ التي تحل مشكلة تنازع القوانين والأختصاص القضائي، ومن هذه المبادئ عمل هذه المنظمة هو " يجب على الدول الأعضاء أن

---

(1)- Eurojust and Europol, Op,Cit , page 8.

(2) - د. محمد ممدوح بدير، المصدر السابق، ص 140.

تجتهد في وضع مبادئ واجبة التطبيق على المستويين الوطني والدولي بغية تحديد القانون الواجب التطبيق بشان الحفاظ على البيانات ذات الطابع الشخصي عبر الحدود"، وقد تبنت بعض الدول والحكومات في هذه المنظمة في عام (1985) بياناً خاصاً بتدفق المعلومات عبر الحدود، وتزايد الأهتمام بحماية المعلومات الخاصة في مجال التعامل الإلكتروني. وقد وصل الأمر إلى ايجاد نوع من التوازن العادل بين حرية إنتقال المعلومات وبين الحماية المقررة للحياة الخاصة وتم الاتفاق على هذا الإرشادات في عام 1998 تحت مسمى (عالم بلا حدود)، ومكان إنعقاد هذا المؤتمر في اوتاوا [1].

3- جامعة الدول العربية

تزايد أهتمام الجامعة العربية في مجال مكافحة الجرائم الالكترونية والجرائم المنظمة العابرة للحدود، وذلك من خلال الامانة العامة لمجلس وزراء الداخلية العرب، بعد أن تم مناقشة موضوع الحد من إنتشار هذه الجرائم، وكان ذلك بحضور فريق متخصص بدراسة هذه الجرائم، وكان ذلك في عام (2000) وبالتحديد في دولة تونس، وقد حصل اجتماعان في تونس في العام نفسه، وقد صدرت نتيجة هذه الاجتماعات مجموعة من القرارات والتوصيات، تمثل نموذجا موحدا لتكوين جهاز متخصص في مكافحة الجرائم التي ترتكب عن طريق الإنترنت والجرائم المنظمة العابرة للحدود، فضلا عن إعداد دراسة حول الإجراءات والتدابير التي تساعد على منع والحد من الجرائم المرتكبة بواسطة الأجهزة الحديثة والمتطورة والتي تكون متخصصة في مجال الإنترنت والتكنولوجيا الحديثة [2]. وبعد ذلك نتج عن هذه الاجتماعات المكثفة توصية بوضع مشروع اتفاقية عربية لمكافحة جرائم الحاسوب والجريمة المنظمة، على غرار الاتفاقية الصادرة عن المجلس الاوروبي عام (2001)، وهذا ما حصل فعلا في بتاريخ 0 21-2003/5/22) عندما تم الاتفاق على مجموعة من التوصيات والقرارات يمكن اعتبارها كقانون إسترشادي لمكافحة الجرائم المعلوماتية والجرائم المنظمة العابرة للحدود، وقد تم اعتماد هذا القانون بتاريخ (2003/10/9) من قبل مجلس وزراء العدل العرب، ومجلس وزراء الداخلية العرب، في دورته الحادية والعشرين في تونس بتاريخ (2004/1/5)، وكما تم الإتفاق في الإجتماع الثاني عشر للجنة المتخصصة بالجرائم المستجدة عام (2004) لموضوع التزوير في مجال بطاقات الإئتمان، وإعتمدت الأمانة العامة مشروع أتفاقية عربية حول جرائم الحاسوب تنفيذا للتوصية الصادرة

(1) - أمير فرج يوسف، الجرائم التجارية الالكترونية وأساليب مكافحتها، ط1، مكتبة الوفاء القانونية، 2013 ، ص215 .

(2) - أمين أعزان ، الحماية الجنائية للتجارة الإلكترونية، (دراسة مقارنة) أطروحة دكتوراه، جامعة عين شمس، كلية الحقوق، 2018 ، ص117.

عن الاجتماع الحادي عشر للجنة المتخصصة بالجرائم المستجدة، ولكن لحد الان لم يتم التصويت على هذا المشروع وهو في إطار الاعداد[1].

الفرع الثاني

تطور الجهود الجنائية الدولية والإقليمية في مواجهة الجرائم الإلكترونية

نلاحظ أن العالم والمجتمع الدولي باسره أخذ يتعامل مع التطور التكنولوجي بكل مجالات الحياة، ونتيجة لهذا التطور والتكنولوجية الحديثة، فقد اصبح العالم يتعامل بعالم أفتراضي، وهذا الأخير الغى جميع الحدود والمسافات، وأختصر الوقت في التعامل على النطاق الأقتصادي والإجتماعي والسياسي، وتعد هذه من إيجابيات التطور التكنولوجي والتقني، ولكن في نفس الوقت ظهر جانب سلبي لهذا التطور التكنولوجي من خلال إرتكاب جرائم معقدة وخطرة على المستوى الدولي والمحلي واصبحت هذه الجرائم تشكل خطراً كبيراً على الحق في الحياة والشرف والإعتبار وغيرها الكثير من جرائم سرقة الاموال والتزوير والنصب والإحتيال، وهذا ما يشكل تحدياً كبيراً لكثير من الدول والمنظمات العالمية والإقليمية، إذ هناك جهود دولية واضحة للحد من هذه الجرائم، من خلال انعقاد العديد من المؤتمرات الدولية والإقليمية للوصول إلى نتائج ناجعة كفيلة لمكافحة جرائم الإنترنت، وتحديد القانون الواجب التطبيق ومبدأ إقليمية القانون، وعدم التعدي على سيادة الدول، من خلال القيام بإجراءات التفتيش عن الجريمة الإلكترونية وإجراءات التحقيق وسماع الشهود ومتابعة المجرمين وتقديمهم للمحاكم المختصة ومعاقبتهم[2].

وإذ أخذت بعض الدول على عاتقها بمبادرة سن قوانين خاصة لمكافحة الجرائم الإلكترونية، وهذه القوانين منفصلة عن القوانين التقليدية، وتعد (السويد) الدولة الأولى التي سنت تشريعات خاصة بجرائم التطور التكنولوجي والانترنت، إذ صدر قانون البيانات السويدي عام (1973)، وتبعتها الولايات المتحدة الامريكية فأصدرت قانونها الخاص بحماية انظمة الحاسب الالي عام (1976 – 1975) وبعدها أصدر (معهد العدالة القومي) خمسة أنواع رئيسة للجرائم الإلكترونية وهي : جرائم الحاسب الآلي الداخلية، جرائم الإستخدام غير المشروع عن بعد، جرائم التلاعب بالحاسب الآلي، دعم التعاملات الاجرامية، وسرقة البرامج الجاهزة والمكونات المادية للحاسب. ونجد أن بريطانيا قد سارت على نهج كل من السويد والولايات المتحدة الأمريكية، وشرعت قانوناً خاصاً بالجرائم الالكترونية عام

(1) - د. رامي متولي القاضي، د. عمر سالم، مكافحة جرائم تقنية المعلومات رقم (175) لسنة 2018، ط1، مركز الدراسات العربية، 2020 ، ص 29 .

(2) - محمد كمال محمود السوقي، المصدر السابق ، ص 126 .

(1981)[1]. وعلى ضوء ذلك سنحاول التكلم عن دور بعض المنظمات الدولية والاقليمية في مجال مواجهة الجريمة الالكترونية.

أولا: دور منظمة الامم المتحدة في مكافحة الارهاب الالكتروني

لقد إعتمدت الدول الاعضاء هذه الاستراتيجية بتاريخ (8 سبتمبر عام 2009) والتي كانت تتضمن مجموعة من القرارات وخطة عمل من شانها تحسين التعاون الدولي في مجال مكافحة الجريمة والإرهاب الإلكتروني، وقد تضمنت المادة (الثانية /الفقرة الثانية) من نص البيان إلى انه " الاستفادة من الإطار الذي تتيحه المنظمات الدولية والاقليمية ودون الإقليمية المعنية لتبادل أفضل الممارسات في مجال بناء القدرة على مكافحة الإرهاب، وتيسير اسهامها في الجهود التي يبذلها المجتمع الدولي في هذا المجال" [2].

ثانيا : المؤتمر الدولي لتجريم الإرهاب الالكتروني (ابو ظبي)

في اليوم الخامس عشر والسادس عشر من شهر ماي 2017 ، انعقد المؤتمر الدولي في ولاية أبو ظبي الامارتية، والذي كان على اثره قد تم مناقشة العديد من الاستراتيجيات القانونية والحقوقية وسبل مواجهة الجريمة الإلكترونية وجرائم الإرهاب، إذ أكد هذا المؤتمر على الحاجة الملحة إلى تفعيل ما تضمن هذا المؤتمر من قرارات واتفاق بين الدول الأعضاء في الامم المتحدة ازاء المخاطر والتهديدات الإرهابية الإلكترونية من خلال اعتماد الية فعالة ملزمة تحظر الإرهاب الإلكتروني بكافة أشكاله[3].

ثالثا : إتفاقية برن الدولية لحماية المصنفات الأدبية والفنية

جاء في هذه الإتفاقية مجموعة من القرارات والنصوص التي تتضمن توفير الحماية اللازمة لحماية المصنفات الأدبية والفنية، وحقوق المؤلفين وغيرها، وكذلك تضمنت هذه الاتفاقية مجموعة من القرارات التي تسمح للمؤلفين والموسيقيين والشعراء والرسامين وما إلى ذلك، سبل التحكم في طريقة إستخدام مصنفاتهم ومن يستخدمها وبأية شروط . وقد إستندت هذه الاتفاقية إلى ثلاثة مبادئ أساسية تتمثل بمجموعة من الأحكام المتعلقة بالحد الأدنى للحماية الواجب منحها وبعض الأحكام الخاصة التي

(1) - ايمان يوسف صبرة، الحقوق الاجرائية للمجني عليه في الجرائم الالكترونية في التشريع الفلسطيني، دراسة مقارنة، الجامعة الاسلامية بغزة، كلية الشريعة والقانون، 2020 ، ص 26.

(2)- ينظر : دليل التعاون الدولي في المسائل الجنائية لمكافحة الارهاب، وثيقة صادرة عن مكتب الامم المتحدة المعني بالمخدرات والجريمة (فيينا) ، 2009، ص 236.

(3)- ينظر: دراسة حول تشريعات مكافحة الارهاب في دول الخليج العربي واليمن، وثيقة عمل صادرة عن مكتب الأمم المتحدة المعني بالمخدرات والجريمة (فيينا)، 2017، ص 34.

وضعت لمصلحة البلدان النامية التي ترغب في إستخدامها[1].

رابعا : المكتب العربي للشرطة الجنائية

من مظاهر التطور التكنولوجي نلاحظ ان الجريمة قد تطورت تطوراً ملحوظا وأصبحت الجريمة معقدة في اسلوبها وتنفيذها في الوقت الحالي، بسبب التطور التكنولوجي الذي أصبح جزءاً لا يتجزأ من حياة الأفراد، مما أدى إلى أن تأخذ الجريمة الإلكترونية بعدا دوليا تتعدى الحدود الاقليمية وتنفذ بكل سهولة، الامر الذي حتم على المشرعين في مختلف الدول إلى إعادة النظر في القواعد المنظمة للتجريم والعقاب لتواكب التطور التكنولوجي السريع.

فمنذ سنوات لم يكن المشرع في الدول العربية يأخذ بنظر الإعتبار بانعكاسات التطور التكنولوجي الذي يعيشه العالم، في ظل استخدام الحاسب الآلي وتطبيقاته، وكذلك ظهور شبكت الإنترنت وغيرها من التقنيات الحديثة التي يعيشها المجتمع في الوقت الحالي، وما ينتج عن هذه التطور التكنولوجي من سلبيات بسبب الاستخدام الخاطئ لهذه التقنيات، أضف الى ذلك وجود نقص تشريعي يواكب هذا التطور ومدى انعكاسه على السياسة الجنائية، التي أصبحت عاجزة عن مكافحة هذه الجرائم (جرائم الإنترنت)، ونلاحظ ان وسائل التقنية الحديثة خاصة الحاسب الآلي وشبكات الإنترنت والهاتف المحمول والكاميرات الحديثة تلعب دوراً كبيراً في إرتكاب هذه الجرائم، سواء تعلقت بالأموال أو الحياة الخاصة للأفراد، أو جرائم المال العام، جميعها جرائم يتم إرتكابها عن بعد وبوسائل تقنية حديثة [2].

وعلى ضوء ما ذكر فقد أهتمت بعض الدول العربية والأوربية على عقد مجموعة من الاتفاقيات الثنائية والجماعية على الصعيد الدولي والإقليمي، كاتفاقية مكافحة جرائم الإنترنت لتسهيل التحقيق في الجرائم المعلوماتية، وعلى المستوى العربي هناك القانون الإسترشادي لمكافحة جرائم تقنية المعلومات والذي تم إعداده من قبل لجنة مشتركة بين المكتب التنفيذي لمؤتمر وزراء العدل العرب- والمكتب التنفيذ لمؤتمر وزراء الداخلية العرب، ونلاحظ أن دولة الامارات العربية المتحدة هي السباقة ومن أوائل الدول العربية التي تصدت لمكافحة جرائم الإنترنت، وهو ما يمثل اهتمام المشرع الجنائي الاماراتي ومدى مواكبته للتطور التكنولوجي [3].

---

(1) - جغدم محمد الامين، جرائم الارهاب الالكتروني والجرائم المنظمة، بحث منشور، مجلة كلية الحقوق، جامعة عبدالحميد ابن باديس، العدد 6، 2018 ، ص 138 .

(2) - عبدالعزيز سالم السنيدي، المصدر السابق ، ص 29.

(3) - عبدالعزيز سالم السنيدي ، المصدر نفسه ،ص 31 .

وفي عام (1982) تأسس مكتب الشرطة الجنائية من قبل مجلس وزراء الداخلية العرب، بناء على إتفاقية خاصة تتضمن إنشاء منظمة عربية للدفاع الإجتماعي لمكافحة الجريمة العابرة للحدود وبعض الجرائم التي تمس الوحدة العربية، ومقر هذا المكتب في العاصمة السورية (دمشق)، ويمثل هذه المكتب ثلاث وزارات متخصصة في هذا الشأن وهي (الداخلية والعدل والشؤون الاجتماعية) على مستوى الدول العربية. ومن أختصاصات هذا المكتب، هو تأمين التعاون في مكافحة الجريمة بين أجهزة الشرطة في الدول العربية الاعضاء، وملاحقة المجرمين بموجب القوانين والانظمة التي تضمنتها الاتفاقية [1]. وقد حقق هذا المكتب منذ تأسيسه خطوات كبيرة في مجال التعاون الامني والعربي المشترك، ودعم جهود مكافحة الجريمة المنظمة بكل اشكالها، وعملت الحكومات العربية الأعضاء على زيادة التعاون في ما بينها من تبادل المعلومات وتبادل الوثائق والمستندات الخاصة بالمجرمين. وامام جميع هذه المعطيات، وعلى الرغم من الجهود العالمية والإقليمية التي أسهمت في الحد من انتشار الجريمة المنظمة والجرائم المعلوماتية، من أجل إستقرار هذه الدول، إلا أنه يتطلب بذل المزيد من الجهود والتعاون الدولي والإقليمي، من أجل الحد من إنتشار هذه الجرائم [2].

ومن الامثلة على التعاون والإتفاقيات العربية، الإتفاقية بين السلطنة العمانية والمملكة العربية السعودية، وكذلك فيما بين دول مجلس التعاون الخليجي، منذ عام (1982) بما يسمى إتفاقية الرياض للتعاون القضائي، واتفاقية مجلس التعاون الخليجي عام (1994)، والإتفاقية الخاصة بالتعاون القضائي بين سلطنة عمان وبين دولة مصر العربية عام (2002)[3].

بالإضافة إلى صدور مجموعة من القوانين العربية المقارنة تتضمن توفير الحماية اللازمة للتعامل التجاري عبر مواقع الإنترنت وشبكات التواصل الاجتماعي، ومنها ما جاء بنص المادة (12) وما بعدها من مشروع قانون التجارة الإلكترونية المصري، وكذلك من التشريعات العربية هو صدور القانون التونسي الخاص بالتجارة الالكترونية (83) لسنة 2000 ، وجاء بمضمون نص المادة (25) منه إلى إلزام البائع بتوفير المعلومات الكافية وبصورة واضحة وقبل ابرام العقد، وقد أحتوت هذه المادة على كافة التفاصيل التي تكفل الحماية اللازمة لأطراف التبادل الالكتروني، وصدر بعدها قانون رقم 22 لسنة 2016 والمتعلق بالحق في النفاذ إلى المعلومة والذي يُعد من أهم والقوانين واحدثها، وأيضا أصدرت إمارة دبي على المستوى المحلي القانون رقم 26 لسنة 2015 القانون الخاص بتنظيم

(1) - محمد كمال محمود السوقي، المصدر السابق ، ص 140.
(2) - لينا محمد الاسدي، المصدر السابق، ص 44.
(3) - د. حسين بن سعيد الغافري، المصدر السابق، ص 655.

وتبادل البيانات في إمارة دبي[1]. ونجد أن دولة لبنان أيضا شرعت بإصدار قانون التبادل والتجارة الالكتروني، وذلك بتشريع قانون المبادلات والتجارة الالكترونية وحماية المستهلك على شبكة الانترنت، رقم 659 لسنة 2005 المعدل[2].

ويرى الباحث أن على المشرع العراقي مواكبة التطور التكنولوجي الذي يعيشه البلد في ظل العولمة والانفتاح الذي يعيشه المجتمع. وأن يحرص على إدراج ما يستجد ويستحدث من الجرائم الإلكترونية، لكون العراق من الدول التي تعتمد القوانين التقليدية لمكافحة جرائم الإنترنت والتكنولوجيا، ولم يتم تشريع اي قانون جديد كما فعلت دول أوروبا وبعض الدول العربية، وهذا يمثل قصوراً تشريعياً يسبب خللاً في الأمن المجتمعي والأقتصادي والسياسي. فالجريمة الإلكترونية لا يمكن وصفها على أنها جريمة عادية لكن بثوب جديد، وإنما هي جريمة جديدة مستحدثة ترتكب بكل سهولة وعن بعد، ولا تتطلب أي مجهود بدني، فهي تستهدف مصلحة معنوية لا مادية، لكونها تستهدف معلومات وأشياء غير محسوسة، لذلك ففي الوقت الحاضر أصبحت تلك المعلومات المعنوية وغير المحسوسة هي المقياس الذي تقاس به قوة الشعوب، بمعنى ادق إن من يملك تقنيات حديثة، يستطيع أن يسيطر على أهم أسباب القوه، لكون هذه المعلومات والتقنيات التكنولوجية تُعد هي أداة حرب واقتصاد وإعلام في الوقت الحاضر. وهذا يعني أن محاولة تطويع النصوص الجنائية التقليدية على الجرائم الإلكترونية، أمر لا يمكن الإعتماد عليه فقد ظهر هناك قصورٌ تشريعي واضح في أغلب التشريعات المقارنة، إزاء الإحاطة بهذه الجرائم التقنية الحديثة.

خامسا : الشرطة الأوربية (يوروبول)

أنشأ الاتحاد الاوربي جهاز يسمى (يوروبول) في عام (1992) بموجب الإتفاقية المؤسسة للإتحاد الاوربي، تسمى اتفاقية (ماستريخت) ،ويكون مقر هذه الجهاز في (لاهاي – هولندا)، وقد بدا هذا الجهاز عمله الفعلي عام (1999)، يتخصص بملاحقة الجناة الذين يرتكبون الجرائم المنظمة العابرة للحدود، وكذلك ملاحقة مرتكبي الجرائم الإلكترونية ، إذ إن هذه الجهاز يُعد همزة وصل بين الشرطة المحلية، في الدول الأعضاء، ويكون عمل هذا الجهاز (يوروبول) من خلال إنشاء مكاتب في كل دول الاعضاء؛ من أجل التنسيق والتعاون في تبادل المعلومات والإجراءات من أجل مكافحة الجريمة العابرة للحدود وجرائم الإنترنت، وتقدم هذه المكاتب المساعدة للجهاز المركزي (يوروبول) من تلقاء نفسها أو بناء على طلب من مجلس إدارة اليوروبول . ويعمل هذا الجهاز في الوقت الحالي من خلال

(1) - د. تامر محمد صالح، الحماية الجنائية للحق في المعلومات الرسمية، ط1، دار الفكر والقانون، 2021 ، ص46 .

(2) - د. فريد منعم جبور، حماية المستهلك عبر الانترنت ومكافحة الجرائم الالكترونية، ط1، منشورات الحلبي الحقوقية، لبنان، بيروت، 2010، ص 33.

تعاون (27) دولة من أعضاء الاتحاد الأوروبي، بالإضافة إلى الشراكة مع جهات تنفيذ القانون في دول خارج الاتحاد الأوربي مثل دولة استراليا وكندا والولايات المتحدة والنرويج. ويتمثل عمل هذا الجهاز والمكاتب (اليوروبول) من خلال تقديم المساعدة والمعلومات وسبل كشف الجرائم وتقديم الإستشارات وإبداء الخبرة والمحللين الجنائيين في القضايا الجنائية، من خلال ارسال فرق متخصصة، ويشرف على جهاز اليوروبول، مجلس الوزراء لشؤون العدل والداخلية الذي يتألف من وزراء العدل والشؤون الداخلية من جميع دول الأعضاء في الاتحاد الأوروبي[1].

(1) - محمد كمال محمود السوقي، المصدر السابق ، ص 137.

الفصل الثاني

مظاهر الحماية الجنائية الموضوعية في ظل التطور التكنولوجي

أن حق الإنسان في سلامة جسده من كافة أشكال الإعتداء والتعذيب وإلحاق الأذى والآلام من الحقوق التي نالت أهتماماً كبيراً خاصة في السنوات الاخيرة التي تتمثل بإستخدام التطور التكنولوجي في كل تفاصيل الحياة، مما يجعل هذا التطور يهدد سلامة الجسد والتكامل الجسدي، وهذا يستلزم تشريع حماية وضمان لسلامة جسد الإنسان، وعلى أساس ذلك فقد نظمت القوانين الداخلية للدول وكذلك المواثيق والإتفاقيات الدولية لحقوق الإنسان مجموعة من هذه الضمانات لحماية سلامة الإنسان، لكون هذا الموضوع يوقع على عاتق الدول التزاماً قانونياً بضرورة حماية الكيان الجسدي للإنسان، فقد جرمت أغلب التشريعات المساس بهذا الجسد وحملت المسؤولية الجزائية في حق المعتدي مهما كانت الطرق والأساليب. وعلى ضوء ذلك سنتناول دراسة هذا الموضوع على مبحثين نخصص المبحث الاول لدراسة تأثير التطور التكنولوجي على حق الإنسان في السلامة الجسدية، ونبحث موضوع تأثير التطور التكنولوجي على ظهور الجرائم الإلكترونية في مبحث ثان.

المبحث الأول

تأثير التطور التكنولوجي على حق الإنسان في السلامة الجسدية

الحق في الحياة أغلى ما يملكه الإنسان، وأحترام كرامة الإنسان يتطلب الحفاظ على حياته وسلامة جسده، فالكرامة الإنسانية أصل حقوق الإنسان الأساسية، إذ أشارت الإتفاقيات الدولية والقوانين الوطنية إلى ضرورة أحترام حياة الإنسان وجسده، وعدم حرمان أي إنسان من حياته تعسفياً، وذلك إستناداً إلى حقه في الكرامة، بمعنى أن الإنسان يمكن حرمانه من حياته، سواء قبل ولادته، كما هو الحال في الانهاء الإرادي للحمل (الجنين)، وسواء بعد ولادته، كما في حالة عقوبة الإعدام، أو كما في حالة القتل بدافع الشفقة (القتل الرحيم). وللإحاطة بموضوع حق الانسان في السلامة الجسدية، سنخصص دراستنا في هذا المبحث لدراسة ماهية حق الانسان في السلامة الجسدية في مطلب أول، ونخصص المطلب الثاني لدراسة أثر التطور التكنولوجي على حق الانسان في سلامة جسده.

المطلب الأول

ماهية حق الانسان في السلامة الجسدية

من أجل بيان ماهية حق الانسان في السلامة الجسدية يتوجب علينا بيان مفهوم حق الانسان في السلامة الجسدية، وذلك من خلال توضيح تعريف الحق لغة واصطلاحا ، وبيان مفهوم السلامة الجسدية وفق المفهوم القانوني والطبي، ومن ثم وبيان حق الانسان في القوانين الجنائية .

الفرع الأول

مفهوم حق الانسان في السلامة الجسدية

أثار مصطلح الحق جدلاً فقهياً، أختلف فقهاء القانون في معناه، ومن أجل معرفة مدى تباين الآراء في مضمون وتعريف الحق عند الفقهاء، فإننا سنحاول بيان التوجهات في تعريف هذا الحق، والآراء التي طرحت من خلال التوجهات الفقهية والفلسفية. ولذا سنتناول تعريف الحق لغة، وإصطلاحاً، ومن أجل عدم إغفال موقف التشريع الاسلامي من مفهوم الحق، سنتناول تعريف الحق في الشريعة الإسلامية على النحو الاتي:

أولا : تعريف الحق:

الحق لغة : هو أسم من أسماء الله تعالى، وصفاته، وهو الثابت الذي لا يمكن إنكاره، والحق يكون في الصدق والصواب. الحق هو نقيض الباطل، والحق هو مصدر حق الشيء إذا وجب وثبت، ويقال حق الأمر حقاً، وحقه حقوقاً صح وثبت وصدق، وجمع الحق، حقوق وحقاق[1]، يقول الله سبحانه وتعالى: (قَالَ الَّذِينَ حَقَّ عَلَيْهِمُ الْقَوْلُ)[2]. اي ثبت. وقوله تعالى: (فَأَمَّا الَّذِينَ آمَنُوا فَيَعْلَمُونَ أَنَّهُ الْحَقُّ مِن رَّبِّهِمْ) [3]. الحق ، بمعنى اليقين.

1- **الحق إصطلاحاً :** ظهرت اتجاهات ثلاثة لتعريف الحق [4]. ونجد أن مفهوم الحق عند أصحاب الإتجاه الشخصي: وهم الذين اقاموا الحق على أساس السلطة التي يخولها القانون لصاحب الحق، أما الاتجاه الثاني: وهو الموضوعي، فقد صوروا الحق على أساس المصلحة التي يقررها القانون لصاحب الحق،

---

(1) - مجمع اللغة العربية، المعجم الوسيط، اخرجة مجموعة من العلماء، الطبعة الثانية، المكتبة الاسلامية، ص188.

(2) - سورة القصص، الآية (63).

(3) - سورة البقرة ، الآية (26).

(4) - ينظر: د. محمد عبدالظاهر موسى، الحماية الجنائية للجسم البشري في ظل التطورات الطبية الحديثة، ط1، دار مصر، 2021 ، ص 4 . وكذلك : عفاف خذيري ، الحماية الجزائية لحق الانسان في سلامة جسده في ظل التطور التكنولوجي، بحث منشور، ضمن اعمال المؤتمر الدولي الأفتراضي، بعنوان (إنعكاسات التطور التكنولوجي على حق الانسان في السلامة الجسدية) ، برلين - المانيا ، 2021 ، ص 132.

وقد وجهت مجموعة انتقادات للاتجاهين السابقين، وعلى أساس ذلك ظهر اتجاه ثالث توفيقي، وهو الاتجاه المختلط: والذي حاول الدمج بين مضمون الاتجاهين السابقين، وقالوا إن الحق، هو مصلحة مشروعة تقوم على تحقيقها سلطة أو قدرة يقرها ويحميها القانون[1].

أما تعريف الحق في سلامة الجسم عند بعض فقهاء القانون الحديث، فقد عُرف الحق: هو المصلحة التي يحميها القانون في أن تسير الوظائف الحيوية في جسم الإنسان على النحو الطبيعي وأن يظل محتفظا متكاملاً جسدياً متحرراً من الالام البدنية[2]. وهذا التعريف يؤكد أن الحق في سلامة الجسم مصلحة قانونية محمية بموجب القانون. وعرف الحق أيضاً: بأنه مصلحة محمية وهو من الحقوق الأساسية المعترف بها القانون، التي يحق لصاحبه في أن يظل جسمه متخذاً صورة، أو وضعاً معيناً، ويعترف له القانون بمصلحته في أن يظل محتفظا بهذا الشعور[3]. وعرف الحق أنه (ميزة يمنحها القانون لشخص ويحميها القانون)، وهو الإتجاه الحديث ومهما قيل بصدد فكرة الحق فإنها باتت من المسلمات القانونية، وأن أختلفت الآراء الفقهية في تحديد عناصرها، وقد قسم فقهاء القانون الحقوق التي يتمتع بها الأفراد، إلى قسمين، حقوق سياسية وغير سياسية، أي مدنية وتنقسم هذه الأخيرة بدوره إلى حقوق خاصة تنشأ نتيجة علاقة الفرد بغيره من الأفراد، وهناك حقوق عامة وهي التي يتمتع بها الإنسان لمجرد كونه إنسان ويتمتع بها الأفراد كافة، ومن هذه الحقوق الحق في الحياة، والحق في الأمن، والحق في سلامة الجسم وتسمى هذه جميعاً بالحقوق اللصيقة بالشخصية[4].

أما مفهوم الحق في الشريعة الإسلامية، فإن مصدر الحق عند فقهاء الإسلام هو (الله) سبحانه وتعالى، وقد قسم فقهاء الإسلام الحق إلى مفهومين: المفهوم الأول: ويقسمون الحقوق إلى ثلاثة أقسام وهي : 1- حقوق الله – هي الأفعال التي كلف الله بها عباده وتمثل حكم الله. 2- حقوق العباد- وهي أفعال المكلفين التي تتعلق بها الأحكام الشرعية والتي يراد بها تحقيق مصلحة خاصة. 3- الحقوق المشتركة- ويقصد بها تحقيق مصلحة المجتمع ومصلحة المكلف، وعلى هذا الاساس فإن الشريعة الاسلامية هي احكام تراعي الصالح العام. أما المفهوم الثاني : فيقسم الحق إلى ثلاثة اقسام ولكنهم يسقطون حقوق العباد الخالصة على أساس أن ما من حق خالص للعبد الا وفيه قدر لله جل جلالة. وعلى ضوء ذلك فان الحق في سلامة الجسم في الشريعة الاسلامي يُعد من الضروريات التي تمثل أهم

---

(1) - د. ضياء عبدالله عبود الأسدي، حق السلامة في جسم المتهم، ط2، منشورات زين الحقوقية، لبنان- بيروت، 2011، ص46.

- د. محروس نصار الهيتي، الحماية الجنائية للحق في السلامة الجسدية ، دار السنهوري، بغداد ، 2016، ص15.

(2) - د. محمود نجيب حسني، شرح قانون العقوبات الخاص، دار النهضة العربية، 1988، ص 426.

(3) - د. اكرم محمود حسين البدو، أ. بيرك فارس حسين، الحق في سلامة الجسم، بحث منشور، مجلة الرافدين للحقوق، مجلد 9 ، العدد 33، 2007، ص 4.

(4) - د. ضياء عبدالله عبود الاسدي، المصدر السابق، ص 47.

مبادئ الاسلام والشريعة، والتي تمثل حقوق خالصة لله، وايضا يمثل الحق في سلامة الجسم حق مشترك بين العبد وربه وهو من الحقوق التي تمثل حماية المصلحة العامة، وقد حرم الله سبحانه وتعالى أي أذى يصيب الجسم بشكل متعمد وأيضا حرم الاعتداء على النفس والجسد باي صورة كانت[1].

ثانيا : تعريف السلامة الجسدية :

يُعد حق الإنسان في سلامة جسده من الحقوق الجسمانية التي تتصل بجسم الإنسان وهو من أهم الحقوق التي يتمتع بها الإنسان بجميع مراحل الحياة، ويُعد من الحقوق الدستورية والتي إجتمع على ضمانها جميع المواثيق الدولية والإقليمية، وعلى ضوء ذلك فقد عرف الفقهاء السلامة الجسدية بتعريفات متقاربة تدور حول معنى واحد، فقد عرفها البعض بأنها: (مصلحة الفرد يحميها القانون في أن يظل جسمه مؤدياً كل وظائفه على النحو الطبيعي الذي ترسمه وتحدده القوانين الطبيعية وأن يحتفظ بتكامله الجسدي وأن يتحرر من الآلام البدنية)[2].ويعرف بعضهم السلامة الجسدية على أنها: (مركز قانوني يخول شاغله في حدود القانون الاستئثار بتكامله الجسدي والمستوى الصحي الذي يعيش والتمتع بالسكينة البدنية والنفسية)[3]. وهناك من يعرف السلامة الجسدية على أنها: (مصلحة ذات جانبين فردي واجتماعي بأن يحافظ الشخص على سلامة جسمه (صحته وتكامله وسكينته) يعترف بها القانون ويقرر الوسائل اللازمة لحمايتها)[4].

وللتعرف على مفهوم جسم الإنسان يقتضي منا بيان المفهوم القانوني والطبي لجسم الانسان.

1-**المفهوم القانوني لجسم الانسان :** يقصد به (ذلك الكيان المادي والنفسي الذي يباشر وظائف الحياة الطبيعية والاجتماعية وهو محل الحق في سلامة الجسم)[5]. ويعرفه بعضهم: بأنه (المحل المادي في

(1) - د. محروس نصار الهيتي، المصدر السابق، ص 17.

(2) - د . محمود نجيب حسني، الحق في سلامة الجسم ومدى الحماية التي يكفلها له قانون العقوبات، مجلة القانون والاقتصاد، العدد 3، السنة، 29، 1959، ص 540 . وكذلك : د. خوالدية فؤاد، الحق في سلامة الجسد في القانون الدولي والوطني في ظل التطور التكنولوجي، بحث منشور، كتاب صدر عن اعمال المؤتمر الدولي (انعكاسات التطور التكنولوجي على حق الانسان في السلامة الجسدية ، برلين - المانيا ، 2021 ، ص46.

(3) - محمد بومديان، الاستخدام السلبي للتطور التكنولوجي في التحقيق مع المتهم، بحث منشور، كتاب صدر عن المؤتمر الدولي الافتراضي ، بعنوان (انعكاسات التطور التكنولوجي على حق الانسان في السلامة الجسدية ، برلين - المانيا ، 2021 ، ص 217.

(4) - د. ضياء عبدالله عبود الاسدي، المصدر السابق، ص 69.

(5) - د. محمد سامي السيد الشوا، الحماية الجنائية لحق الانسان في سلامة جسمه، أطروحة دكتورته، جامعة القاهرة، كلية الحقوق، 1985، ص 65.

جرائم الإيذاء البدني وصفة الإنسان)[1]، وهذا يعني أنه محل الحق هو جسم الإنسان بجميع جزيئاته سواء كانت تؤدي وظائف عضوية كالجهاز الهضمي والقلب والاطراف، أم وظائف ذهنية أو نفسية. وتتساوى جميع أعضاء الجسم في أهميتها من حيث الحماية التي تصبغ عليها سواء كانت خارجية أم داخلية، فالإعتداء الذي يقع على عضو خارجي كالأطراف يماثل الإعتداء الذي يقع على عضو داخلي كالكبد وغيره، وسواء كانت تلك الأعضاء بشكلها المعتاد والمتعارف عليه، أم كانت تختلف، زيادة أو نقصان، كالأصبع السادس في اليد أو القدم. فلا يمكن الحاق الضرر بهذا الأصبع، بحجة انه زائد عن الحاجة فكل مساس به يُعّد مساساً بسلامة الجسم، ولا يقتصر جسم الإنسان على الأعضاء الطبيعية الاصلية التي توجد في جزء في جسم الإنسان منذ ولادته، وإنما يشمل أيضاً الأعضاء التي نقلت إليها من إنسان آخر بسبب الحاجة إليها، كالكلية، فبمجرد نقلها وغرسها في جسم المتلقي أصبحت جزءً من جسمه وتتمتع بالحماية القانونية نفسها التي تتمتع بها أعضاء الجسم الاصلية، ومن ثم فإن أي اعتداء يقع عليها يعد اعتداء على الجسم ولا يقتصر وصف أعضاء الجسم على الأعضاء الصحيحة، أي التي تؤدي وظائفها بانتظام وإنما يشمل أيضا الأعضاء العاجزة التي لا تستطيع أن تؤدي وظائفها المخصصة لها بصورة كاملة أو جزئية، فالإعتداء الذي يقع على طرف علوي أو سفلي عاجز عن القيام بوظيفته، يعد إعتداء على سلامة الجسم، لان عجز العضو عن القيام بوظيفته لا يخرجه عن دائرة الحماية الجنائية بل تضل الحماية ملازمة له ما دام متصل ببقية أعضاء الجسم كما أنه أي مساس بها صحيح أنه لا يؤثر على أداء وظيفته ما دامت عاجزه أصلا عن أدائها إلاّ أنه يؤثر على الناحية الجمالية للجسم فالإعتداء الواقع على الأجزاء العاجزة بالقطع فهو فضلا عن كونه يشكل مساساً بالتكامل الجسدي للمتهم فإنه يؤثر أيضاً على حالته النفسية ومن ثم على صحته لما يشكل مساسا بسلامة الجسم [2].

وأيضا من الناحية القانونية ينطلق مدلول الحق في سلامة الجسم من وجهة نظر رجال القانون، أساساً من مبدأ أن الحق مصلحة يحميها القانون، وإستناداً لذلك ذهب بعض الأساتذة لتعريف الحق في السلامة الجسدية على انها: (المصلحة القانونية التي يحميها القانون في أن يظل الجسم مؤديا كل وظائفه على النحو العادي الطبيعي حتى لا تتعطل إحدى الوظائف ولو كانت أقلها أهمية أو كان التعطيل وقتيا)[3].

---

(1) - د. ماهر عبد شويش الدرة، شرح قانون العقوبات القسم الخاص، العاتك للنشر، بغداد، 184. وكذلك: د.عوض محمد، جرائم الاشخاص والاموال، الطبعة الاولى، دار النجاح، الاسكندرية، 1972، ص 135.

(2) - د. ضياء عبدالله عبود الاسدي، المصدر السابق، ص 50 و 51 . وكذلك : د. منذر الفضل، التصرف القانوني في الاعضاء البشرية، دار الشؤون الثقافية العامة، بغداد، 1990، ص 34.

وكذلك: د. أكرم محمود حسين، أ. بيرك فارس حسين، الحق في سلامة الجسم، المصدر السابق، ص 5.

(3) - د. محمود نجيب حسني، الحق في سلامة الجسم، بحث منشور، مجلة القانون والاقتصاد، جامعة القاهرة، كلية الحقوق، العدد 3، السنة 29، 1959، ص 571.

ومنهم من وصف هذا الحق في السلامة الجسدية: بأنه (مركز قانوني يخول شاغلة في حدود القانون الإستثماري بتكامله الجسدي والمستوى الصحي الذي يعيشه بسكينة البدنية والنفسية)[1]. كما أن الحق في السلامة الجسدية من أهم المبادئ التي استقر عليها التشريع الفرنسي بموجب أحكام القانون رقم 653/94 الصادر عام 1994 والخاص باحترام الجسم البشري، بخصوص احترام جسم الإنسان وحماية كيانه، إذ نصت المادة 16/01 منه: على أن لكل شخص الحق في احترام جسمه وجسده وجسم الإنسان غير قابل للمساس والإعتداء. والحق في سلامة الجسم حسب هذا القانون هو المصلحة التي يحميها القانون ضمن العناصر التالية السير الطبيعي لوظائف الحياة في الجسم و التحرر من الآلام البدنية و التكامل الجسدي[2]. فالحق في السلامة الجسدية، هو ضمانة دستورية وقانونية بموجبها يُصان هذا الحق ويمنح الحماية للاستقلال الجسدي للإنسان من القتل بشكل غير قانوني ويحمي من الإختفاء والتعذيب والسجن على أساس سياسي، ويكون إنتهاك حقوق الإنسان في السلامة الجسدية بأعمال الإرهاب أو غيرها[3]. وهناك من يعرف حق السلامة الجسدية بانه: (حق الإنسان بالحماية من إجراء اي عمليات عليه لأغراض التجربة والحماية من التعذيب والاختفاء)، وذلك لأن هذا الحق من الحقوق غير قابلة للتقييد في أي ظرف من الظروف الإستثنائية أو الإعتيادية[4]. ويعرف بأنه: (حق كل إنسان بما فيهم الأطفال السلامة الجسدية وللقدرة على التحكم بأجسادهم، ويُعتبر أي تقييد لهذا الحق بمثابة انتهاك لحقوق الإنسان). ارتبط تعريف هذا الحق بشكل تقليدي بحماية الإنسان من التعذيب والاختفاء القسري والمعاملة التي تحط من الكرامة الإنسانية، وإرتبط هذا الحق بحماية حقوق الأطفال مثل الحماية من العقوبات الجسدية أو الحماية من إجراء العمليات لأغراض غير علاجية مثل التجارب، وأن حماية الأطفال من هذه العمليات مسألة ضرورية جداً لأن أجسادهم ضعيفة ولا تتحمل إجراء مثل هذه العمليات[5].

---

(1) - د. خوالدية فؤاد، الحق في سلامة الجسد في القانون الدولي والوطني في ظل التطور التكنولوجي، المصدر السابق، ص 46.

(2) - د. محمد عبدالظاهر موسى، المصدر السابق، ص 7 . وكذلك: حبيبه سيف سالم راشد ، (النظام القانوني لحماية جسم الانسان)، أطروحة دكتوراه ، جامعة عين شمس، كلية الحقوق، 2005، ص 51.

(3)- James I. Walsh and James A. Piazza, Why Respecting Physical Integrity Rights Reduces Terrorism, Comparative Political Studies, 2010, 552.

(4)- A Nienaber, The right to physical integrity and informed refusal: Just how far does a patient's right to refuse medical treatment go?, SAJBL, Vol. 9, No. 2, 2016, 73.

(5)- Bodily Integrity, Child Rights international Network, the link: ((https://archive.crin.org/en/home/whatwedo/policy/bodilyintegrity.html#:~:text=The%20principle%20of%20bodily%20integrity,as%20a%20human%20rights%20violation.)), Accessed at (04-07-2022).

2- **التعريف الطبي لجسم الانسان:** ذهب بعضهم إلى تحديد مدلول الحق في سلامة الجسم في إطار صحة الكائنات البشرية فالصحة هي: (إتحاد مادة الجسم بجميع جزيئاته وقدراته على الإدراك، والشخص المعافى هو الذي يتمتع بسلامة الجسم في مجموع هذه العناصر على نحو يحقق الانسجام والملائمة بينهما[1]. أما المرض فهو عجز مؤقت أو نهائي للجسم عن تحقيق كل أو جزء من أهدافه الحياتية وهذا الخلل في البرنامج الجيني أو الإستراتيجيات الفردية أو لضغط كبير في المحيط أو حالة من القلق تجاه فاعلية هذا الجسم كما إستند مفهوم الحق في السلامة الجسدية من الناحية الطبية إلى وجود بعض العناصر التي يقوم عليها مفهوم الصحة وهذه العناصر هي خلو الجسم من الأمراض وكذلك الصحة هي عدم إحساس باي الم وبالإضافة تُعد الصحة هي العمل الطبيعي لوظائف الجسم[2]. ومنهم من وصفه بانه: (مجموعة الاعضاء التي يتكون منها جسم الانسان، وهذه الاعضاء مختلفة ومتباينة فيما بينها، وكل واحد منها يتكون من انسجة متغايرة، وهذه الانسجة هي الاساس في تكوين جسم الانسان وتقوم بأداء وظائفها الحيوية)[3].

وعلى ضوء ذلك يقصد بالسلامة الجسدية هو أن تستمر أعضاء الجسم تؤدي وظائفها على النحو الطبيعي، فالحق في التكامل الجسدي، هو حق الإنسان في أن يحتفظ بأعضاء الجسم كاملة غير منقوصة سواء بالبتر أو التغيير ولو كان ذلك بفترة يسيرة[4]، إذ إن أي فعل ينقص من تماسك الأنسجة يُعد من قبيل المساس بسلامة الجسم ولكل إنسان الحق في ألاّ تضعف صحته، ولا يعتل بدنه، ومن أجل ذلك فإن كل فعل ينقص من هذا المستوى يُعد اعتداء على السلامة الجسدية سواء تحقق ذلك عن طريق مرض لم يكن موجودا من قبل أم بالزيادة من مقدار مرض كان المجني عليه يعاني منه [5].

أما فيما يخص السلامة الجسدية لجسم الانسان في الشريعة الاسلامية، فقد أخذ هذا الموضوع اهتماما كبيرا من قبل فقهاء الشريعة الاسلامية، وقالوا ان حق تصرف الانسان على جسمه هو حق انتفاع، أما ملكية الرقبة هي لله عز وجل، فان تصرف الانسان في جسمه أو في جزء منه هو تصرف فيما لا

(1) - د. أحمد عمر ابو خطوة، شرح القسم الخاص من قانون العقوبات، جرائم الاعتداء على الاشخاص، دار النهضة العربية، 2010، ص 139.

(2) - د. عيساني رفيقة، بحث بعنوان (الحماية القانونية للسلامة الجسدية للإنسان في ظل التطور التكنولوجي الطبي)، كتاب صدر عن المؤتمر الدولي الافتراضي ، بعنوان (انعكاسات التطور التكنولوجي على حق الانسان في السلامة الجسدية ، برلين - المانيا ، 2021 ، ص 153.

(3) - صباح سامي داود، المسؤولية الجنائية عن تعذيب الاشخاص، اطروحة دكتوراه، جامعة بغداد، كلية القانون، 2000، ص 3.

(4) - عاقلي فضيلة، الحماية القانونية للحق في حرمة الحياة الخاصة، أطروحة دكتوراه، جامعة الاخوة منتوري – قسنطينة، كلية الحقوق، 2012، ص 290.

(5) - عبد السميع بالعيد محمد، (الاثار المترتبة عن التطور التكنولوجي على حق الانسان في سلامة جسده) ورقة عمل مقدمة، ضمن اعمال المؤتمر الدولي بعنوان (انعكاسات التطور التكنولوجي على حق الانسان في السلامة الجسدية) ، برلين - المانيا ، 2021 ، ص 306.

يملك، لأن الاطار الشرعي لا يحق للإنسان ان يؤذي نفسه وجسده[1]. وتناولوا ايضا موضوع السلامة الجسدية من خلال الافعال أو الاعمال المباحة في مجال استعمال الحق عند تأديب الزوج لزوجته وابنائه، وفيما يخص تأديب الزوج زوجته، قال تعالى: (..... وَاللَّاتِي تَخَافُونَ نُشُوزَهُنَّ فَعِظُوهُنَّ وَاهْجُرُوهُنَّ فِي الْمَضَاجِعِ وَاضْرِبُوهُنَّ فَإِنْ أَطَعْنَكُمْ فَلَا تَبْغُوا عَلَيْهِنَّ سَبِيلًا إِنَّ اللَّهَ كَانَ عَلِيًّا كَبِيرًا)[2]. وقد أختلف الفقهاء في تفسير هذه الآية الكريمة، فذهب الأمام (مالك والأمام ابو حنيفة) إلى أن الضرب لا يكون على أول معصية، وانما يكون في المرة الثالثة، لان الواو، التي وردت في الآية الكريمة تفيد الترتيب، ويتفق هذا الرأي مع الرأي الاكثر قبولا عند مذهب الإمام الشافعي واحمد، وهناك من ذهب إلى أن الواو في الآية الكريمة تفيد للجمع المطلق وليس للترتيب، كما جاء في الرأي الاول، وعلى ضوء ذلك فان تباين الرأيين يؤدي إلى أمر ذي أهمية بالغة، من خلال الاثار التي تترتب عليهما، فوفقا للرأي الاول فأن الزوج يعاقب على جريمة ضرب زوجته، اذا رفعت الزوجة أمرها إلى القاضي، وانه لم يسبق له ان وعضها في المعصية الاولى، أو هجرها في المعصية الثانية، أما وفقا للرأي الثاني فلا يعاقب الزوج على ضربه زوجته لأول معصية ولو اقر بذلك. أما عند الامامية (المذهب الجعفري) فقد إتفقوا على أن حق تأديب الزوج لزوجته لا بد من توافر حالة، لكي يحق للزوج أن يضرب زوجته من باب إستعمال الحق، وهذه الحالة هي حالة النشوز، والتي جاء ذكرها في الآية الكريمة (34) من سورة النساء، والنشوز عبارة عن خروج الزوجة عما يجب عليها من حق الزوج الخاص؛ وذلك لعدم تمكينه مما يستحقه من الإستمتاع بها، وقبل أن يقوم الزوج بضرب زوجته لتأديبها، فلابد على الزوج أن يبادر بالموعظة والنصح وإرشادها بجميع السبل، فإن لم ينفع ذلك معها فعليه إتخاذ الأسلوب الثاني وهو أن يقوم بهجرها، لعلها ترجع عن منع زوجها، فإن لم ينفع أيضا معها هذا الإجراء، فعليه بضربها، أي ضرباً تأديبياً غير جارح، ولا مبرح، وأن لا يسبب احمراراً، أو ارقاقاً، أو سواداً في جسمها، لردعها عن تمردها[3]. والرأي الذي نؤيده هو الرأي الاول لـ (مالك وأبو حنيفة)، لان الترتيب الوارد في الآية الكريمة يفيد التدرج في العقاب التأديبي، وهو ما يعتمد في معظم النصوص العقابية [4].

(1) - أحمد عمران، حماية الجسم البشري في ظل الممارسات الطبية والعلمية الحديثة، أطروحة دكتوراه، جامعة وهران، كلية الحقوق، 2010، ص 177.

(2) - سورة النساء الاية (34).

(3) - ينظر: اسراء أسد، المرأة في القرآن الكريم، التعاونية الثقافية للمجمع العالمي لاهل البيت عليهم السلام، الطبعة الاولى، 1430 هـ، ص 137. وينظر كذلك: الشيخ حسين الراضي، مقالات ودراسات الآداب الزوجية، القسم الثالث عشر، 2016، ص 322.

(4) - د. رابح فغرور، حق تأديب الزوجة والاولاد والضمانات الواردة عليه، بحث منشور، مجلة جامعة الامير عبدالقادر للعلوم الاسلامية، الجزائر، المجلد 33، العدد 2، 2019، ص 466.

ومن خلال ما تقدم فان تأديب الزوج لزوجته أو أبنائه، له حدود شرعية لا يمكن تجاوزها؛ لأن في ذلك مساس بسلامة جسم الانسان وهذا الأمر مخالف لمبادئ الشريعة الإسلامية السمحاء، لأن الأخيرة جاءت تؤكد على أحترام الحياة الخاصة وكرامة الإنسان، ويتعين أن يكون التأديب بالقدر اللازم والضروري فقط وعدم المبالغة في الضرب، حتى لا يتأثر إستقرار الحياة الزوجية والاسرية، والتي تبنى على أساس الأحترام والوئام المتبادل[1].

ومن خلال ما تقدم يمكن تعريف الحق في السلامة الجسدية من قبل الباحث على أنه: (هو حق ومركز قانوني، يحميه القانون من أي إعتداء، من أجل أحتفاظ الانسان بتكامله الجسدي وسكينته، وان يؤدي جسمه كل وظائفه على النحو الطبيعي، وهذا الحق يمثل مصلحه عامة، وهو من المبادئ الاساسية والدستورية).

الفرع الثاني

حق الإنسان في السلامة الجسدية في قانون العقوبات

لقد أهتمت أغلب التشريعات القانونية بموضوع الحماية المقررة للسلامة الجسدية، وذلك من خلال وجود العديد من الضمانات القانونية لحقوق الإنسان التي نصت عليها مختلف التشريعات والمواثيق الدولية، وهنا يكون دور قانون العقوبات هو ضمان لحماية الجسم البشري من خلال تجريم مجموعة من الأفعال التي تمس سلامة الجسم كالتعذيب والضرب والجرح والعنف[2]، بالإضافة إلى ذلك يُعد هذا القانون هو ضمان لحماية الحقوق والحريات، ويعرض من ينتهكها بإيقاع الجزاء والعقوبة القانونية، وايضا تتمثل الحماية القانونية في ظل قانون العقوبات للحق في السلامة الجسدية، في الجزاء الجنائي الذي يقرره عند المساس بهذا الحق، وقد تكون حماية أصلية، أو حماية تبعية[3]. ونجد أن قانون العقوبات القطري رقم (11) لسنة 2004 خصص باباً مستقلاً معنوناً بالجرائم الماسة بحياة الإنسان وسلامته. وهو ما يعكس رغبة المشرع القطري في التركيز على حماية الإنسان من الأفعال التي تلحق أضراراً بحياته وسلامته، وتضمن الفصل الأول من الباب المذكور جميع الجرائم المتعلقة في القتل والإنتحار والإعتداء على سلامة الجسم، إذ نصت المادة (300) من قانون العقوبات القطري على تجريم قتل النفس عمدا مع تشديد العقوبة لتصل إلى الإعدام في بعض الحالات، ومن أهمها إذا كان

(1) - د. عبدالفتاح خضر، النظام الجنائي (أسسه العامة في الإتجاهات المعاصرة والفقه الاسلامي) ، من دون دار نشر، 2007، ص 185.

(2) - د. خوالدية فؤاد، الحق في سلامة الجسد في القانون الدولي والوطني في ظل التطور التكنولوجي،المصدر السابق، ص 47.

(3) - ينظر: د. محمد عبدالظاهر موسى، المصدر السابق، ص 25 وما بعدها.

الفعل ازهاق الروح وقع مع سبق الاصرار أو الترصد أو عن طريق استعمال مادة سامة أو متفجرة أو إذا وقع على موظف عام أو من في حكمه، أثناء أو بسبب تأدية وظيفته أو عمله[1].

وبناء على ما تقدم نجد أن المشرع القطري وسع من نطاق الحالات التي جرم فيها فعل إزهاق الروح العمدي، والذي يعد أشد الأفعال الجرمية إعتداء على السلامة الجسدية للإنسان مع الأخذ في الحسبان تخفيف العقوبة اذا عفى ولي الدم أو قبل الدية وذلك تماشا مع أحكام الشريعة الاسلامية، ولم يكتفِ المشرع القطري بتجريم فعل إزهاق الروح من قبل الجاني بل جرم أيضا أي فعل من شأنه تحريض أو مساعدة اي شخص باي وسيلة للإنتحار، وإشترط المشرع بأن يكون الإنتحار قد تم بعلاقة سببية نتيجة التحريض، أو المساعدة التي قدمت للشخص مع الأخذ في الحسبان تخفيف العقوبة وتشديدها في بعض الحالات، التي نصت عليها المادة (305) وفي السياق ذاته شدد المشرع القطري على أي فعل يضر بالسلامة الجسدية للفرد، وقد أفرد المشرع القطري ثلاثة نصوص في قانون العقوبات جرم فيها الإعتداء على السلامة الجسدية بأي وسيلة كانت، وفي المادة (306) شدد المشرع القطري العقوبة لتصل إلى مرتبة الجنائية بالحبس عشر سنوات مرتكب أي فعل من شأنه الإعتداء على سلامة جسم غيره وأدى ذلك إلى موته، وشدد العقوبة إذا كان الفعل قد سبقه إصرار وترصد من قبل الجاني إذ تكون عقوبة الحبس (15) عاماً، و نصت المادة (308) من قانون العقوبات القطري على أنه: يعاقب بالحبس مدة لا تتجاوز سنتين إذا أدى اعتداء الجاني على سلامة الجسم المجني عليه إلى مرضه أو عجزه عن القيام بأعماله الشخصية لمدة تزيد على 20 يوماً، وشدد العقوبة لتكون بالحبس مدة لا تتجاوز ثلاث سنوات إذا سبقه فعل الاعتداء سبق الاصرار أو الترصد أو كان الفعل قد ارتكبه عدد من الأشخاص وعاقب المشرع القطري في المادة (309) من القانون ذاته على إرتكاب أي فعل من شأنه الإعتداء على سلامة الجسم المجنى عليه حتى لو لم يؤدِ ذلك إلى ضرر جسيم كما هو مذكور في المادتين السابقتين[2]. أما قانون العقوبات اللبناني رقم (340) لسنة 1943 المادة (549) والتي عدلت المرسوم رقم (112) لسنة 1983 ، إذ جرم المشرع اللبناني القتل العمد، ونص بأن تكون عقوبة الإعدام في الحالات ذاتها التي نص عليها المشرع القطري، إذ اشترط أن يكون قد سبق في القتل إصرار أو ترصد، أو إذا وقعت الجريمة على احد الأصول الجاني أو فروعه، أو إذا كان فعل القتل على موظف عام اثناء تأديته لوظيفته أو بسببها. وفي هذا المجال نلاحظ انه كل الحالات السابقة من

(1) - فاطمة عبد الله علي عمران، دور التشريعات الداخلية في حماية حق الانسان في السلامة الجسدية من الاثار السلبية للتطور التكنولوجي، بحث منشور، كتاب صدر عن المؤتمر الدولي الافتراضي، بعنوان انعكاسات التطور التكنولوجي على حق الانسان في السلامة الجسدية ، برلين - المانيا ، 2021 ، ص 59

(2) - فاطمة عبد الله علي عمران، دور التشريعات الداخلية في حماية حق الانسان في السلامة الجسدية من الاثار السلبية للتطور التكنولوجي، المصدر السابق ، ص 61.

الممكن أن تتم الأفعال الجرمية عن طريق استخدام السلبي للتكنولوجيا المتطورة، إذ قد يلجأ المجرم إلى استخدام الوسائل الإلكترونية في الترصد ومراقبة المجني عليه، أو قد يستخدم الجاني أي من الآلات التقنية الحديثة، كالمتفجرات أو المفرقعات لإزهاق روح المجنى عليه، أو قد تكون الجريمة ترتكب بإستخدام سلاح إلكتروني غير مصرح به أو تعسف الجاني في إستعمال السلطة.

ونجد المشرع البحريني كان له موقفاً إيجابياً في القانون رقم (60) لسنة 2014 بشأن جرائم تقنية المعلومات، فقد جاء في نص المادة (3) منه على انه: يعاقب بالحبس والغرامة التي لا تتجاوز(50,000 دينار) أو بإحدى هاتين العقوبتين من أحدث تلفا في بيانات وسيلة تقنية المعلومات أو نظام تقنية المعلومات وتضاعف العقوبة إذا ترتب على ارتكاب الجريمة أي مما يلي: أ-اعاقة لسير أي من المرافق العامة أو الأعمال ذات المنفعة العامة. ب- تهديد لحياة الناس أو امنهم أو صحتهم . ج- مساس بسلامة جسم الإنسان، د- تغيير أو تعييب أو شطب فحوص طبية أو تشخيص طبي أو علاج إنسان وتكون العقوبة السجن المؤبد أو المؤقت إذا ترتب على إرتكاب الجريمة موت إنسان عمداً. وقد شدد المشرع البحريني العقوبة إذا كان الفعل إتلاف البيانات في وسائل تقنية المعلومات ينتج عنه أضرار بحياة الإنسان وسلامته أو أمنه، وهو ما يؤكد حرص المشرع على تجريم كل ما يمس بسلامة الإنسان بشكل عام على الرغم من تضمن القانون ذاته نصوصا مستقلة لاحقاً لتجريم عدد من الأفعال المؤدية إلى الأضرار بالإنسان[1].

ونلاحظ أن بعض القوانين المقارنة كما في القانون الفرنسي فقد أعطى المشرع الفرنسي وأكد على ضرورة أحترام جسم الإنسان وذلك بمقتضى القانون رقم (94 - 653) الصادر عام 1994 إذ نص المشرع الفرنسي صراحة على أن " كل شخص له الحق في أحترام جسده" ولكن جانب من الفقه يرى أن هذا النص معيب لأن الشخص لا يمكنه أن يطالب باحترام جسده إستقلالاً عن الشخص نفسه، فاحترام الجسد يتعلق بالشخص نفسه، ولذلك فاحترام جسد الإنسان يعتمد على عدة مبادئ أساسية، وهي مبدأ عدم جواز المساس بجسم الإنسان، ومبدأ عدم جواز التصرف في جسم الإنسان، ومبدأ عدم جواز التعامل المالي في جسم الإنسان، وقد نص المشرع الفرنسي أيضا على مبدأ تكامل الجنس البشري في القانون الصادر عام 1994 والمضاف إلى المادة (16 -4) من التقنين المدني الفرنسي. وقد قرر المجلس الدستوري الفرنسي في حكمه الصادر بتاريخ (27) يوليو عام 1994 إن هذه المبادئ تعد ضمانة أساسية خاصة باحترام المبدأ الدستوري الخاص باحترام الكرامة الإنسانية. وعلى ضوء ذلك ترى غالبية الفقه الفرنسي أن ضمانات مبدأ الكرامة الإنسانية التي ذكرها المجلس الدستوري في

(1) - فاطمة عبد الله علي عمران، دور التشريعات الداخلية في حماية حق الانسان في السلامة الجسدية من الاثار السلبية للتطور التكنولوجي، المصدر السابق ، ص 63.

حكمه السابق، إن الإشارة إليه لا تشكل في حد ذاتها مبادئ دستورية، ومع ذلك فإن هذه الضمانات تتميز بأنها ثابته ولا يمكن للمشرع أن يتجاوزها أو إلغائها دون أن يحل محلها ضمانات معادلة[1].

ونجد ان القوانين التي تحكم مفردات الحياة اليومية في المجتمع كثيرة ومتنوعة، ولعل من أهم هذه القوانين قانون العقوبات، ذلك القانون الذي يختلف عن باقي فروع القانون، لكونه يقي المجتمع ويحمي المصالح العامة، فقانون العقوبات يمتد ليشمل ركائز وجود المجتمع الأساسية ودعائمها اما مقومات الرقي بالمجتمع فهي من اختصاص القوانين الاخرى، وعلى ضوء ذلك فان قانون العقوبات هو (مجموعة من القواعد القانونية تحدد الأفعال التي تعد جرائم وتبين الجزاء المقرر لها)، أو هو (مجموعة القواعد التي تفرضها الدولة وتحدد ما يعد من الافعال جرائم وما يفرض لها من جزاء). وبعضهم وصف قانون العقوبات بانه (مجموعة القواعد القانونية تضعها الجماعة لتنظيم شؤونها وسد حاجاتها اذ هي قواعد متأخرة عن الجماعة)، أو هي في مستوى الجماعة اليوم، بمعنى انها قواعد عامة، تسري على كل الجرائم أو أغلبها، وعلى كل العقوبات أو أغلبها، خاصة بكل جريمة على حدة تبين اركانها وتحدد عقوباتها، فقانون العقوبات يتناول بالتجريم كل الأفعال التي تنال من حقوق الإنسان ومنها حقه في الحياة وسلامة الجسم[2]، وهذا ما جاء في قانون العقوبات العراقي، الجرائم الماسة بسلامة البدن في المواد (412 لغاية 415) وهو ما تضمنه الفصل الثالث بعنوان (الجرح والضرب والايذاء العمد) من الباب الأول الجرائم الماسة بحياة الإنسان وسلامة بدنه، والجرائم الماسة بالحق في سلامة الجسم شأنها شان باقي الجرائم تكون على صورتين من حيث الركن المعنوي، فهي أما عمدية، إذ يتطلب القانون توافر القصد الجنائي فيها أو غير عمديه تحصل بمجرد توافر الخطأ من جانب الجاني وأين كان صورته سواء تحقق هذا الفعل بالإهمال أم الرعونة أم عدم الانتباه أو عدم الأحتياط أو عدم مراعاة القوانين والأنظمة والأوامر، ولعل من المناسب هنا بأن الحكمة التي دعت المشرع إلى تجريم الأفعال التي من شأنها المساس بسلامة جسم الإنسان أو الجسم المجنى عليه، فالحكمة تتجلي في حماية حق الإنسان في التكامل الجسدي، أي حقه في الاحتفاظ بمادة جسده كامله، فقانون العقوبات يعد كل مساس بهذا التكامل الجسدي وأيا كانت صورته، فهو فعل مجرم يمس سلامة جسم المجنى عليه، ونلاحظ أن قوانين العقوبات المقارنة أيضاً عالجت هذا الأمر ومنها قانون العقوبات المصري في المواد (236 ، 240 ، 244) بعنوان الجنايات والجنح التي تحصل لأحاد الناس، الباب الأول، وكذلك قانون العقوبات الجزائري لسنة 1966 المواد (264 لغاية 272)، وكذلك قانون العقوبات الأردني

(1) - د. شريف يوسف خاطر ، الحماية الدستورية للكرامة الانسانية، دار النهضة ، القاهرة، 2006، ص186.
- وكذلك ينظر: د. أحسن بوسقيعة، الوجيز في القانون الجزائي العام، الطبعة الثامنة عشرة، دار هومه، 2019، ص 170.
(2) - ينظر: د. سلطان الشاوي، الجرائم الماسة بسلامة الجسم، من دون دار نشر ، 2007، ص 52 وما بعدها.

رقم (16) لسنة 1960 المعدل، وعلى أساس ذلك فإن الركن المادي لهذه الجرائم يتكون من أربعة عناصر وهي: 1- فعل السلوك يقع من الجاني 2- وقوع الفعل على مصلحة يحميها القانون. 3- نتيجة ظاهرة تصيب هذه المصلحة 4- العلاقة السببية التي تربط بين الفعل والنتيجة ظاهرة، ويمكن القول أن قانون العقوبات هو قانون يترجم واقع وحال المجتمع، فإن بالضرورة يوازن بين المصالح المتعارضة بالقدر الذي يؤمن سير حياة المجتمع بالشكل الذي ترسمه السياسة الجنائية للبلد، فقانون العقوبات حين يقرر تجريم أعمال العنف والضرب والجرح والإيذاء وإعطاء المواد الضارة، بوصفها تنال من سلامة الجسم ومن تكامله الجسدي، فانه في موضوع آخر يبيح بعض الأعمال التي تُعد مساساً بهذه السلامة وذلك إستنادا من الأصل العام في التجريم والعقاب على هذا المساس، وذلك لحماية مصلحة راجحة يقرر المشرع جدارته بالحماية الجنائية فأباحها في بعض هذه الأفعال أو الحالات، ومنها حق ممارس الالعاب الرياضية، وحق ممارس اعمال الجراحة (العمليات الجراحية) وفق أصول الفن والمهنة، إذا ما توافرت الشروط العامة التي يتطلبها القانون لإباحة كل عمل من هذه الأعمال[1].

إن الحق في سلامة الجسم هو مصلحة للفرد والمجتمع، يقررها القانون ويرسم حدودها ويحميها بالشكل الذي تسير به وظائف الحياة في الجسم على النحو الطبيعي، وأن يحتفظ بتكامله الجسدي ويتحرر من الألآم البدنية ويعد حق الإنسان في التكامل الجسدي من عناصر الحق في سلامة الجسم وهذا يعني أن تسير أعضاء الجسم سيرا طبيعيا في أداء وظائفها، وأن تبقى هذه الأعضاء كاملة غير منقوصة ، فجميع القوانين كانت قد حرمت أفعال الجرح، والضرب، وإعطاء مواد ضارة، التي من شأنها المساس بسلامة جسم إنسان، والنيل من ذلك والقصد من ذلك هو حماية جسم الإنسان، بمعنى أن التكامل الجسدي هو الحفاظ على سلامة الجسم، بأن يحتفظ الشخص بمادة جسمه كاملة غير منقوصة وإن أي فعل أو تصرف يؤدي إلى انتقاص من سلامته يُعد مساساً بالحق في سلامة الجسم[2].

وعلى ضوء ما تقدم فإن المساس بسلامة الجسم يكون على ثلاثة فروض، (أولاً): الإخلال بالسير الطبيعي لوظائف الجسم، وهو ما نعني به هبوط المستوى الصحي للمجنى عليه. (ثانيا): المساس بمادة الجسم سواء بالإنتقاص أو أحداث أي تغيير فيها مثل الاستئصال، (ثالثا): الإيلام البدني، ويتحقق هذا الأمر عندما يلحق المجني عليه من آذى في شعوره بالارتياح ولو لم يصل إلى حد جسيم، مثال ذلك ما ينشأ من صفع المجنى عليه أو دفعه أرضاً. وعلى ذلك فحق الإنسان في سلامة جسمه ينهض على ثلاثة عناصر العنصر النصر الأول: الحق في أن تظل أعضاء الجسم تؤدي وظائفها على نحو طبيعي.

---

(1) - ينظر - د. محروس نصار الهيتي ، المصدر السابق، ص 34و 35 .

(2) - زهير خريبط خلف، الحماية الجزائية لسلامة الجسد في ضوء الاعمال الطبية الحديثة، أطروحة دكتوراه، الجامعة الاسلامية في لبنان، كلية الحقوق والعلوم السياسية، 2018، ص 20 .

أما العنصر الثاني: الحق في الاحتفاظ بكل أعضاء الجسم كاملة غير منقوصة فكل فعل يؤدي إلى الانتقاص من هذه الأعضاء كالبتر، يُعد مساساً بسلامة الجسم، ويستوي في هذا الإعتداء كونه قد ترك أثرا في جسم المجني عليه. ثالثا: الحق في التحرر من الآلام البدنية وتتحقق هذه الآلام بما يلحق الشخص من إيذاء في شعوره بالارتياح والسكينة[1].

أما المشرع العراقي فقد جرائم الافعال التي تمس السلامة البدنية في قانون العقوبات رقم (111) لسنة 1969 ، ضمن عنوان الجرائم الواقعة على الاشخاص الباب الاول، الفصل الثاني المادتين (410 و 411) عقوبات، بعنوان (الضرب المفضي إلى الموت والقتل خطأ)، وخصص المواد (412 ولغاية 416) الفصل الثالث بعنوان (الجرح والضرب والايذاء العمد)، ويرى جانب من الفقه أن المشرع العراقي لم يكن دقيقاً عندما أورد لفظ الإيذاء العمد لأنه قد حشره بين هذه الجرائم التي ميزها بالجرائم العمدية جريمة الإيذاء الخطأ في المادة (416)، وفي ذلك تناقض واضح لكون العنوان لا يتفق مع المحتوى، وهذا الشيء معيب للمشرع الذي يجب أن يكون حريصاً على الدقة، ويبتعد عن التداخل والتناقض في وصف الجرائم والمواد، وكان الأجدر بالمشرع أن يفرد فصلا لجريمة الايذاء الخطأ[2].

ونحن نشاطر هذا الرأي، فكان الأجدر بالمشرع العراقي أن يكون أكثر دقة في توزيع المواد وتصنيفها، ويكون كالاتي: يكون عنوان الفصل الثاني من الباب الاول هو (الايذاء المفضي إلى الموت والقتل خطأ) بدلا من (الضرب المفضي إلى الموت والقتل الخطأ)، لكون تسمية الايذاء تكون اكثر شمولا من الضرب، ويكون عنوان الفصل الثالث من الباب نفسه بعنوان (الإعتداء بالضرب والجرح والايذاء العمد) بدلا من (الجرح والضرب والإيذاء العمد)، لكون فعل الإعتداء اوسع من حصر وصف الضرب والجرح والإيذاء العمد، فقد يكون فعل الاعتداء بطريقة غير الفعل المادي، كالضرب والجرح والايذاء البدني، ولكي تسهل عملية إسناد المواد القانونية على الواقعة الجرمية والمتهم من قبل قاضي المحكمة.

الفرع الثالث

حق الانسان في السلامة الجسدية في قانون أصول المحاكمات الجزائية

يتميز قانون الإجراءات بطابع تنظيمي للحقوق والحريات في جميع مراحل الإتهام والإستجواب للمتهم، فقانون الإجراءات يمتاز بكونه يقيد حق السلطة العامة في الدولة بتوجيه العقاب والمساس

(1) - محروس نصار الهيتي، المصدر السابق، ص 20 و 21 .
- وكذلك : د. محمد عبدالظاهر موسى، المصدر السابق، ص 13 وما بعدها.
(2) - د. ضياء عبدالله عبود جابر الاسدي، المصدر السابق ، ص 205 . وكذلك : زهير خريبط خلف، الحماية الجزائية لسلامة الجسد في ضوء الاعمال الطبية الحديثة، المصدر السابق، 187.

بسلامة الجسم، من جميع الممارسات التي تمس كرامة الإنسان وتعرض تكامله الجسدي للخطر، فقانون الإجراءات ليس مجرد وسائل تهدف إلى كشف الحقيقة وانما هي مجموعة قواعد تستهدف ضمان الحماية المقررة للمتهم وجميع أطراف الدعوى، وضمان الحفاظ على كرامة وحقوق المتهم، ولهذا فأن الإجراءات الجنائية ليس فقط تطبيق لسير أحكام القضاء، بل هي أعمال تمس الحرية الشخصية وغيرها من الحقوق والحريات عند مباشرتها في مواجهة المتهم في الإجراءات الجنائية بكل ما تحمله من معاني الاتهام والتحقيق والمحاكمة وكل ما يساعد على جمع الأدلة لكشف الحقيقة. وعلى ضوء ذلك يُعّد قانون الإجراءات الجنائية من القوانين المنظمة للحقوق والحريات التي تخص المتهم وطرفي الدعوى بشكل عام، ولذلك نقول أن هذا القانون يتعرض لازمة شديدة كلما تعرضت الحريات في الدولة لازمات، وهذا خلاف الحال في النظم الديمقراطية التي تكون فيها السلطة للشعب قولاً وفعلاً، فإن قانون الإجراءات الجنائية يجب أن يكون وسيلة لتحقيق العدالة الجنائية القائمة على التوازن بين الحقوق والحريات ومصلحة الدولة وهو ما يتطلب في هذا القانون أن يضمن كافة الحقوق والحريات مما يقتضي ضمان حقوق الدفاع وتوفير المحاكمة المنصفة. وهذه جميعها تعد ضمانات تمس السلامة الجسدية والتكامل جسدي، بمعنى أن لا تكون هذه الإجراءات أثناء التحقيق وغيرها وسيلة للإعتداء على الحق أو حرية، أو سلامة جسد المتهم، وهو ما يستلزم تشريع قوانين تجرم وتعاقب اي مساس بسلامة جسم المتهم[1].

فالقوانين الإجرائية هي مجموعة قواعد قانونية، وتتميز عن غيرها من القواعد التي تحكم نشاط الأفراد بعنصر الجزاء، فلا يمكن تصور قوة الإلزام لأي قاعدة قانونية دون عنصر الجزاء، وإلا فإن القاعدة تصبح مجرد نصح، أو إرشاد، وعلى ضوء ذلك فإن قواعد قانون الإجراءات الجنائية تتميز عن قواعد القانون الموضوعي بأنها تتضمن جزاء ذا طبيعة خاصة، هو الجزاء الإجرائي بالإضافة إلى غيره من أنواع الجزاءات الأخرى. ولهذا فإن قانون الإجراءات الجنائية يهدف إلى ضمان حسن إدارة العدالة الجنائية واحترام حقوق المتهم وسلامة جسمه، فضلا عن ضمان احترام الشرعية الاجرائية إعمالا لسيادة القانون[2].

و تتجلي أهمية هذه الإجراءات في أنها تؤدي إلى تكوين الدليل الجنائي، سواء كان ضد المتهم، أو لصالحه، وعلى ضوء ذلك فإن قانون الإجراءات الجنائية يُعد من أهم الضمانات الإجرائية لسلامة

(1) - د. احمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، الطبعة العاشرة، دار النهضة العربية، 2016، ص37.

(2) - د. محمد عبدالظاهر موسى، المصدر السابق، ص 28.

جسم الإنسان أثناء مرحلة التحقيق أو المحاكمة، وضمان سلامة جسده من التعذيب، وهذا الحق هو من المبادئ الدستورية والتي لا يمكن المساس بها[1].

ونجد أن قانون الإجراءات الجنائية القطري رقم (23) لسنة 2004 تضمن نصوصا لضمان حماية حق الإنسان في السلامة الجسدية، وذلك من خلال النص على عدد من الأحكام التي تضمن حماية المتهم من التعرض للمعاملة اللاإنسانية والتعذيب، من خلال العديد من الأساليب التقليدية، أو التي تستخدم بواسطة التكنولوجيا الحديثة، فقد نص القانون على عدم اخذ أي أقوال يثبت أنها صدرت نتيجة التعذيب أو الإكراه أو التهديد، إذ نصت المادة (232) على أنه: "يحكم القاضي في الدعوى حسب العقيدة التي تتكون لديه بكامل حريته، ومع ذلك لا يجوز له أن يبني حكمه على أي دليل لم يطرح أمامه في الجلسة، أو تم التوصل إليه بطريقة غير مشروعة . وكل قول يثبت أنه صدر من أحد المتهمين أو الشهود تحت وطأة الكره أو تهديد لا يعول عليه". ونجد كذلك قد تضمنت المادة (40) من قانون الإجراءات الجنائية القطري نص صريح في وجوب معاملة المحبوس بما يحفظ كرامته وعدم ايذائه، بدنياً ومعنوياً، إذ نصت على أنه: لا يجوز القبض على أي شخص أو حبسه إلا بأمر من السلطات المختصة بذلك، وفي الأحوال المقررة قانونا، كما يجب معاملته بما يحفظ كرامة الإنسان، ولا يجوز ايذائه بدنيا ومعنويا. ويجب على مأمور الضبط القضائي أن ينبه المتهم إلى حقه في الصمت وفي الاتصال بمن يرى". وقد نصت على ذلك أيضا عدد من التشريعات الأخرى مثل التشريع العماني رقم (97) لسنة 1999 وايضا قانون الإجراءات الجزائية في المادة (41) التي تنص على أنه: " لا يجوز القبض على أي إنسان أو حبسه إلاّ بأمر من السلطة المختصة بذلك قانونا، ويجب معاملة المقبوض عليه بما يحفظ عليه كرامته، ويحظر على مأموري الضبط القضائي وأي شخص ذي سلطة عامه أن يلجأ إلى التعذيب أو الاكراه أو الاغراء أو المعاملة الماسة بالكرامة للحصول على أي أقوال أو منع الأدلاء بها أثناء جمع الاستدلالات أو التحقيق الابتدائي أو المحكمة[2].

وأخذ المشرع المصري بالاتجاه ذاته في المادة (302) من قانون الإجراءات الجنائية، والتي تنصت على أنه: "يحكم القاضي في الدعوى حسب العقيدة التي تكون لديه بكامل حريته مع ذلك لا يجوز له أن يبني حكمه على أي دليل لم يطرح امامه في الجلسة. وكل قول يثبت انه صدر من أحد المتهمين أو الشهود تحت وطأة الاكراه أو التهديد به يهدر ولا يعول عليه". ونلاحظ أن كلا النصين السابقين يتوافقان مع المادة (15) من إتفاقية مناهضة التعذيب التي تنص على أنه: " يجب على كل دولة طرف في الاتفاقية أن تضمن عدم الاستشهاد بآية اقوال يثبت أنه تم الأدلاء بها نتيجة للتعذيب كدليل في أية

(1) - د. احمد فتحي سرور، المصدر السابق، ص 619.
(2) - فاطمة عبدالله علي ، المصدر السابق، ص 67و68.

إجراءات[1]، باستثناء إذا كان ذلك ضد شخص متهم بارتكاب التعذيب كدليل على الادلاء بهذه الاقوال[2].

وعلى أساس ذلك لا يكفي أن يقع على عاتق قانون العقوبات ضمان حق الحياة، بل لا بد أن يضمن أيضاً الحق في ممارسة هذه الحياة، فالمصلحة التي يحميها قانون العقوبات في جرائم القتل هي مصلحة حق الحياة، أم المصلحة التي يحميها في جرائم الإيذاء والجرح وإعطاء المواد الضارة فهي مصلحة حق الإنسان في التكامل الجسدي، أما قانون الإجراءات أو أصول المحاكمات الجزائية، فهو قانون يضمن سلامة جسم المتهم أثناء التحقيق ويترتب على هذا ضمانات للمتهم في أن يعامل المتهم بكل أحترام وكرامة، وعدم المساس بسلامة جسده سواء بالتعذيب أو غيرها، وذلك من خلال عدم المساس بجسم الإنسان وجميع أعضاء الداخلية أو الخارجية، وعلى ذلك فإن أي عدوان على جسم الإنسان من شأنه أن يضعف من قدراتها في أداء وظائفها، وهذا الإعتداء جرمه القانون وجميع الشرائع السماوية[3].

وعلى ضوء ما تقدم فإن الحرية الشخصية للإفراد هي الأساس في حقوق الإنسان وشرط لازم لاحتفاظ الفرد بوجوده وقيمته الإنسانية، إلاّ أن هذا قد يتعارض مع متطلبات المجتمع في البقاء في ظل التطور التكنولوجي الذي يعيشه العالم الآن، فالدولة عن طريق موظفي السلطة العامة قد تنتهك حقاً مشروعاً من هذه الحقوق، ومنها حق الإنسان في التحرر من الإلام، خصوصا إذا ما أسيء إستخدام هذه السلطة، من قبل القائمين عليها و خاصة وضع المجنى عليه أثناء التحقيق أو عند قيام الموظف العام بإلقاء القبض على أحد المتهمين أو التحقيق معه، وهذا ما يحدث عن طريق موظفي السلطة العامة، إذ ينتهك المكلف بخدمة عامة (الموظفين) حق من هذه الحقوق عند إستعمال القسوة مع أحد الأشخاص، استغلال لوظيفته، إذ جاء بنص المادة (332) من قانون العقوبات العراقي رقم (111) لسنة 1969، على أنه: (يعاقب بالحبس مدة لا تزيد على سنة وغرامة لا تزيد على مائة دينار أو بإحدى هاتين العقوبتين كل موظف أو مكلف بخدمة عامة استعمل القسوة مع أحد من الناس إعتماداً على وظيفته فأخل بإعتباره وشرفه أو أحدث الماً ببدنه وذلك دون الاخلال بأية عقوبة أشد ينص عليها القانون). وايضا جاء بنص المادة (333) من قانون العقوبات على انه: (يعاقب بالسجن أو الحبس كل موظف أو مكلف بخدمة عامة عذب أو أمر بتعذيب متهم أو شاهد أو خبير لحملة على الاعتراف بالجريمة أو

(1) - د. احسن بو سقيعة، الوجيز في شرح القانون الجزائي الخاص، المصدر السابق، ص 59.
(2) - د. محمد عبدالظاهر موسى، المصدر السابق، ص 29 .
(3) - د. محروس نصار الهيتي، المصدر السابق، ص 5.

للإدلاء بأقوال ومعلومات بشأنها أو لكتمان أمر من الأمور أو لإعطاء رأي معين بشأنها، ويكون بحكم التعذيب استعمال القوة والتهديد)[1].

وبناء على ما تقدم يمكن القول بأن القوانين الجنائية هي قوانين الحريات العامة يضمنها ويحميها ضمن حدود، فلا ملاحقة ولا تجريم ولا حجز ولا عقاب إلا إذا حصل خرق لنص قانوني، ولذا فإن المجتمع يبقى بمأمن من تدخل السلطة العامة في حياته الخاصة وسلامة جسده[2]، وهذا ما ترجمه لنا قانون أصول المحاكمات الجزائية العراقي رقم (23) لسنة 1971 ، في المادة (108) إذ خول ألقائم بالقبض استخدام القدر اللازم من العنف مع الحالات التي توحي بخطورة المتهم وذلك بقولها: (على كل فرد من أفراد الشرطة أو عضو من أعضاء الضبط القضائي أن يقبض على أي من الأشخاص الاتي بيانهم:

1- كل شخص صدر أمر بإلقاء القبض عليه من جهة مختصة .
2- كل من كان يحمل السلاح ظاهراً أو مخبئاً خلافاً لأحكام القانون.
3- كل شخص ظن لأسباب معقوله أنه إرتكب جناية أو جنحة عمدية ولم يكن له محل إقامة معين.
4- كل من تعرض لأحد أعضاء الضبط القضائي أي مكلف بخدمة عامة في أداء واجبه.

أما المادة (102) من القانون ذاته فقد خول كل شخص إلقاء القبض على مجموعة من المتهمين بجناية أو جنحة في حالات تحددها هذه المادة، وذلك عند غياب السلطة العامة عن محل الحادث . وهذا يستدعي قدر من العنف أثناء القبض، وذلك بقولها (أ- لكل شخص ولو بغير امر من السلطة المختصة ان يقبض على أي متهم بجناية أو جنحة في إحدى الحالات الاتية:

1- إذا كانت الجريمة مشهودة.
2- اذا كان قد فر بعد القبض عليه.
3- إذا كان قد حكم عليه غيابيا بعقوبة مقيدة للحرية.

ب- لكل شخص ولو بغير أمر من السلطة المختصة أن يقبض على كل من وجد في محل عام في حالة سكر بين .....)[3].

وإن مثل هذه العبارات والنصوص المرنة يمكن تفسيرها حسب وجهة نظر المسؤول في المركز الذي يستطيع أن يتحجج بمثل هذه الأمور ليتولى التحقيق بنفسه، وأن هذا الأمر قد يؤدي إلى إتخاذ إجراءات تمثل مساساً بسلامة جسم المتهم، أثناء القبض عليه، وأخذ عينة من دمه أو شعره أو اظافره، ثم يتبين بعد ذلك عدم صحة إعتقاد المسؤول في مركز الشرطة لمجرد إعتقاده ان ضرراً قد يلحق التحقيق أو

(1) – ينظر: المادة (332 و 333) من قانون اصول المحاكمات الجزائية العراقي رقم 23 لسنة 1971 .
(2) - ينظر: د. محروس نصار ، المصدر السابق، ص 90 و 91.
(3) - المادة (102) من قانون اصول المحاكمات الجزائية العراقي رقم 23 لسنة 1971 المعدل.

إحتمال هرب المتهم، وعلى ضوء ذلك يجب الإشارة إلى أنه نظام القاضي الخفر مطبق حالياً في جميع أنحاء البلد، ولذا وخوفاً من خرق الضمانات المقررة للمتهم. وهناك جانب من الفقه يدعو إلى تعيين مجموعة من المحققين المختصين في مراكز الشرطة وفتح باب الدورات الخاصة من أجل ضمان الحماية المقررة لسلامة جسم المتهم من التعذيب بالإضافة إلى تحديد مدة زمنية يلزم فيها المسؤول في مركز الشرطة بتقديم الاوراق التحقيقية إلى قاضي التحقيق أو المحقق ويفضل أن تكون هذه المدة خلال (48) ساعة [1].

ويرى الباحث أنه من الضروري عدم الأخذ بأي أقوال للمتهم في حال تعرض لأي أنواع التعذيب أو الإكراه أو الضغط النفسي، لكون جميع هذه الأفعال تدخل في نطاق المساس بسلامة الجسم، ويترتب على ذلك بطلان جميع الإجراءات والأحكام والأدلة التي إستندت على أقوال المتهم بعد إعترافه بسبب التعذيب الذي تعرض له، ويجب أن يتم إستجواب المتهم بحضور محام له، وعلى أساس ذلك يتوجب على المشرع الجنائي أن يلتفت لهذا الأمر الذي يشكل خطراً على سلامة الجسم والكرامة التي يتمتع بها الإنسان بحكم الحقوق الدستورية.

المطلب الثاني

اثر التطور التكنولوجي على حق الانسان في سلامة جسده

أن التطور التكنولوجي له آثار قد تنعكس على تصوراتنا الفكرية بمعنى أن التطور التكنولوجي وما ينتج عنه من تقنيات لم تعد مجرد أدوات أو ملحقات ثانوية في حياتنا بل أصبحت الأساس المعتمد عليه في أغلب تفاصيل حياتنا اليومية، ولا شك أن التقدم الملحوظ في المزايا التقنية للأجهزة الإلكترونية تساعد على منح الاشخاص أفضل مستوى من الخدمات الإلكترونية التي لا غنى عنها في حياتنا في شتى مجالات الحياة، والسبب يعود لارتباط هذه التكنولوجيا الحديثة بأصغر الإنجازات اليومية في حياة الفرد. وعلى ضوء ذلك سنقسم دراستنا لهذا الموضوع على فرعين، نتناول بحث آثر التكنولوجيا على حق الانسان في سلامة جسده في الفرع الاول، أما الفرع الثاني سيكون لدراسة دور السياسة الجنائية لحماية الانسان في السلامة الجسدية في ظل التطور التكنولوجي.

(1) - د. ضياء عبدالله عبود الأسدي ، المصدر السابق، ص 107.

الفرع الأول

الأثر السلبي للتكنولوجيا على حق الانسان في سلامة جسده

إن من أهم الآثار التي تؤثر على سلامة جسم الإنسان وصحته بسبب الاستعمال السلبي للتطور التكنولوجي هو مساهمة التكنولوجيا الحديثة في إنتشار العنف في المجتمع، وذلك نظرا لوجود العديد من برامج ومحتوى العنف فيها وأيضا التحريض على القتل وإنتشار الجريمة المنظمة، وكذلك نجد دوراً كبيراً للألعاب القتالية والأفلام العنيفة وغيرها من البرامج والتطبيقات الالكترونية التي يستطيع الفرد الحصول عليها بكل سهولة من خلال تقنيات تكنولوجية حديثة، الأمر الذي يؤثر سلبا على سلوك الإنسان وخاصة الأطفال[1]، وكذلك جعلت التكنولوجيا الحديثة وخاصة الهاتف المحمول العديد من الناس يعيشون في عزلة تامة بين جدران صفحات التواصل الاجتماعي إذ يعيش الفرد في عالم أفتراضي بكل ما تحمله هذه الكلمة من معنى بالإضافة إلى ذلك تلعب التكنولوجيا الحديثة دوراً كبيراً في تعطيل القدرات العقلية للإنسان وذلك نظراً لإعتماد الإنسان على أدوات تكنولوجيا الحاسوب والهاتف المحمول وإجراء العمليات الحسابية وتخزين البيانات الأمر الذي ادى إلى تقليل استخدام العقل والذاكرة، وضعف قدراته العقلية وقد أسهمت التكنولوجيا الحديثة بتعويد الإنسان على الكسل بالإعتماد على هذه الاجهزة الدقيقة والمتطورة، إذ أصبح الشخص يحصل أي معلومة جديدة بمجرد الدخول إلى الإنترنت دون أن يبذل أي جهد[2]. فالتقدم التكنولوجي يعد تحدياً لأن مسألة قبول أو رفض التقنية الجديدة لم يعد خياراً متاحاً، بل أصبح مسألة وعي اجتماعي، ونلاحظ مؤخرا هناك دراسة احصائية لمؤسسة (جارتنر) وهي مؤسسة أبحاث وإستشارات عالمية، مقرها في مدينة ستانفورد الأمريكية، تقدم المعلومات والمشورة والادوات في مجال التكنولوجيا والمعلومات. وقد أجرت هذه المؤسسة دراسات وبحوث في مجال التقنية التكنولوجية العالمية تقريرا سنويا يعرض التنبؤات المستقبلية، ووجدوا زيادة أعداد أجهزة التواصل الإلكتروني الحديث اذ تشير الدراسات أن عدد الأجهزة الذكية المستخدمة والمتصلة بشبكات الإنترنت قد يصل إلى (8,4) مليار في عام 2017 ، أما في عام 2020 فقد يرتفع عدد مستخدمي الاجهزة الذكية لما يقارب (4,20) مليار، لا شك أن هذا الإرتفاع الواضح في معدلات الإستخدام يُعد عاملا محوريا في تغيير معالم حياتنا ليس فقط على العالم المادي الملموس، بل على

---

(1) - د. سلام سميرة، د. سلام محمد أمين، التكنولوجيا الرقمية وتأثيرها على السلامة الجسدية والعقلية للطفل، بحث مقدم، ضمن اعمال المؤتمر الدولي الافتراضي، بعنوان، انعكاسات التطور التكنولوجي على حق الانسان في السلامة الجسدية ، برلين - المانيا ، 2021 ، ص 96.

(2) - د. مشنف أحمد، د. قايد حفيظة، بحث منشور (دراسة تحليلية لتأثير التقدم التكنولوجي على سلامة الانسان)، كتاب صدر عن المؤتمر الدولي الافتراضي ، بعنوان (انعكاسات التطور التكنولوجي على حق الانسان في السلامة الجسدية ، برلين - المانيا ، 2021 ، ص 150.

طريقة تشكيل تفكيرنا وإدراكنا المعرفي والحسي، للقضايا المختلفة، وذلك نتيجة التقدم التكنولوجي الذي يُعّد تحدياً ولم يعد خياراً متاحاً وإنما أصبح مسألة وعي إجتماعي يجب تقبله بكل مزاياه وآثاره[1].

ولقد أهتم الإعلان العالمي لحقوق الإنسان في سلامة الجسد، إذ جاء في مضمونه على أنه لكل فرد الحق في الحياة وسلامته الشخصية، كما أهتمت الإتفاقية الدولية للحقوق السياسية والمدنية بالحق في سلامة الجسد وتضمنت المادة (السابعة) على أنه: لا يجوز إخضاع أحد للتعذيب ولا للمعاملة القاسية التي تمس الكرامة، وعلى وجه الخصوص لا يجوز إجراء تجربة طبية أو علمية على إحد دون رضاه. كما عالجت الإتفاقية الإقليمية هذا الحق بنص الإتفاقية الأوروبية لحقوق الإنسان في المادة (3) على أنه: "لا يجوز إخضاع أي إنسان للتعذيب". كما تضمنه أيضا الميثاق الأفريقي لحقوق الإنسان والشعوب في المادة (4): " لا يجوز إنتهاك حرمة الإنسان، ومن حقه أحترام حياته وسلامة شخصه البدنية والمعنوية ولا يجوز حرمانه من هذا الحق تعسف". وأن إنتهاك هذا الحق لا يكون فقط بإستعمال القوة وتعذيب الأشخاص قبل السلطة في الدولة أو العدو، من خلال التعذيب البدني والصعق الكهربائي، والجلد، الوخز بالإبر، والأشواك، والحرمان من الأكل والتعذيب بالمياه، بل يشمل اليوم التعذيب إنتهاك حرمة الجسد بإدخال مواد سامة للجسم بقصد التعذيب أو الإضرار وخاصة الإشعاعات النووية، أو تعريض الأشخاص له والأضرار بهم، وإن ما يؤكد هذا هو تلك الأضرار والآثار التي يخلفها هذا الإشعاع، وما ينتج عنه من آثار خطرة[2].

وأيضا ما تضمنته اتفاقية بودابست (2001/11/23) حول مكافحة الإجرام المعلوماتي في مدينة بودابست عاصمة دولة المجر، والتي ضمت (26) دولة من أعضاء الاتحاد الاوروبي، وبعض الدول خارج الاتحاد، مثل الولايات المتحدة الامريكية واليابان وكندا وجنوب افريقيا ، وتُعد هذه الإتفاقية من أهم الإتفاقيات التي تطرقت إلى ضرورة أتخاذ التدابير التشريعية والتنظيمية لمتابعة وكشف الجرائم الإلكترونية والمعلوماتية، وتوفير قوانين ملائمة للبحث والتحري والتحقيق والمحاكمة، وبذل الجهود من أجل التعاون الدولي [3].

---

(1) - د. سكوتي خالد، (التهديد التكنولوجي على حق الانسان في سلامة جسده)، ورقة عمل مقدمة، ضمن اعمال المؤتمر الدولي الافتراضي ، بعنوان (انعكاسات التطور التكنولوجي على حق الانسان في السلامة الجسدية ، برلين - المانيا ، 2021 ، ص 87.

(2) - د. أسود ياسين، (حق الانسان في الحياة وسلامة الجسد والحق في بيئة نظيفة)، بحث منشور، ضمن اعمال المؤتمر الدولي الافتراضي، بعنوان (انعكاسات التطور التكنولوجي على حق الانسان في السلامة الجسدية)، برلين - المانيا ، 2021 ، ص 19و20.

(3) - فايز محمد راجح غلاب، الجرائم المعلوماتية في القانون الجزائري واليمني، اطروحة دكتوراه، جامعة الجزائر، كلية الحقوق، 2010، ص 420.

ومن الآثار السلبية التي تنتج عن التطور التكنولوجي هو وجود النفايات الإلكترونية، والتي تشكل خطراً على حياة الإنسان لأنها تحتوي على مواد سامة وخطيرة يفوق عددها أكثر من الف نوع من العناصر الكيميائية، مثل المعادن الثقيلة والمواد البلاستيكية والغازات وغيرها من المواد الأخرى. فالتعامل مع هذه النفايات بطريقة عشوائية وغير علمية من شأنه أن يؤدي إلى الوفاة أو الأذى في السلامة الجسدية، مثال على ذلك وهو التعامل مع مادة (الكادميوم)، إذ يسبب ضرراً بالجهاز العصبي للإنسان وخلق تشوهات جينية، وأحداث الاجهاض للحوامل، كما أن التعامل مع مادة (البيريليوم)، من شأنه أن يسبب سرطان الرئة عند إستنشاق الأبخرة والغبار الصادر منه، كما يؤدي إلى تسمم الجسم ثم الوفاة. وإن النفايات الإلكترونية تحتوي على مادة الرصاص الذي يسبب خللاً في النشاط المعرفي واللفظي للفرد، ويؤدي في بعض الأحيان إلى الغيبوبة ثم الموت. وكذلك فأن خطورة التعرض الدائم للمكونات الخطرة للنفايات الإلكترونية، أو الناتجة عن إحراقها، أو طمرها في التربة قد يؤدي إلى الإصابة بأمراض خطيرة تتفاقم ببطء، وتؤدي إلى الوفاة. وبذلك فإنه خطورة النفايات الإلكترونية على حياة الإنسان تزداد بحسب المكونات التي تدخل في تصنيعها أو بعض أجزائها، فقد تكون مواد مسرطنة تؤدي إلى الوفاة، أو سامة وقاتلة بمجرد التعامل معها[1].

ويمكن القول إن تجريم بعض الأفعال في ظل العولمة والتطور التكنولوجي أصبح محل أهتمام جميع الفقهاء والباحثين في القانون والهدف هو لحماية المجتمع، أما تأثيرات العولمة، فلم يعد أحد بمنأى عنها، إذ وصل الأمر بالتعامل مع التكنولوجيا الحديثة سواء بالأجهزة الإلكترونية أو عن طريق شبكات الإنترنت، فأصبحت أغلب الشعوب تتعامل في حياتهم اليومية وأوضاعهم المعيشية وقيمهم الإجتماعية ترتبط بإستخدام التكنولوجيا الحديثة، فهي اليوم ترتبط بما يرونه يسمعونه في وسائل الإعلام وبرامج التواصل الاجتماعي أغلب الأوقات والإمكنة، وعلى اساس ذلك نجد من البديهي أن تتأثر السياسة الجنائية لكل دولة، تأثيراً واضحاً من أجل مواكبة الجرائم التي تنشأ عن الإستخدام السلبي للتطور التكنولوجي، من أجل حماية أمن الافراد وممتلكاتهم وحياتهم الخاصة[2].

---

(1) - خميخم محمد ، (تأثير التطور التكنولوجي على التمتع بالحق في الصحة والحياة- النفايات الالكترونية نموذجا)، بحث منشور، ضمن المؤتمر الدولي الافتراضي، بعنوان (إنعكاسات التطور التكنولوجي على حق الانسان في السلامة الجسدية)، برلين - المانيا ، 2021 ، ص 38.

وكذلك ينظر: حامد احمد مال. العولمة في ظل التطور التقني واثارها في مستقبل الوطن العربي، اطروحة دكتوراه، جامعة سانت كليمنتس، قسم العلوم السياسية، 2009، ص 196.

(2) - بن زرفة هوارية، العولمة وتأثيرها على الجريمة والعقاب، بحث منشور، مجلة المعيار، المركز الجامعي بجامعة تيسمسيلت، الجزائر ، مجلد 25، العدد 56، 2021، ص 547.

الفرع الثاني

دور السياسة الجنائية لحماية الانسان في ظل التطور التكنولوجي

لاحظنا كيف أثرت التكنولوجيا الحديثة على سلامة الجسد من خلال العديد من الافعال التي لها الاثر السلبي على سلامة الجسد والتي تتمثل بالتعذيب بواسطة الأجهزة التقنية الحديثة أو تأثرها بالإشعاعات النووية، أو إجراء عمليات التجارب العلمية والعمليات الجراحية ومنها عمليات التجميل بواسطة الأجهزة الإلكترونية الحديثة، أو بسبب وجود النفايات الإلكترونية وما لها من تأثير خطير جدا على تلوث البيئة وما تسببه من أمراض سرطانية وغيرها تؤثر على سلامة الجسد، وهذا الأمر يتطلب وضع ضوابط قانونية وتشريع ينظم عمليات التجميل، إذ نرى كيف دخل جسم الإنسان في مجال التعامل القانوني من خلال عمليات التجميل، ولاحظنا كيفك كانت النظرة القانونية المتشددة في بادئ الأمر لتلك العمليات، ثم تدرج ذلك الموقف إلى أن وصل أخيراً إلى مرحلة الإباحة والاعتراف بضرورة تقرير مشروعيتها، نظراً لما لهذا النوع من الجراحة من دور مهم في إنقاذ العديد من الأثار النفسية السيئة، كادت أن تؤثر بالسلب على حياة بعض الافراد الشخصية والعملية، فتأتي تلك العمليات لتعيد إلى نفوس الثقة والامل في إمكانية اندماجهم في المجتمع مرة أخرى، وذلك من خلال إستعدادهم للإنخراط في الحياة العملية، أو إيجاد فرصة الإرتباط بشركاء جدد لحياتهم بعد أن كانوا شبه منبوذين في مجتمعاتهم بسبب عاهة خلقية ولدوا بها، أو تشوه طرأ على حياتهم فيما بعد لأي سبب كان، ولذا إذا كان مبدأ مشروعية استخدام الاجهزة التقنية الحديثة سواء الخاصة بشبكات الإتصال أو التي تدخل ضمن العمليات الجراحية أو التجميل قد إستقر، فإنه يلزم لاستخدام هذه المشروعية ، توافر ضوابط معين لممارسة هذا النوع من العمليات وهذه الضوابط هي : أ- ضرورة الإلتزام بتبصير المريض ب- ضرورة الحصول على رضا المريض المستنير ج- ضرورة رجحان الفوائد المتوقعة من عمليات التجميل على المخاطر الناتجة عنها[1].

إذ أصبح جسم الإنسان بفعل الممارسات الطبية الحديثة والوسائل التكنولوجية الحديثة عرضة للمخاطر على حقه في الحياة، وتكامله الجسدي، وأصبح الأمر أشد خطورة و تأثيراً عندما تشكل هذه الممارسات خروجاً عن القواعد الشرعية والقانونية أحياناً والأخلاقية أحياًناً أخرى، فحياة الإنسان وصحته تُعد في مقدمات أهتمامات الإنسان، على مدى التاريخ ومن أولويات القوانين والمجتمعات كافة، ومن قبل الشرائع والأديان السماوية، وقد حقق الإنسان إنجازات عظيمة بفضل تطور العلوم الطبية والبيولوجية والتكنولوجية ولعل أبرز هذه الإنجازات العلمية المشهود لها بالتطور زماناً ومكاناً هو عمليات نقل وزرع الأعضاء البشرية، والتي تخطت حدود التجارب العلمية، والطبية، ودخلت منذ

(1) - حبيبه سيف سالم راشد ، (النظام القانوني لحماية جسم الانسان)، المصدر السابق، ص 158.

عهد ليس بالبعيد حيز العلاج الجراحي، وإذ أصبحت التكنولوجيا الحديثة وما نتج عنها سبباً في الكثير من تطور نجاح العمليات الجراحية التي تدخل في أعضاء جسم الإنسان ، وبعث بذلك الأمل في نفوس كثير من المرضى وجعلهم يأملون برغبه شديدة في الحصول على الأعضاء التي يحتاجون إليها للمحافظة على حياتهم وإنقاذها من الهلاك، سواء من متبرع حي، أو موصي بالتبرع بأحد أعضائه بعد الوفاة ، ولذا فالطب أعطى الأمل للكثير من الأشخاص الذين انقذت حياتهم بفضل ما تلقوه قطع غيار بشرية (اعضاء بشريه) من غيرهم[1].

ويرى الباحث من الضروري سد النقص التشريعي في قانون العقوبات العراقي رقم (111) لسنة 1969 أو تشريع قانون خاص يتضمن ضوابط وشروط إجراء عمليات التجميل، ونقل وزرع الاعضاء البشرية بواسطة الاجهزة التقنية الحديثة، وذلك لما يسببه هذا الامر من خسائر بشرية أو تشوهات، وما يسببه التطور التكنولوجي جراء إستعمال الأجهزة التقنية الحديثة التي تدخل في عمليات التجميل بكل أنواعها وعمليات نقل وزرع الأعضاء دون مراعاة للضوابط المهنية، فأننا نلاحظ في الوقت الحاضر مجموعة كبيرة ومتنوعة من الاجهزة التقنية الحديثة التي تستعمل وتدخل في مجال عمليات التجميل، والتنحيف، وقص المعدة، وتغيير لون البشرة، والجلد، ونقل الكلية، والمفاصل، والقلب، وتصنيع الفايروسات المعدلة والمعدية ....الخ.

أولا : دور السياسة الجنائية في التجريم

سياسة التجريم لها الدور الأهم والأبرز لضمان الحماية المقررة لسلامة الجسد من أي خطر قد يلحقه بسبب الأفعال المادية التقليدية أم على صعيد التطور التكنولوجي والتقني وما ينتج عنه من وسائل وادوات وأجهزة قد تسبب خطر يمس السلامة الجسدية للإنسان، من خلال تجريم جميع الأفعال التي تشكل خطراً على التكامل الجسدي، وهذا يعني أن السياسة الجنائية في التجريم يتمثل دورها في تشريع النصوص الجنائية المناسبة والكفيلة لتقرير الحماية من اي خطر قد يصيب السلامة الجسدية بسبب الإستعمال السلبي للأجهزة التكنولوجية والتقنية[2]، وقد لاحظنا أن أغلب الدول المتطورة في مجال إستخدام التكنولوجيا قد بادرت بالإسراع في تشريع مجموعة من القوانين الرادعة لتجريم اي فعل يمس السلامة الجسدية بواسطة الاجهزة التقنية الحديثة مهما كانت الطرق والأسباب، وهذا يعني لا بد من تفعيل دور السياسة الجنائية في مجال التجريم من خلال تشريع قوانين رادعة وناجعة لحماية سلامة

(1) - أحمد عمراني، حماية الجسم البشري في ظل الممارسات الطبية والعلمية الحديثة، اطروحة دكتوراه، جامعة وهران، كلية الحقوق، الجزائر، 2010، ص 163.

(2) - زروقي فايزة، بوراس عبدالقادر، السياسة الجنائية المعاصرة بين انسنة العقوبة وتطوير قواعد العدالة، بحث منشور، مجلة الحقوق والعلوم الانسانية، الجزائر، المجلد 14، العدد 3، 2021، ص 297.

الجسد من تأثير التطور التكنولوجي وما ينتج عنه من أجهزة متطورة قد تؤثر سلبا على سلامة الجسد[1].

وإن من أهم الضوابط القانونية التي تحكم التطورات والإنجازات التكنولوجية مع تزايد استخدام هذه التكنولوجيا، وبالمقابل هناك من يعاني من المجتمعات من الآثار الضارة وغير المرغوب بها في ظل هذا التطور التكنولوجي، هو الحاجة الماسة لضبط مسيرة التطور التكنولوجي بضوابط قانونية تضمن تحقيق المصالح العامة للمجتمعات الإنسانية وتدرئ أو تقلل من المفاسد والأخطار والآثار السلبية نتيجة الإستخدام السلبي لهذا التطور التكنولوجي في مختلف مجالات الحياة[2]، فإن الأمر يتطلب الحديث عن هذه الضوابط التي يمكن أن تستمد من القيم العليا للمجتمعات الإنسانية والمبادئ العامة للشرائع السماوية عامة والشريعة الإسلامية خاصة، والمناهج الدراسات العلمية التي تختص بهذا الأمر، ومن أبرز هذه الدراسات هي مراعاة مشروعية التطور التكنولوجي، ويقصد بالمشروعية أن تكون التكنولوجيا المنتجة بفكرتها وفلسفتها ووسائلها ومنتجاتها متفقة وأحكام مبادئ القانون، بالإضافة إلى الالتزام بأن يكون الاستخدام للتكنولوجيا ومنتجاتها موافقا للأحكام الموضوعة قانوناً، وكذلك من خلال تقديم الأولوية في عملية الإنتاج، إذ إن القانون يضع للتطور التكنولوجي المشروع أولويات من الواجب اتباعها في إدارة حركة النشاط التكنولوجي التي تبدأ بإنتاج الضروريات فالحاجيات، وهي مع ذلك لا تحارب التطور التكنولوجي في دائرة الترف المقبول، ما دام ذلك في حدود المسموح به قانوناً[3]. بالإضافة إلى ذلك يجب تحقيق المصلحة العامة من خلال إستخدام التكنولوجيا الحديثة ولتحقيق هذه المصلحة، يستلزم من حركة التطور التكنولوجي أن تنظم في سلك المصلحة العامة ذات الاعتبار القانوني، وبناء على ذلك فلا يتوقع من التكنولوجيا المطلوبة قانونا أن يترتب عنها مشكلة بيئية تسبب ضرراً للسلامة الجسدية، كما هو حاصل الآن في بعض صور التطور التكنولوجي، فإن كانت التكنولوجيا الحديثة كذلك فإنها تكون فاقدة لمشروعيتها، فعلى أساس ذلك يجب أن يكون التقدم التكنولوجي بكل التقنيات الحديثة وأدواتها المعاصرة أن يكون نافعا يستخدم لصالح البشرية لا الإضرار به، وما عدا ذلك فهو مجرم، وهنالك ضابط مهم لإستخدام التكنولوجيا الحديثة يجب ألا يترتب عليها ضرر يؤثر على المصلحة المرجوة، (لا ضرر ولا ضرار)، ويندرج تحت هذا الضابط امور يجب مراعاتها عند الإنتاج أو استخدام التكنولوجيا المعاصرة وهي عدم الإضرار بالإنسان

(1) - د. رزق سعد علي، انعكاسات التحول الرقمي على السياسة الجنائية المعاصرة، بحث منشور، مجلة الدراسات القانونية والاقتصادية، المجلد 7، العدد 2، 2021، ص 173.

(2) - د. منصور رحماني، الوجيز في القانون الجنائي العام، دار العلوم للنشر، الجزائر، 2006، ص 175.

(3) - د. عبدالفتاح بيومي حجازي، علم الجريمة والمجرم المعلوماتي، منشأة المعارف، الاسكندرية، الطبعة الاولى، 2009 ، ص 308.

وحقوق، ويقصد بذلك أن يكون مضمون التطور التكنولوجي ووسائله الحديثة ليس فيها إعتداء على حق من حقوق الإنسان، والتي من أهمها حقه في الحياة والسلامة الجسدية، وحقه في خصوصيته، وحقه في العمل[1].

ونجد أن كل من المشرع الاماراتي والمصري، قد حاولا أن يطبقا سياسة القوانين التقليدية على الجرائم الإلكترونية في بادئ الأمر على أعتبار الجرائم الالكترونية هي جرائم عادية وأنما ترتكب بوسائل حديثة، الاّ أن هذه السياسة قد سببت فراغاً تشريعياً لا بد من معالجته وقد سبب صعوبة مكافحة الجرائم الإلكترونية وأيضا واجهت القوانين التقليدية تصادماً مع مبدأ الشرعية الجنائية ومنهج تفسير القانون، لعدم وجود نص صريح يجرم بعض الافعال التي ترتكب بواسطة الأجهزة الإلكترونية أو بواسطة الإنترنت، وتُعد تعدياً على المصالح المعتبرة، مما أدى بالمشرعين الاماراتي والمصري إلى سن مجموعة قوانين خاصة لمكافحة الجرائم الإلكترونية، وظهر جليا مدى الحاجة إلى تطبيق سياسة جنائية حديثة لمواكبة ومكافحة الجرائم الإلكترونية وضرورة وجود تشريعات تضفي حماية لإستخدام الحكومة الإلكترونية، وعلى اثر هذا التطور التكنولوجي فقد تأثرت السياسة الجنائية من خلال توسع نطاق التجريم والعقاب، إذ اضطر المشرع للتدخل بتجريم صور سلوك تمثل مساسا بسلامة الجسد، والحياة الخاصة[2].

أما دور المشرع الجنائي الفرنسي في موضوع التجريم في ظل التطور التكنولوجي نجده قد أكد على ضرورة احترام جسم الإنسان وذلك بمقتضى التعديل على القانون رقم (94 - 653) الصادر عام 1992 إذ نص المشرع الفرنسي صراحة على أن " كل شخص له الحق في احترام جسده" ولكن جانب من الفقه يرى أن هذا النص معيب، لأن الشخص لا يمكنه أن يطالب بأحترام جسده إستقلالاً عن الشخص نفسه، فاحترام الجسد يتعلق بالشخص نفسه، ولذلك فأحترام جسد الإنسان يعتمد على عدة مبادئ أساسية، وهي مبدأ عدم جواز المساس بجسم الإنسان، ومبدأ عدم جواز التصرف في جسم الإنسان، ومبدأ عدم جواز التعامل المالي في جسم الإنسان، وقد نص المشرع الفرنسي أيضاً على مبدأ تكامل الجنس البشري في القانون الصادر عام 1992 والمضاف إلى المادة (16 -4) من التقنين المدني الفرنسي، ومن خلال هذه القوانين نلاحظ أن المشرع الفرنسي يحاول دائما مواكبة التطور الذي يعيشه المجتمع في ظل الواقع الذي يعيشه سواء على الصعيد الاجتماعي والتكنولوجي[3].

---

(1) - عفاف خذيري ، المصدر السابق، ص 133.

(2) - سعود علي عبدالله اللوغاني، السياسة الجنائية في مكافحة الجريمة الالكترونية، المصدر السابق، ص139 وما بعدها.

(3) - د. رزق سعد علي، المصدر السابق، ص 179.

ولقد كان من نتاج تطور الوسائل العلمية والتقنية الحديثة في العصر الحديث أن بعض التشريعات حرصت على توفير أكبر قدر ممكن من الحماية المدنية كانت أم الجنائية، ما يضمن صاحبه مواجهة أي إعتداء عليه بواسطة برامج التكنولوجيا الحديثة وغيرها، ولكن هذه الحماية تختلف بأختلاف التشريعات التي تأخذ بهذا المبدأ، فهي تتغير من زمان إلى زمان، ومن مكان إلى آخر ومن شخص إلى شخص[1].

ونجد ان المشرع العراقي قد تناول الجرائم الماسة بحياة الأنسان وسلامة بدنه، في المواد من (410 ولغاية المادة 416) من قانون العقوبات رقم (111) لسنة 1969 ، وهذا يعني أن المشرع العراقي قد أعطى أهمية بالغة لحماية السلامة الجسدية بعد أن خصص لها خمسة نصوص جنائية، وأيضاً من خلال إطلاعنا على مشروع تعديل قانون العقوبات، والمحال إلى مجلس النواب للتصويت عليه، لاحظنا ان اللجنة المختصة بتعديل القانون لم تراعِ وتنظر بجدية للتطور التكنولوجي ومدى إنعكاسه على السلامة الجسدية في ظل الاجهزة التقنية المستخدمة على جميع الأصعدة الطبية والتجميل والعسكرية والإتصالات، وكان من الضروري أن يتم تشريع نصوص قانونية تعالج هذا النقص، بوضع عبارة مكملة ضمن نص المادة (405) الخاصة بظروف التشديد أو ضمن المادة (406) من مشروع تعديل قانون العقوبات وهي: (.... أو من اعتدى بأي وسيلة كانت عادية أو تقنية أو بسبب عدم الأختصاص أو الإهمال) فلا يمكن الاعتماد على مثل هذه النصوص التقليدية، في ظل التطور التكنولوجي والتقني الذي يعيشه العالم الآن، فقد اوجد التطور التكنولوجي مجموعة كبيرة من الأجهزة التقنية، والتي لها الأثر المباشر على سلامة الجسد وقد تسبب له مخاطر جسيمة في حال تم استخدامهاً إستخداماً سلبياً من قبل الجناة، أو دون مراعاة للضوابط أو بسبب الإهمال، لذا كان على المشرع العراقي أن يواكب هذا التطور التقني وإصدار قانون خاص بالجرائم الإلكترونية والمعلوماتية[2].

وبناء على ما تقدم، فإننا ندعو المشرع العراقي إلى الأسراع بتشريع قانون خاص، يعالج النقص في قانون العقوبات العراقي رقم (111) لسنة 1969 المعدل، لكونه أصبح قانوناً تقليدياً، ولا يواكب التطور التكنولوجي والتقني والطبي الحاصل والذي يعيشه المجتمع بكل تفاصيل حياته، ويمكن أن يسمى هذا القانون بـ (قانون الجرائم المعلوماتية والإلكترونية والتقنية) يتضمن مجموعة من الفصول،

---

(1) - عاقلي فضيلة، المصدر السابق، ص 56

(2) - يجدر الإشارة إلى أن المشرع العراقي لم يشرع قانونا خاصاً بالجرائم الإلكترونية، ولكن يوجد مشروع قانون ولم يتم إقراره منذ عام 2011 ،إذ أن مشروع القانون الاخير، يتضمن ثلاثة محاور، المحور الأول: يتحدث عن الجرائم المعلوماتية، وأنواعه، اما المحور الثاني: فانه يتناول الجرائم المعلوماتية في التشريعات العراقية، والمحور الثالث: يتضمن وسائل سد الفراغ التشريعي وبالأخير يبقى مجرد مشروع قانون لم يتم المصادقة عليه لحد الآن.

من أجل الاحاطة بجميع الجرائم التي تدخل في ضمن إطار التطور التكنولوجي المعلوماتي والإنترنت. ويمكن تشريع مثل هذا القانون ويكون قانوناً ناجعاً، ذا محتوى وقائي ورادع، من خلال الأطلاع على القوانين في الدول المتقدمة في إستخدام التكنولوجيا ودراستها وكذلك الأخذ بنظر الإعتبار أختلاف القيم الإجتماعية والأخلاقية لكل بلد، من خلال دراسة علمية شاملة لكافة تفاصيل الحياة والمجتمع.

ثانيا : دور السياسة الجنائية في تشديد العقاب

إن أهم دور تلعبه السياسة العقابية للتعامل مع التهديد الناشئ عن التطور التكنولوجي هو الوقاية المتمثلة في تلافي إرتكاب أي فعل يمثل مساساً بالسلامة الجسدية أو بالمبادئ الأخلاقية والعلمية عند إستعمال هذه التكنولوجيا وما ينتج عنها من الأدوات والآلات عند التجارب والبحوث التقنية والطبية، التي تؤثر على سلامة الجسد، بمعنى أن السياسة العقابية هي سياسة علمية وعملية مكملة لسياسة التجريم[1]، وفيما يخص طبيعة التعامل مع الأجهزة التقنية الحديثة، لابد من الحصول على رخصة من الجهات الإدارية المعنية وإسنادها لأصحاب الاختصاص، وهذا يؤكد على ضرورة وجود رقابة إدارية، وأمنية، لمراقبة هذه التجارب ومدى ملائمتها للقواعد القانونية والأخلاقية، ومن المستحسن أن تكون هذه الهيئات مستقلة ومختلطة، تتشكل من قبل أعضاء من السلك الامني والطبي وأعضاء من مهن أخرى علمية وتقنية، من أجل تحقيق رقابة اجتماعية، وأيضا يتمثل دور السياسة العقابية من خلال الردع (الخاص والعام) والذي يتمثل بإيقاع العقاب لإصلاح الجاني، أو لردع أي شخص تسول له نفسه ارتكاب فعل يمثل خطرا على السلامة الجسدية أو اي مصلحة يحميها القانون[2]، وأما على المستوى الدولي أكدت أغلب المنظمات والمؤسسات الحكومية ومنظمات المجتمع المدني، على وجوب احترام المبادئ الأخلاقية والعلمية في التجارب التقنية والعلمية والتطبيق بصفة عامة، ومن أهم المبادئ التي جاءت فيها هذه الاتفاقيات هي: 1- سن تشريع بمعاقبة كل من يقوم بإجراء التجارب العلمية على أبناء البلاد المختلفة وأسرى الحرب وخاصة التجارب البيولوجية. 2- عدم إجبار الأطباء على ممارسة أعمال مخالفة لقواعد مهنة الطب. 3- لا يجوز إخضاع الأشخاص إلى العمل الطبي لا تبرره حاجتهم الملحة لهذه الاعمال [3].

(1) - زروقي فايزة، بوراس عبدالقادر، السياسة الجنائية المعاصرة بين أنسنة العقوبة وتطوير قواعد العدالة، المصدر السابق، ص 298.

(2) - د. واثبة داود السعدي ، المصدر السابق، ص 181.

(3) - د. سديرة نجوى ، أ. منار صبرينة، (أثر تطور التكنولوجيا الحيوية في تقرير المسؤولية القانونية عن الاخلال بشروط التجارب على الاجنة البشرية)، بحث منشور، ضمن اعمال المؤتمر الدولي الافتراضي ، بعنوان (انعكاسات التطور التكنولوجي على حق الانسان في السلامة الجسدية) ، برلين - المانيا ، 2021 ، ص71.

وقد إزدادت في الفترة الأخيرة جرائم الإنترنت وذلك على المستوى العالمي، إذ يمكن النظر للإنترنت والتطور التكنولوجي بصورة عامة بانه احد اهم الاسباب التي تهدد الأمن المجتمعي والاقتصادي والسياسي، وخاصة في المجتمعات المغلقة، والشرقية، إذ إن تعرض مثل هذه المجتمعات لقيم وسلوكيات المجتمعات الأخرى، قد يسبب تلوث ثقافيا يؤدي إلى تفسخ إجتماعي وانهيار النظام الإجتماعي العام لهذه المجتمعات، وأن الأستخدام غير الأخلاقي واللا قانوني لشبكات الإنترنت والبرامج والأجهزة التقنية الحديثة، قد يصل إلى مئات المراهقين والهواة مما يؤثر سلبا على نمو شخصياتهم، ويوقعهم في أزمات تؤثر على قيمهم، إذ لا تتماشى مع النظام الإجتماعي السائد وخاصة عند التعامل مع المواضيع غير الأخلاقية، وتقديم الصور، والمواد الإباحية وغيرها من جرائم الإنترنت والتهديد بالقتل والإبتزاز، وهذا ما يمثل تهديدا للسلامة الجسدية نتيجة استخدام هذه التكنولوجيا الحديثة[1].

ونلاحظ أن معظم التشريعات العالمية والإقليمية والمحلية جرمت الإعتداءات الواقعة على الجسم البشري لكون الإعتداء عليه يشكل إعتداء على الإنسان وحقوقه الأساسية المشمولة بحقه في حماية كيانه الجسدي، ولتحقيق هذه الحماية فقد أحاطت هذه تشريعات جسم الإنسان بمجموعة من النصوص القانونية من خلال تجريم الأفعال التي تمثل مساساً بسلامة الجسد البشري، وتشديد العقوبة، سواء أدت هذه الأفعال إلى الحاق الأضرار بالجسم كله، أم الإنتقاص من منفعة بعض أعضائه إذ تُعد الحماية الجنائية لجسم الإنسان أحد أنواع الحماية وخطرها، لكونها تمس التكامل الجسدي وكيان الإنسان وحرياته وأساس هذه الحماية يمثلها القانون الجنائي، اذ تنفرد قواعده ونصوصه بتحقيق تلك الحماية، وتشترك معه في بعض الأحيان فروع القوانين الاخرى[2].

ومن الضمانات المقررة لحماية سلامة جسم الإنسان من التطور التكنولوجي التقني والطبي، هو تقرير مبدأ مهم وهو (يُعد الحق في سلامة الجسم أحد الحقوق الهامة اللصيقة بالفرد)، والتي تعني أن الإنسان يملك حقوقا طبيعية لصيقة به تهدف إلى حماية الشخص في ذاته، وحماية القيم المتصلة به بغض النظر عن جنسيته أو جنسه أو ديانته أو أصله العرقي أو القومي أو وضعه الإجتماعي أو الأقتصادي، وإذا كانت الحقوق تختلف من مجتمع إلى آخر، وذلك على ضوء الظروف السياسية والأقتصادية والإجتماعية الخاصة به فإن المجتمع الدولي متمثل بالأمم المتحدة، قد عمل على تحديد هذه الحقوق الأساسية، وإبرازها كقيم مشتركة بين المجتمعات جميعا، من أجل ضمان حماية الحق في سلامة الجسم

(1) - نسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي ، منشأة المعارف، الاسكندرية، 2008، ص 217.

(2) - عبد السميع بالعيد محمد ، المصدر السابق، ص 311.

بهدف حمايته من بعض التدخلات التي تنتج نتيجة الاستخدام السلبي للتطور التكنولوجي و الطبي في ظل التقدم العلمي[1].

ويمكن القول إن الوقاية من الجريمة هي إحدى وسائل الحماية الجنائية الحديثة، والتي تعتمد أساساً على وضع تدابير وإجراءات عملية تطبيقية، من خلال تقرير العقوبة المناسبة لأي فعل يمس السلامة الجسدية، وتشديدها في حال إرتكب اي فعل يمس السلامة الجسدية عن طريق الأجهزة الإلكترونية، وذلك بتطبيق برامج وأساليب وطرق وتقنيات ميدانية علمية مدروسة وحديثة واضحة المعالم والأهداف من البداية، والسؤال الذي يطرح كيف يتم ذلك؟ الجواب على السؤال هو من خلال طريقة مثلى واحدة، إذ بطبيعة الحال نجد أن لكل مجتمع خصوصيات وظروفه الخاصة، وهو ما يجب أن يؤخذ بعين الإعتبار عند إعتماد أو تطبيق أي سياسة جنائية أو برامج أو أسلوب وقائي، ولكن هناك إطارا عاما، وتوجيهات أساسية يمكن أن تكون المنطق المناسب لغالبية المجتمعات في العمل الوقائي الميداني للوصول لأفضل وإنجع الأساليب للحماية من التهديد التكنولوجي الذي يرتكب من خلال البرامج الحديثة والتقنية الحديثة، ومن خلال هذه التوجهات والمنطلقات والتي تُعد هي حصيلة التجارب السابقة مرت بها المجتمعات والشعوب التي كانت لها الأسبقية في هذا الميدان، يمكن تشريع سياسة جنائية وقائية تضمن الحماية اللازمة لسلامة جسم الانسان وتكامله الجسدي[2].

ولا يمكن لأحد أن ينكر ما للتقدم العلمي والتكنولوجي الحديث من أثر بالغ الأهمية في تحديد حرمة الحياة وسلامة جسم الإنسان والمجتمع بشكل عام، الأمر الذي دفع بالمشرع الجنائي في كل الدول إلى سن تشريعات لحماية السلامة الجسدية للفرد، سواء بطريقة مباشرة أو غير مباشرة، ضد خطر الإعتداءات التي يحدثها إستخدام تلك الأجهزة الحديثة وغيرها من التقنيات التي أفرزتها التكنولوجيا الحديثة، وكان هذا مصدر إشارة للقلق والتساؤل بين رجال القانون والتشريع في الدول المتقدمة حول مدى كفاية النصوص التقليدية في قانون العقوبات وغيرها من القوانين، سواء العامة أو الخاصة، أم يجب وضع تشريعات جديدة لحماية الحياة الخاصة والسلامة الجسدية في مواجهة هذه الأخطار في حالة عدم كفاية الحماية التي تقررها تلك القوانين[3].

---

(1) - د. عيساني رفيقة، (الحماية القانونية للسلامة الجسدية للإنسان في ظل التطور التكنولوجي الطبي)، بحث منشور، ضمن اعمال المؤتمر الدولي الافتراضي، بعنوان (إنعكاسات التطور التكنولوجي على حق الانسان في السلامة الجسدية) ، برلين - المانيا ، 2021 ، ص 158.

(2) - سعداوي محمد صغير، (السياسة الجزائية لمكافحة الجريمة)، اطروحة دكتوراه، جامعة ابو بكر بلقايد، كلية الآداب والعلوم الاجتماعية والعلوم الانسانية، الجزائر، 2010، ص 275.

(3) - ميلود رابح، أثر العولمة على سياسة التجريم والعقاب، رسالة ماجستير، جامعة مولود معمري، تيزي وزو، كلية الحقوق، 2017، ص23.

ونلاحظ في الوقت الحالي وبسبب تطور التكنولوجيا، فقد تطورت أساليب التعذيب، من خلال ممارسة الإكراه المادي والمعنوي، الذي يمارسه رجال السلطة العامة على المتهم لحملة على الاعتراف، أو نتيجة تعرض المجنى عليه من قبل شخص آخر بواسطة الأجهزة المتطورة تكنولوجياً لتحقيق غايات خاصة، فجميع هذه الطرق والأساليب تمس السلامة الجسدية سواء في شكلها المادي أو المعنوي، وصور التعذيب كثيرة ومتنوعة، لا يمكن لها من حصر، وفي ظل التطور التكنولوجي والعلمي فأن إساليب التعذيب باتت غير تقليدية، وذلك لكون التطور التكنولوجي أفرز أساليب حديثة في مجال التعذيب ومن هذه الأساليب والطرق الحديثة هو وضع الشخص تحت جهاز كشف الكذب، والتخدير ، والتنويم المغناطيسي وغيرها من الطرق الوحشية التي يترتب عليها آثاراً سلبية لها آثار خطرة على سلامة الجسد[1]. لذا ذهبت بعض التشريعات المقارنة إلى تشديد العقاب من اجل فرض سياسة عقابية ناجعة، تهدف إلى (الردع والمنع)، من ارتكاب اي فعل تم تجريمه، أو عدم العود في إرتكاب الجريمة، وهذا ما إنتهجه المشرع الإماراتي من خلال تتبعنا لتشريعه لقانون مكافحة الجرائم التقنية والمعلوماتية رقم (2) لسنة 2006 وما طرأ عليه من تعديلات حتى صدور المرسوم بقانون رقم (5) لعام 2012، فقد شدد المشرع الإماراتي العقوبات، وذلك نظرا للتطورات التقنية التي يعيشها البلد والعالم على مختلف الاصعدة، فغاية المشرع من تشديد العقاب في ظل القانون أعلاه، هو لبسط سياسة الردع والمنع، من إرتكاب اي فعل مجرم يمس المصالح المحمية بموجب القانون[2]. فالظروف المشددة هي عناصر تبعية تقترن بالجريمة لتضفي عليها وصفاً يرتب أثراً مشددا وفق ما يحدده القانون، فوجود هذه العناصر التي توجب تشديد العقاب، لها تأثير كبير في وصف الجريمة وتحديد العقاب المناسب، وحسب جسامة الفعل وخطورة المجرم[3].

ومن خلال ما تقدم بيانه يرى الباحث بوجوب أن تكون السياسة العقابية سياسة رادعة ومانعة ووقائية، ويتحقق ذلك من خلال تشديد العقاب، وعدم التهاون مع الجاني في حال ارتكب أي فعل يشكل خطرا على السلامة الجسدية أو اي مصلحة معتبرة محمية بموجب القانون، من أجل زرع الثقة داخل نفوس المجتمع، وأيضا من أجل تحقيق الهدف المرجو من السياسة العقابية وهو الردع العام والخاص، بالإضافة إلى تأهيل وإصلاح المجرم، ويبقى حاضرا في أذهان الافراد المعنيين بتطبيق القانون.

---

(1) - عاقلي فضيلة، المصدر السابق، ص 164 .

(2) - د. محمد شاكر الحمادي، نظرات في السياسة العقابية لقانون مكافحة المخدرات الاماراتي بين النص التشريعي والتطبيق القضائي، بحث منشور، مجلة العلوم القانونية والاقتصادية، المجلد 60، العدد 2، مصر، 2018 ص 868.

(3) - د. سعد صالح شكطي، الخروج عن القاعدة في الظروف المشددة للجرائم، بحث منشور، مجلة جامعة تكريت للعلوم القانونية، المجلد 1، العدد 28، 2015، ص 73 .

المبحث الثاني

أثر التطور التكنولوجي في ظهور الجرائم الإلكترونية

تختلف الجريمة التي ترتكب بواسطة التكنولوجيا الحديثة والانترنت، عن الجرائم العادية التقليدية من حيث الوسائل والدوافع والخصائص، ونجد أن العالم قد شهد تطوراً هائلاً في إستعمال مجال الأتصالات وتقنية المعلومات، كإستخدام الحاسوب والهواتف النقالة الذكية ومواقع التواصل الإجتماعي، حتى أضحى العالم يتنافس على استخدام هذه التكنولوجيا الحديثة، وأصبح العالم لا تفصله حدود كما هو الحال في الماضي، وأصبحت الدول يقاس مدى تقدمها من خلال قدرتها وكفاءتها في التعامل مع هذا التطور التكنولوجي.

وعلى ضوء ذلك سنحاول دراسة موضوع تأثير التطور التكنولوجي على ظهور بعض الجرائم الالكترونية من خلال تقسيم هذا الموضوع إلى مطلبين، نبحث في المطلب الاول ماهية الجريمة الالكترونية، أما المطلب الثاني فنخصصه لدراسة دور السياسة الجنائية في حماية الانسان من الجرائم الناشئة عن التطور التكنولوجي.

المطلب الأول

ماهية الجرائم الالكترونية

تشكل الجرائم الالكترونية أحد أبرز المواضيع في الوقت الحالي لدى الباحثين والفقهاء والمشرعين، فالجريمة الالكترونية لها مسميات وسمات كثيرة، وللإحاطة بماهية الجريمة الالكترونية، لذا سنقسم دراستنا في هذا المطلب إلى فرعين، نخصص الفرع الاول لدراسة مفهوم الجريمة الالكترونية، ونبحث في الفرع الثاني خصائص الجريمة الالكترونية.

الفرع الاول

مفهوم الجريمة الالكترونية

أدت الحداثة التي تتميز بها جريمة المرتكبة عبر الإنترنت، واختلاف النظم القانونية والثقافية بين الدول، إلى عدم الإتفاق على مصطلح محدد للدلالة عليها، وعدم الاتفاق على وجود تعريف واحد محدد لهذه الظاهرة الإجرامية، وذلك خشية حصر هذه الجرائم الإلكترونية في مجال ضيق ومحدود، لذا فقد تعددت التعريفات التي جاءت حول تعريف الجريمة الإلكترونية من حيث طبيعة مصدرها، وهناك

تعريفات تشريعية وقد اختلفت باختلاف المصدر الذي ينظر إلى هذه الجرائم، وهذا النوع من الجرائم قد تعددت مسمياتها، فبعضهم أسماها الجرائم الإلكترونية، وبعضهم الآخر أطلق عليها جرائم الحاسوب، وهنالك من أسماها بجرائم التكنولوجيا الحديثة، وأيضاً سميت بالجرائم المعلوماتية وغيرها من المسميات الأخرى. ولذلك نجد أن الفقه قد انقسم إلى أربعة إتجاهات، وهذه الأخيرة تقوم على أسس مختلفة في تعريف الجريمة المرتكبة عبر الإنترنت، وهي:

أولاً : تعريف الجريمة الإلكترونية.

1- الجريمة لغة : الجريمة، من الفعل جرم ، جرماً أذنب. ويقال جرم نفسه وقومه، بمعنى التعدي، والجرم: الذنب والجمع أجرام وجروم وهو الجريمة، وجرم يجرم جرماً، وأجترم وأجرم، فهو مجرم[1]. وأجرم أرتكب جرماً، ويقال: أجرم عليهم واليهم جنى جناية[2].

2- الجريمة الإلكترونية اصطلاحاً : لقد انقسم الفقه إلى أربعة إتجاهات، تقوم على أسس مختلفة في تعريف الجريمة الإلكترونية وهي:

الاتجاه الاول: يعرف الجريمة الإلكترونية على أساس وسيلة إرتكاب الجريمة، فهناك من يعرف الجريمة الإلكترونية بالاعتماد على الوسيلة التي يتم إرتكاب الجريمة من خلالها، ألا وهي الحاسب الآلي، وقالوا هي الجرائم التي يتم إرتكابها عن طريق الحاسب الآلي[3].

أما الاتجاه الثاني: فقد عرفوا الجريمة الإلكترونية على أساس توافر المعرفة بتقنية المعلومات- وقالوا بان الجريمة الإلكترونية : هي (السلوك الذي ينتهجه الجاني في إطار فعله الإجرامي)[4]. في حين هناك من يعرف الجريمة الإلكترونية بالإعتماد على توافر شرط إلمام الجاني بتقنية المعلومات. وقالوا بأن الجريمة الإلكترونية هي: (كل نشاط إيجابي أو سلبي من شأنه الاتصال دون وجه حق بالكيان المعنوي للحاسب الآلي أو بنظام المعلومات العالمية (الإنترنت) أو الإبقاء عليه عند تحققه، أو التأثير عليه بتعطيله أو اضعاف قدرته على أداء وظائفه بالنسخ أو التعديل أو الإضافة أو الحذف الكلي أو الجزئي أو بالمناقلة للخصائص الاساسية للبرامج)[5]. وآخرون يعرفونها بأنها (كل فعل أو إمتناع

(1) - ينظر: ابن منظور، أبو الفضل جمال الدين محمد بن مكرم، لسان العرب، بيروت، ص91.
(2) - ينظر: المعجم الوسيط، صادر عن مجمع اللغة العربية بجمهورية مصر ، ط 4 ، مكتبة الشروق الدولية، 1435 هـ، 2004 م، ص 118 .
(3) - د. عبد الفتاح بيومي ، المصدر السابق، ص 26 .
(4) - د. محمد كمال محمود الدسوقي، المصدر السابق، ص14 .
(5) - د. خالد ممدوح ابراهيم، حوكمت الانترنت، دار الفكر الجامعي، الاسكندرية، 2011، ص 356

عمدي ينشأ عن الأستخدام غير المشروع لتقنية المعلوماتية ويهدف إلى الإعتداء على الأموال المادية أو المعنوية)[1].

والاتجاه الثالث: فقد تناول تعريف الجريمة الإلكترونية على أساس موضوع الجريمة، وقالوا بأن الجريمة الإلكترونية: (هي الجريمة التي يتم إرتكابها إذا قام شخص ما بإستخدام معرفته بالحاسب الآلي بعمل غير قانوني)[2]، ويعرفها بعضهم على أنها: (الجرائم التي لا تعرف الحدود الجغرافية والتي يتم إرتكبها بأداة هي الحاسب الآلي عن طريق شبكات الإنترنت أو بواسطة شخص على دراية فائقة بهما)[3]، ويعرفها الاستاذ (Rosenblatt) بأنها: (كل نشاط غير مشروع موجه لنسخ أو تغيير أو لحذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه)[4]. ويعرفها الاستاذ (Elsie d. ball) بأنها: (فعل إجرامي يستخدم الكمبيوتر في إرتكبها كأداة رئيسية). أما الفقيه الفرنسي (vivant) يعرف الجريمة الإلكترونية على أنها: (مجموعة من الأعمال المرتبطة بالمعلومات الإلكترونية والتي يمكن أن تكون جديرة بالعقاب)[5]. في حين هناك بعض الفقهاء تبنى تعريف للجريمة الإلكترونية على أنها: (الجريمة التي يكون موضوعها يتمثل بالمعلومات والبيانات الإلكترونية، وتكون هذه هي محل الجريمة، وذلك عندما يتجه قصد الجاني إلى الإعتداء عليها كأتلاف أو تخريب البرامج أو تزويرها)[6]. وهناك من يعرفها: بأنها (الجريمة التي تقع على جهاز الكمبيوتر أو داخل نظامه فقط). وهناك رأي فقهي آخر عرفها: بأنها (كل عمل أو إمتناع يأتيه الأنسان اضراراً بمكونات الحاسب المادية والمعنوية وشبكات الأتصال الخاصة به بإعتبارها المصالح والقيم المتطورة التي تمتد مظلة قانون العقوبات لحمايتها)[7].

أما الاتجاه الرابع: حاول الدمج بين أفكار وروئ الاتجاهات الثلاث في تعريف الجريمة الإلكترونية - الجريمة الإلكترونية هي كل عمل محظور ممنوع من قبل القانون، لهذا يجب أن تكون هناك قوانين من أجل تحديد الأفعال المسموحة والممنوعة، ومصطلح الجريمة الإلكترونية مفهوم غامض له عدة مفاهيم

(1) - د. عفيفي كامل، المصدر السابق، ص 460 .

(2) - د. محمد الامين البشري، التحقيق في جرائم الحاسب الالي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، كلية القانون والشريعة، جامعة الامارات، 2005، ص 6، مشار اليه لدى، د. عبدالفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، دار الفكر الجامعي، الاسكندرية، 2006، ص 20.

(3) - عادل يوسف عبدالنبي، الجريمة المعلوماتية وازمة الشرعية الجزائية، بحث منشور، مجلة مركز دراسات الكوفة، العدد 7، 2011، ص 112.

(4) - د. علي محمود علي ، المصدر السابق، ص 16 .

(5) - صدام حسين ياسين العبيدي ، المصدر السابق، ص 39.

(6) مصطفى محمد موسى ، اساليب إجرامية بالتقنية الرقمية (ماهيتها مكافحتها)، دار الكتب القانونية ، 2005 ، ص56.

(7) - بلقيس عبد الرحمن حامد، المخدرات الرقمية، بحث منشور، مجلة العدل، العدد 48، السنة 19، 2017 ، ص72.

وتفاسير[1]، فالمجرم هنا مخفي وراء شاشة بعيده والجريمة تقع في عالم أفتراضي غير ملموس، والضحية والجاني لم يلتقيا ولم يحصل بينهما تصادم، وقد يكون كل منهما في بلد مختلف. وُتعد الجرائم الإلكترونية كل الجرائم التي ترتكب بإستخدام الإنترنت أو شبكة كمبيوتر أخر، ويمكن أن تكون أجهزة الكمبيوتر متورطة في الجريمة الإلكترونية بطريقة مختلفة، كما تكون عن طريق الكمبيوتر، والشبكة هما أداة الجريمة تستخدم لإرتكاب الجريمة أو أن تكون شبكة الكمبيوتر هي الضحية وقد يكون إستخدام الكمبيوتر أو الشبكة لأغراض عرضية تتعلق بالجريمة[2].

3- **التعريف التشريعي للجريمة الإلكترونية:** لقد عرف **المشرع السعودي** الجريمة الإلكترونية وفقا لنص المادة (1) من نظام مكافحة الجرائم المعلوماتية، بأنها: أي فعل يرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لإحكام هذا النظام. **أما المشرع الكويتي** فقد تطرق لتعريف الجريمة الالكترونية من خلال نص المادة (1) من قانون مكافحة جرائم تقنية المعلومات رقم 63 لسنة 2015 على أنها: (كل فعل يرتكب من خلال إستخدام الحاسب الآلي أو الشبكة المعلوماتية أو غير ذلك من وسائل تقنية المعلومات مخالفة لإحكام هذا القانون)[3]. أما **المشرع الامريكي** فقد عرفها على أنها: (الإستخدام غير المصرح به لأنظمة الكمبيوتر المحمية أو ملف البيانات أو الإستخدام المتعمد الضار لأجهزة الكمبيوتر أو ملفات البيانات وتتراوح خطورة تلك الجريمة ما بين جنحة من الدرجة الثانية إلى الجناية من الدرجة الثالثة). أما **المشرع الجزائري** فقد عرف الجريمة الإلكترونية من خلال القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها وعرفها بانها: (جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل إرتكبها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية)[4]. ونجد منظمة التعاون والتطوير الأقتصادي عرفت الجريمة الإلكترونية على أنها: (تصرف غير شرعي وغير أخلاقي أو غير مسموح به في الإنتقال أو المعالجة الآلية للمعطيات، وهذا لا يخص فقط نشاطات الإنترنت وانما كل ما يمكن فعله من خلال المعلومات الإلكترونية والاتصالات عن بعد، بما فيها الهواتف الثابتة أو النقالة). أما المنظمة الأوروبية للتعاون والتنمية الاقتصادية، فقد عرفت الجريمة الإلكترونية على أنها: (كل سلوك غير مشروع أو مناف للأخلاق أو غير مسموح به

(1) - د. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، منشأة المعارف، الاسكندرية، من دون سنة نشر، ص 462.

(2) - فيلالي أسماء، ورقة عمل بعنوان، المجرمون المعلوماتيون خطر حقيقي يهدد عالم المعلوماتية، اصدار المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، برلين، الجزء الاول، 2020 ، ص51.

(3) - المادة (1) من قانون مكافحة جرائم تقنية المعلومات الكويتي رقم 63 لسنة 2015.

(4) - خرشي عثمان، المفهوم الفقهي للجريمة المعلوماتية، بحث منشور، اصدار المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية ، بعنوان ، الجريمة المعلوماتية وأثرها على التنمية الاقتصادية، الجزء الاول، برلين، 2020 ، ص 28.

يرتبط بالمعالجة الآلية للبيانات أو بنقلها). وكذلك عرف مكتب التقنية بالولايات المتحدة الأمريكية بأنها: (الجرائم التي تلعب فيها البيانات الإلكترونية والبرامج المعلوماتية دورا رئيسياً) [1].

أما المجلس الأوروبي فقد قام بإصدار توصية عام (1989) الغرض منها تشجيع الدول الأعضاء على تبني نصوصاً عقابية خاصة بالجرائم الإلكترونية، الاّ أن الدول قد أختلفت في أختيار التقنية التشريعية المناسبة فمنها من قام على دمج نصوص خاصة بالجرائم الإلكترونية في قانون العقوبات النافذ في الدولة، في حين اتجه آخرون إلى وضع قوانين جنائية مستقلة للجرام الإلكترونية والمعلوماتية، فالجريمة الإلكترونية توصف بأنها ذلك الفعل الذي يستخدم تقنية المعلومات عبر النظام الإلكتروني الحاسوب كوسيلة لإرتكاب الفعل المخالف للقانون محدثاً ضرراً على كل من الفرد والمجتمع، هذه الوسيلة التي شقت طريقها لتصل إلى أقصى مراحل التطور العلمي والتكنولوجي والتقني فجعلت الحياة أسهل كما في إبرام العقود الإلكترونية والتجارة الإلكترونية و المعاملات المدنية[2]، الإّ أن هذا الأمر لا يخلو من بعض الجوانب السلبية والتي تمثلت بالجرائم الإلكترونية الحديثة إلاّ أن هذا التقدم العلمي والتطور السريع جعل المشرعين غير قادرين على مواكبة هذا التطور إلا أنهم قاموا بوضع وأضافه بعض النصوص إلى القانون الجنائي، إلا أن دمج النصوص الجديدة في القانون التقليدي قد أثار عددا من الإشكاليات من ضمنها الموقع الذي سيوضع فيه هذه النصوص ، فبعض الفقهاء، إشار إلى إمكانية دمجها مع جرائم الأموال بإعتبار إمكانية إسباغ صفة المال على البيانات المادية والمعنوية للحاسوب[3]، في حين ذهب بعض آخر من الفقهاء إلى دمج هذه النصوص بالجرائم الخاصة، ضمن نصوص القانون الخاص، على أساس أن الكيان المادي للحاسوب هي عناصر مادية قابلة للتملك[4]، وذهب جانب آخر منهم إلى أُنه من الأفضل إلحاق الجريمة الإلكترونية بما يقابلها في قانون عقوبات التقليدي، كما في وضع جريمة التزوير المعلوماتي في باب تزوير المحررات[5].

(1) - خرشي عثمان، المصدر السابق، ص 29.

(2) - لينا محمد ، المصدر السابق، ص 169.

(3) - د. عبدالقادر الشيخلي، الجهود والإتفاقيات العربية والدولية لمكافحة الجريمة، بحث مقدم إلى الدورة التدريبة لمكافحة الجريمة الأقتصادية، جامعة نايف العربية للعلوم الامنية، 2007 ، ص 8.

(4) - د. تيانتي مريم ، ورقة عمل بعنوان، الجريمة الإلكترونية بين القيام والتجريم، إصدار المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والأقتصادية، بعنوان ، الجريمة المعلوماتية وأثرها على التنمية الأقتصادية، الجزء الأول، برلين، 2020 ص 41 .

(5) - د. محمد كمال محمود الدسوقي ، المصدر السابق، ص14.

ويرى الباحث أن أغلب هذه التعاريف تعرف الجريمة الالكترونية من ناحية ضيقة وعدم الذهاب لنظرة أبعد مما نعيشه الآن في ظل التطور التكنولوجي؛ لكون أغلب هذه التعاريف تتضمن المساس بالبيانات أو الحاسوب والانترنت فقط.

ولذا يمكننا تعريف الجريمة الإلكترونية بأنها: (كل فعل يسبب ضررا ماديا أو معنويا للفرد أو للآمن المجتمعي والالكتروني بواسطة التكنولوجيا الحديثة، سواء عن طريق الحاسوب أم الإنترنت، أم اي تقنية حديثة، على المكونات المادية والمعنوية لأي نظام إلكتروني عام او خاص).

ثانيا : أسباب ودوافع الجريمة الإلكترونية.

1- أسباب الجريمة الالكترونية

لإرتكاب الجريمة الإلكترونية عدة أسباب، منها ما يقع على المستوى العالمي، ومنها ما يقع على المستوى الإجتماعي، ومنها ما يقع على المستوى الأقتصادي أو السياسي، ومنها ما يقع لأسباب خاصة، أو لأسباب عامة، اي أن أسباب إرتكاب الجريمة الإلكترونية تتفاوت وفق نوعها ونوع الشخص المستهدف ونوع الجاني، فجرائم الشباب والهواة تختلف عن أسباب جرائم المحترفين، وتختلف هذه الأسباب نتيجة لإختلاف الدافع والهدف لإرتكاب الجريمة، فهناك جرائم الكترونية ترتكب لأسباب التحدي، أو لأسباب حب الظهور في الإعلام والشهرة، وقد ترتكب الجرائم الإلكترونية لأسباب إنتهاز الفرصة، مثال على ذلك، إن وقت الانحراف عن قواعد الامتثال والمراقبة ليلاً ونهاراً وفي أي مكان وعدم وجود رقابة، جميع هذه الأسباب والعوامل تزيد من فرصة إرتكاب الجريمة الإلكترونية[1]، أما الأسباب الإجتماعية لإرتكاب الجرائم الإلكترونية، فيمكن القول إن أهم أسباب إرتكاب الجريمة هو الهجرة من الريف إلى المدينة، ومن ثم فأن العيش في المدينة يتطلب مصاريف كبيرة، مما يؤدي بالشخص إلى التفكير في كيفية تلبية متطلبات الحياة الحضرية، ونتيجة لذلك فأن الشخص يجد نفسة في تنافس شديد، وقد يؤدي به إلى الإستثمار في الجريمة الإلكترونية، من خلال الادمان على المواقع ولسهولة ارتكابها، ونجد أيضا أن سبب البطالة لها علاقة كبيرة وأهم أسباب إرتكاب الجريمة الإلكترونية، كما يوصف بعض الفقهاء سبب البطالة بمقولة (العقل العاطل عن العمل هو ورشة عمل للشيطان). بالإضافة إلى أن هناك سبباً اخر لإرتكاب الجريمة الإلكترونية وهو ضعف القانون وتطبيقه على الجرائم التي ترتكب بواسطة الإنترنت والتكنولوجيا الحديثة، فهناك دول عديدة لم

(1) - د. أكرم سلام عبدالرؤوف سلام، الجرائم الالكترونية في الفقه الاسلامي والقانون الوضعي، بحث منشور، كتاب صدر عن اعمال المؤتمر الدولي الافتراضي، بعنوان (الجرائم الالكترونية في الفقه الاسلامي والقانون الوضعي)، برلين- المانيا، 2022، ص 57 .

تواكب تشريعاتها الجنائية الحداثة والتطور التكنولوجي، وأجهزة العدالة فيها لا ترتقي إلى المستوى المطلوب لمكافحة الجريمة الإلكترونية، وهذا ما يسبب عاملاً مهماً ورئيسياً لإرتكاب الجريمة، لعدم وجود أجهزة وقوانين تستطيع التعامل مع الأدلة الرقمية، وهذا يُعد من أهم الاسباب التي تؤدي إلى تزايد الجرائم الالكترونية وذلك بسبب غياب التشريعات الجنائية وضعف الممارسات العدلية والقضائية[1].

2- دوافع ارتكاب الجريمة الالكترونية

الدافع أو الباعث هو العامل المحرك للإرادة الذي يوجه السلوك الاجرامي، كالمحبة والشفقة والبغضاء والإنتقام، جميعها عبارة عن قوة نفسية تدفع بالشخص بإرادته نحو ارتكاب الجريمة لتحقيق غاية معينة[2]، ويقول الدكتور (Adam graycar) وهو مدير المعهد الإسترالي لعلم الإجرام، بأن الجريمة تحتاج إلى أربعة عناصر مهمه تدفع المجرم للقيام بجريمته وهذه العناصر هي : (دافع شخصي لارتكاب الفعل، وهدف ضحية ، والعمل على الفرصة المواتية، وغياب عيون الأمن). فالدافع والباعث يشكل أهم ركائز إرتكاب الجريمة[3].

ونلاحظ أن المجتمع العالمي بدأ يتعامل مع التطور التكنولوجي في شتى تفاصيل الحياة، وأصبح التعامل مع شبكات الإنترنت والبرامج والتطبيقات الإلكترونية أمراً لا يمكن الاستغناء عنه، ونتيجة لهذا الواقع الذي تعيشه المجتمعات والأسر، فقد أدى ذلك إلى ظهور عدد كبير من الجرائم الإلكترونية، وهذه الجرائم ترتكب نتيجة لدوافع شخصية أو لدوافع سياسية أو أقتصادية أو إجتماعية، وعلى ضوء ذلك سنحاول بيان بعض الدوافع التي تؤدي إلى إرتكاب الجرائم الإلكترونية وهي :

أ- دوافع شخصية : وتنقسم هذه الدوافع إلى قسمين ، القسم الاول وهي (الدوافع المادية) وتتمثل بتحقيق الربح وكسب المال، ويُعدّ هذا الدافع من أكثر الدوافع التي تحرك المجرم لإرتكاب الجريمة الإلكترونية، لكون هذه الجرائم تكسب الجاني أرباحاً كبيرة ودون بذل جهد أو عنف، وبهذا فان المجرم تتزايد لديه الرغبة بإرتكاب مثل هذه الجرائم لسهولتها وصعوبة تتبعه، بالإضافة إلى سهولة محو الدليل[4]. أما القسم الثاني فهو (الدوافع الذهنية)[5]، في بعض الأحيان يكون الدافع لدى الجاني في

---

(1) - د. رمسيس بهنام، علم الاجرام، منشأة المعارف، الطبعة الاولى، 1961، ص 111. وينظر كذلك: د.ذياب موسى البداية، ورقة عمل، الجرائم الالكترونية (المفهوم والاسباب)، ضمن اعمال الملتقى العلمي بعنوان (الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية)، المقام في الاردن، 2014، ص14.

(2) - د. حسين بن سعيد الغافري، المصدر السابق، ص 55.

(3) - نسرين عبدالحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف، الاسكندرية، 2008، ص43.

(4) - علي عدنان سلمان الركابي، جريمة الارهاب المعلوماتي، دار السنهوري، بيروت، 2020 ، ص 55.

(5) - د. محمد ممدوح بدير، المصدر السابق، ص 59.

الجرائم الإلكترونية هو الرغبة في إثبات الذات، وتحقيق الإنتصار، دون أن تكون لديهم الرغبة للأضرار بالمجنى عليه، فهدفهم هو السباق لخرق الأنظمة الإلكترونية، بباعث التسلية أو المنافسة، وقد ترتقي مثل هذه الأفعال إلى درجة الجريمة لكونها تمثل خرقا وضرراً جسيماً يمس الأمن الإلكتروني[1].

ب- الدوافع الخارجية : بمعنى أن المجرم من الممكن أن يتاثر ببعض الظروف والتي قد تدفعه لإرتكاب الجريمة الإلكترونية، ويهدف الجاني من وراء هذا الجرائم إلى الإنتقام أو لكسب المال أو للمساومة على أمر ما. مثال على ذلك فقد يكون الدافع لإرتكاب الجريمة هو نتيجة لأثبات الذات (الانتقام) وقد يكون الإنتقام من صديق، أو أحد الاقارب أو من رب العمل، لألحاق الضرر بهم، ويقوم المجرم بهذه الأفعال، نتيجة لتعرضهم لظروف وضغوطات نفسية كبيرة، ناجمة عن ضغط العمل أو لأسباب مالية، أو نتيجة لظلم يتعرضون له، فهذه الدوافع هي من ثم تمثل دوافع لإشباع رغبات المجرم بالإنتقام[2].

ت- دوافع سياسية أو أقتصادية : من اهم الدوافع التي تدفع بالمجرم إلى القيام بجريمته هي الدوافع السياسية والاقتصادية، فقد تكون الدوافع لأغراض المنافسة، لتحقيق أهداف تجارية أو سياسية، وقد تكون الدوافع الرغبة في الحصول على الربح خاصة في الجرائم التجارية، وإثبات التفوق على المنافسين؛ لكون مرتكبي هذه الجرائم لديهم الشغف في التفوق والربح[3].

ث- تهديد الأمن القومي والعسكري : ترتكب بعض الجرائم الإلكترونية بدافع تهديد الامن القومي والعسكري لزعزعة النظام الأمني للدول، ويكون الهدف من وراء إرتكاب مثل هذه الجرائم هي لدوافع سياسية تتمثل في تهديد الأمن القومي، وبعضهم يسميها بحرب المعلومات والتجسس الإلكتروني والإرهاب الإلكتروني، وقد حصل في المدة الماضية العديد من الحوادث التي تمثل مثل هذه الحرب الإلكترونية أو التهديد الأمني الإلكتروني، كما حصل ما بين سنة (1990 و 1991) عندما أستطاع مجموعة من المتسللين من هولندا، ونجحوا بالتسلل إلى (34) نظاما الإلكترونيا[4].

---

(1) - نسرين عبدالحميد نبيه، المصدر السابق، ص 45.

(2) - ياسمينة بونعارة، الجريمة الالكترونية، مجلة المعيار ، العدد 39، 2015، ص 288.

(3) - د. محمود احمد طه ، المواجهة التشريعية لجرائم الكمبيوتر والانترنت، دار الفكر والقانون، مصر، 2012، ص16 . وكذلك : د. أكرم سلام عبدالرؤوف سلام، الجرائم الالكترونية في الفقه الاسلامي والقانون الوضعي، المصدر السابق، ص 58.

(4) - د. حسين بن سعيد الغافري، المصدر السابق ، ص 59 .

الفرع الثاني

خصائص الجريمة الالكترونية

تتميز الجرائم إلكترونية بخصائص وسمات عدة مما تجعلها تختلف عن بقية الجرائم التقليدية ومن هذه الخصائص والسمات هي:

أولا: يكون فيها المجرم أو الجاني ذو خبرة في المجال التقني، فقد ثبت في عديد من القضايا، وأن عددا من المجرمين لا يرتكبون سوى جرائم الكمبيوتر، أي أنهم يتخصصون في هذا النوع من الجرائم، فهذا النوع من الجرائم يتم من خلال إستخدام الحاسب الآلي، بمعنى أن جهاز الحاسب الآلي هو الأداة الرئيسية التي يقوم الجاني من خلالها بإرتكاب جريمته وهذا ما يمثل الركن المادي للجريمة الإلكترونية، وهذا ما يشكل أيضا صعوبة الإبلاغ عن مثل هذه الجرائم، وذلك بسبب عدم معرفة شخص مرتكب الجريمة وصعوبة تتبعه[1]. بالإضافة إلى ان هذه الجرائم (الإلكترونية) تتميز على أنها جرائم ترتكب من قبل أشخاص يتمتعون بدهاء، وذي خبرة، وأختصاص في المجال التقني والمعلوماتي وعلى دراية فائقة في كيفية التعامل مع هذه الجرائم من خلال الحاسب الآلي وشبكات الإنترنت[2].

ثانيا: الجرائم الإلكترونية يتميز فيها المجرم بكونه مجرماً عائدا إلى الإجرام، أي بمعنى أن المجرم يعود كثيراً إلى إرتكاب جرائم اخرى في مجال الحاسب الآلي، انطلاقاً من الرغبة في سد الثغرات أو التوصل إلى أهداف أو سرقة الأموال أو الإبتزاز، إضافة إلى سبب عدم كشفهم وسهولة إرتكاب الجريمة وإخفاء الأدلة [3].

ثالثا: تعد من الجرائم الناعمة[4]، بمعنى أن المجرم عند ارتكابه لأي فعل في جرائم الكمبيوتر، فانه لا يحتاج إلى جهد بدني ووسائل مادية كالسكين أو الاسلحة النارية أو مواد سامة، وانما يعتمد على التقنية الحديثة وجهاز حاسوب، لان جرائمه تنتمي إلى جرائم الحيلة[5]، والسبب في ذلك لكونها جرائم لا تترك أثراً لها، فلا توجد دماء أو جثة أو بصمات أو أداة إرتكاب الجريمة كالسكين أو الأسلحة،

(1) - د. عبد الفتاح بيومي ، المصدر السابق، ص 97.
(2) - د. سحر سعد عبد السميع ، المصدر السابق ، ص 27 .
(3) - د. علي عدنان الفيلي، الاجرام الالكتروني، منشورات زين الحقوقية، 2011 ، ص 74.
(4) - د. اكرم سلام عبدالرؤوف سلام، المصدر السابق، ص 66.
(5) - د. يعيش تمام شوقي، الجريمة المعلوماتية، مطبعة الرمال، الجزائر، 2019، ص 29.

بالإضافة إلى طبيعة التطور التكنولوجي الذي يجعل من هذه الجرائم سهلة التنفيذ وعدم بذل أي جهد بدني يذكر مما يصعب أو يستحيل الوصول إلى الجاني [1].

رابعا: صعوبة اكتشاف الجريمة الإلكترونية بالإضافة إلى عدم وجود الخبرة اللازمة لدى بعض الأجهزة الأمنية والقضائية في التعامل مع مثل هذه الجرائم. وهذا ما يسبب صعوبة للتوصل لمرتكب الجرائم الالكترونية، وذلك نظرا لسرعة غياب الدليل الرقمي و سهولة إتلاف البيانات وتدميرها[2].

خامسا: تتسم الجريمة الإلكترونية بكونها جريمة عابرة للحدود والدول والقارات وغير خاضعة لنظام إقليمي محددة[3]. فمثل هذه الجرائم لها أبعاد دولية، تتخطى آثارها ونتائجها أكثر من دولة، فتؤدي إلى حدوث أضرار مادية ومعنوية تمس مصالح أساسية للدول، والنظام العام فيها، سواء على الصعيد الأمني أو الأقتصادي أو الإجتماعي، لذلك إتفق أغلب الفقهاء والمشرعين على أن الجرائم الالكتروني تعد من جرائم أمن الدولة[4].

سادسا : صعوبة إجراء التحقيق والمحاكمة، أن أهم ما يميز الجرائم الإلكترونية، هو غموضها وصعوبة إثباتها والتحري عنها والتحقيق فيها، وذلك لسهولة إتلاف الأدلة وبالإضافة إلى صعوبة تحديد مكان إرتكاب الجريمة، وهذا ما يسبب إشكالية كبيرة في تحديد أختصاص المحكمة المختصة بالنظر في هذه الجرائم وإجراءات الضبط والتفتيش والملاحقة[5].

المطلب الثاني

دور السياسة الجنائية في حماية الإنسان من الجرائم الناشئة عن التطور التكنولوجي

يمكن القول إن غالبية برامج التواصل الاجتماعي والتي تعد وليدة التطور التكنولوجي وأساس فاعلية شبكات الانترنت، وأغلب جرائم الانترنت ترتكب عن طريق هذه البرامج، أو بسببها، أو عن طريقها، وغدت هذه البرامج بمثابة وسائل حديثة لصناعة وتوليد الرأي العام في القضايا والمواضيع وهي أداة فاعلة لا يمكن إغفالها ولا سيما أنها تشهد مزيدا من الأقبال والداخلين الجدد إليها من الجمهور بمختلف

(1) - د. سلام عيسى العبادي ، الارهاب الالكتروني أخطاره وخصائصه وأهدافه ومكافحته، الطبعة الاولى، 2018، ص 94 .

(2) - د. رامي متولي القاضي، شرح قانون مكافحة جرائم تقنية المعلومات، مركز الدراسات العربية، 2020، ص259 .

(3) - علي عدنان سلمان الركابي، المصدر السابق، ص 40. وكذلك: د. خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، 2009 ، ص 77.

(4) - د. حازم حسن الجمل، الحماية الجنائية للأمن الالكتروني، دار الفكر والقانون، مصر، 2022 ، ص 14.

(5) - د. حسين بن سعيد الغافري، المصدر السابق ، ص 55.

الفئات والأعمار ومستوياته[1]، إذ أصبح أن لكل صناعة إستراتيجيات ومنها صناعة الرأي عبر مواقع التواصل الإجتماعي وإستخدام عدد من الحكومات والجهات والشركات شبكات التواصل في مجالات عدة لتسويق أفكارها ومنتجاتها وطرحها بأساليب مختلفة، نجح بعضها في جذب الجمهور واخفق بعضها الآخر، وإن أحد أهم الإستراتيجيات المستخدمة في صناعة الإعلام عبر شبكات التواصل الإجتماعي هو التركيز على معرفة مدى حاجة الفئات المستهدفة وكيفية بلورة المنتج والفكرة، وصياغته لتقديمه للجمهور بطريقة تجعلهم يتفاعلون معه ويقدمون آراءهم فيه، حيث تكون ورش عمل مفتوحة لصناعة الرأي تتيح للجهات والشركات والمؤسسات معرفة إتجاهات المجتمع وآرائه وملاحظاته على المنتج أو الفكرة المقدمة وهذا ما يؤثر إيجاباً أو سلباً على الأمن الأسري والأمن ألإلكتروني على حد سواء.

الفرع الأول

الجرائم الإلكترونية الماسة بالأمن الاسري

إن دراسة وبحث الجرائم الماسة بالأمن الأسري، يتطلب منا في البدء معرفة وتعريف الامن الإسري من خلال بيان التعريف لكلا المصطلحين (الأمن ، والأسرة) لغة وإصطلاحا.

يقصد بالأمن لغة: سكون القلب أو الهدوء النفسي وعدم الخوف، ويعرف بأنه الأمانة التي هي ضد الخيانة بمعنى سكون القلب، والأمان والأمانة يأتي بمعنى واحد، وقد آمن من باب فهم وسلم، وآمناً وآمنة، بفتحتين فهو امن، وأمنه والأمن ضد الخوف، وقد يقال الأمن والأمان كصاحب ضد الخائن، أمن كفرح، أمناً وأماناً بفتحهما، وأمناً وأمنةً محركتين، وامناً بالكسر، فهو أمن آمين، كفرح وأمير، ورجل أمنة، كهمزة، يأمنه كل احد في كل شيء[2].

ويقصد به أيضا الثقة والطمأنينة، فهو الأمان والأمانة، وقد أمنت فأنا أمن، أمنت غيري من الامن والأمان، والأمن ضد الخوف والأمانة ضد الخيانة، والمأمن موضع الأمن، والأمن المستجير ليأمن على نفسه، وقد وردا المفهوم في القرآن الكريم قوله تعالى (فليعبدوا رب هذا البيت الذي اطعمهم من جوع وآمنهم من خوف)[3]. ويدل على انه فلانة آمنة، أي يامن كل حدا ويثق به ويأمنه الناس ولا يخافون غائلته (شره)[4].

---

(1) - د. رياض أحمد، وسائل التواصل الاجتماعي ودورها في تعبئة الرأي العام العالمي في الحد من انتشار وباء كورونا ،المجلة الجزائرية للبحوث والإعلام، المجلد 3، العدد 1، 2020، ص 165.

(2) - د. علي هاشم عبدالحسن ، المصدر السابق، ص12 و 13 .

(3) – الآيتين (3-4) سورة قريش.

(4) - ابي القاسم محمود بن عمر الزمخشري، اساس البلاغة، دار الفكر، بيروت، 1979، ص 10.

أما معنى الأسرة لغة: الأسرة من الناحية اللغوية أهل الرجل وعشيرته، والجماعة التي يرتبط بها أمر مشترك، وإن هذا المعنى يدل على النصرة والحماية، والأسرة هي الدرع الحصين، ويقال الأسرة الحصاد والبيض المكلل والرمح وجمعه، أسر، وأسر الهمزة والسين والراء، أصل واحد وقياس مطرد، وهو الحبس، وهو الإمساك، ومن ذلك الأسر، وكانوا يشدونه بالقيد، وهو الإسار، والأسر شدة الخلق، وتعني أيضا بأنها القوة والشدة[1]. لذلك جاء تفسيرها على أنها الدرع الحصين على أساس أن أعضاء الأسرة يشد بعضهم بعضاً ويعدون لبعضهم درعاً[2].

أما تعريف الأمن الأسري إصطلاحاً: فقد أختلفت إتجاهات المفكرين والباحثين ورجال الدراسات في وضع تعريف عام وشامل، يتضمن جوهره وأهدافه وأبعاده، وأنواعه، ومن أهم تلك الأختلافات هو تأثير رؤية كل منهم لزاوية النظر إلى الأمن[3]، وأيضاً إنعكاس التخصصات العلمية والدراسات الأكاديمية في النظر للأمن، فعرف الأمن بأنه (أطمئنان الافراد، وأسرهم والمجتمع في مقابل أن يحيوا حياة طيبة لا يخشون الخوف على الأموال أو الاولاد من أوجه التعدي بلا وجه حق)، ويلاحظ أن هذا التعريف قد ركز على الطمأنينة من الأخطار التي قد تلحق بالأفراد ويركز أيضا انه مقابل الأطمئنان يكون الاستمرار في الحياة، ولم يكن التعريف شاملا. وهناك من يعرف الآمن بأنه (الأطمئنان الذي يوفرها للشخص على نفسه وماله وأهله وكافة حقوقه الإجتماعية والقانونية وغيرها وعدم شعورهم بالخوف الآني أو مستقبلا سواء كان في داخل البلاد أم خارجه)[4]. وأيضا هناك من يعرف الآمن بأنه (الإحساس الذي يتملك الإنسان بأن يتحرر من الخوف أو أي خطر الأخر ممكن أن يواجه ويمنح والشعور والطمأنينة التي تتحقق من خلال ممارسة الدور الوقائي والعلاجي للأفراد)[5]. ومن جانب آخر يعرف الأمن على أنه (الإجراءات الأمنية التي تتخذ من اجل حفظ أسرار الدولة من جانب وتأمين الافراد من جانب آخر من جهة الداخل والخارج وأن الطمأنينة والهدوء والقدرة على مواجهة الأحداث والطوارئ دون اضطراب)[6]. وما يؤخذ على هذا التعريف انه مختصر على الإجراءات الأمنية، في حين أن هناك إجراءات أخرى يمكن أن تتخذ لحفظ الأمن الأسري كالإجراءات التي تقوم بها السلطة

(1) - ابن منظور محمد بن مكرم، المصدر السابق، ص 22.
(2) - د. السعيد بن محمد هراوة، حماية الاسرة في ظل الشريعة الاسلامية والاتفاقيات الدولية، مطبعة سامي، 2022، ص 17.
(3) - د. علي هاشم عبدالحسن ، المصدر السابق، ص12 و 13 .
(4) - د. نور الدين الخادمي، القواعد الفقهية والامن الشامل، المجلة العربية للدراسات الامنية والتدريب، المجلد 21، العدد 42، 2006، ص 21.
(5) - حواسة جمال، دور الاسرة في تحقيق الامن الاجتماعي، بحث منشور، مجلة دراسات ، جامعة 8 ماي 1945 قالمة، الجزائر ، المجلد 7، العدد 3، 2018، ص 138 .
(6) - أمينة دير، أثر التهديدات البيئية على واقع الامن الانساني في افريقيا، رسالة ماجستير، جامعة محمد خيضر، بسكرة، كلية الحقوق والعلوم السياسية، 2014، ص 11.

التشريعية عبر النص على توفير الحماية الجنائية للأمن الأسري. وأيضا هناك من يعرف الأمن على أنه (الإحساس بالاستقرار المتولد في نفوس الافراد والمجتمع تجاه النفس أو المال أو المستقبل والشعور بالاستقلال والتحرر من اي ضغوط أو الاستغلال أو الخوف أو القهر)[1].

ولقد أهتمت أغلب التشريعات المقارنة في تعريف (الأمن الأسري)، ونجد ان دستور جمهورية العراق لعام 2005 اشار في المادة (29/اولا) منه إلى ان: (الأسرة أساس المجتمع وتحافظ الدولة على كيانها وقيمها الدينية والأخلاقية والوطنية). وعلى هذا الأساس فإنه مصطلح الأسرة قد يتسع وقد يضيق وذلك حسب القوانين التي تنظم الأمن الأسري، وعند الرجوع إلى قانون الحماية الاجتماعية العراقي رقم (11) لسنة 2014 ، فالمشرع قد ضيق من معنى الأسرة، إذ أنه شمل الزوج والزوجة أو كلاهما، أو الاولاد، أو لوحدهم حتى الفرد، ويكون أفراد الأسرة في حالة تعدد الزوجات من أسرة واحدة، وأيضا عند وفاة الزوج تشكل كل أرملة اسرة مستقلة بذاتها عن غيرها، في حين يتسع في موضوع آخر كما في مشروع قانون مناهضة العنف الأسري، إذ انه يشمل فضلا عن الذين حددهم كل من الاحفاد أو الأولاد لاحد الزوجين من زوج آخر، وكذلك والدا الزوجين والأخوة والأخوات لكل الزوجين والشخص المشمول بالوصية، أو القيمومة أو الضم، وقد توسع أيضا المشرع العراقي في تعريف الأسرة فعرفها القانون المدني العراقي رقم 40 لسنة 1951 بموجب المادة (38) على أنها: (أسرة الشخص تتكون من ذويه قربائه، ويعد من ذوي القربى من يجمعهم أصل مشترك). وهذا التعريف يراد به المعنى الواسع للإسراء كونها تشمل الازواج والأولاد والآباء والأخوة والأخوات والأعمال والأخوال والأجداد اذ يربط بينهم أصل واحد أو مشترك فقد يكون الأب أو الأم وان علوا، اما تعريف الأسرة في التشريع الأماراتي فقد عرفها المشرع الأماراتي بموجب قانون الضمان الاجتماعي الاتحادي رقم (2) لسنة 2001 في المادة (الأولى) من الباب الأول، بأنها : (مجموعة مكونة من زوج وزوجة أو أكثر وأولادهم وبعض أفراد هذه المجموعة، إذا كانت تجمعهم معيشه واحدة). أما بالنسبة للتشريع المصري فقد أورد مصطلح الأسرة بموجب دستور جمهورية مصر العام 2014 المعدل في المادة (10) على أن الأسرة أساس المجتمع قوامها الدين والأخلاق والوطنية وتحرص الدولة على تماسكها واستقرارها وترسيخ قيمها[2].

أما التعريف الفقهي للأسرة : تعرف الأسرة بأنها: (رابطة اجتماعية تتكون من زوج وزوجه بأطفال أو بلا أطفال، أو قد يكون من زوج بمفرده مع الأطفال، أو قد يكون من زوجة مع الأطفال، وقد يتسع

(1) - د. السعيد بن محمد هراوة، حماية الاسرة في ظل الشريعة الاسلامية والاتفاقيات الدولية، المصدر السابق، ص15.

(2) - د. نادر عبد الكريم غزواني، الحماية الجنائية من جرائم الإنترنت ، دار الجامعة الجديد، من دون سنة نشر، ص60 .

المفهوم ليشمل كلا من الاعمام والأخوال والأجداد والأحفاد وبعض الأقارب أحيانا على أن يكونوا في معيشة واحدة)[1]. وهناك من يعرف الأسرة بأنها: (جماعة تتكون من الازواج والأولاد غير المتزوجين الذين يقيمون في معيشة ومسكن واحدة. ويؤخذ على هذا التعريف أنه قد حصر نطاق الاسرة في الازواج والأولاد)[2]، وهناك من يعرف الأسرة على انها: (تجمع قانوني لأفراد اتحدوا بروابط كالزواج أو القرابة أو روابط التبني، ويشارك بعضهم بعضاً في منزل واحد، يتفاعلون في ما بينهم تفاعل متبادل لبعضهم بعضاً طبقا للأدوار الاجتماعية المحددة)[3]. وهناك من يعرف الأسرة على أنها: (وحدة ثنائية تتكون من رجل وامرأة تربطهم علاقة روحية مرتبطة متماسكة مع أي من الأطفال والأقارب ويكون وجودهم قائماً على دوافع غريزي والمصالح المتبادلة، ذلك الشعور المشترك الذي يتناسب والأفراد)[4]. وأيضا عرفت الأسرة على أنها: (النظام الاجتماعي الذي يحكمه العقل وتتحكم بإرادته ويقرر الفاعل الجامع كون أنها لم تكن نظاماً طبيعياً خاضعا لدوافع تلك الطبيعة، ومقتضيات الغرائز وأنها اهم النظم التي أقامها الإنسان وأوسعها من ناحية الانتشار كونها موجودة في كل مجتمع)[5].

وتأسيساً على ما تقدم نلاحظ هناك علاقة وثيقة بين التفكك الأسري، وعمليات التنشئة الإجتماعية، غير أننا نحاول أن نبرز مفهوم عملية التنشئة، لأن هناك فرقاً بين التفكك الراجع لبنية الأسرة، وهيكلها المادي، والتفكك المعنوي ألراجع لتخلخل العلاقات العائلية وفشل أساليب التربية، والتأكيد بأن التأثير الاكبر على سلوك الطفل خلال عملية التنشئة الاجتماعية يأتي أساسا من التفكك المعنوي أكثر، مما يأتي من التفكك المادي. ويرى بعضهم إلى أن التوتر والصراع يكون موجوداً في الأسرة قبل الانفصال ومن شأن هذا الوضع ان يهدد حياة الأطفال بصورة أخطر من الأنفصال الفعلي، وتشير دراسات (سكوت/ Scott) إلى ان الطفل يمكن أن يلجأ إلى سلسة من الهرب ليتغلب على القلق الذي يثيره الوضع العائلي المليء بالصراع، ونتيجة هذا التوتر العائلي يمكن أن يدفع الطفل إلى الأنضمام لجماعة من المنحرفين هروباً من أسرته، ومن ثم ما يؤدي به إلى تعلم بعض السلوكيات السيئة كارتياد مقاهي الإنترنت بدون علم أولياء أمره، وخاصة في المساء أو بعد أوقات دوام المدارس، ومن ثم يتعلم المزيد من الأفكار السلبية التي قد يتعرض لها المراهق أثناء تصفح الإنترنت مما يؤدي به إلى تعلم بعض

(1) - حواسة جمال، المصدر السابق، ص 139.
(2) - د. علي هاشم عبد الحسن، المصدر السابق ، ص 15 .
(3) - د. مصطفى الخشاب، المدخل إلى علم الاجتماع، مكتبة الانجلو المصرية، القاهرة، 1980، ص 354.
(4) - احسان محمد الحسن، مدخل إلى علم الاجتماع ، بيروت للنشر والطباعة، 1988، ص 188.
(5) - زيدان عبدالباقي، الاسرة والطفولة، مكتبة النهضة المصرية، القاهرة، 1998، ص 95.

أساليب السرقة أو السطو على ممتلكات شخصية، عبر الإنترنت ، وهذا قد يكون بدافع الفضول ثم يتطور الامر إلى ان يصبح مدمناً على إرتكاب مثل هذه الأفعال[1].

وقد أصبحت مواقع التواصل الإجتماعي سلاحاً ذا حدين فهي تقنية من التقنيات الحديثة في عالم التواصل بين الأفراد والمجتمعات، جعلت العالم قرية صغيرة فمن خلاله يتبادل الفرد مع الآخرين المعلومات والآراء والأفكار، ومن أهم ما يميز مواقع التواصل الإجتماعي هو المساحة الواسعة التي تتيحها من حرية للفرد، دون وجود قيود خارجية تتحكم في إستخدامها، ومن ثم كسر الحواجز الإنسانية، والجغرافية، والعمرية، والزمنية[2]، ولكن في الوقت نفسه ومع الإنتشار الهائل في إستخدام شبكات الإنترنت تحولت تلك المواقع إلى وسيلة لإرتكاب الجرائم الإلكترونية على شبكات الإنترنت والتي تتعدد صورها وأشكالها، ولقد جذبت مواقع التواصل الإجتماعي ملايين من الشباب المراهقين وفئات عديدة من المجتمع، في جميع أنحاء العالم، إذ أنها تتيح لهم التواصل مع أصدقائهم، المشاركة في أهتماماتهم وهواياتهم مع بعضهم، من خلال تداول الصور ومقاطع الفيديو أنواع مختلفة من الفنون أيضا أتاحت لهم الأنضمام إلى مجموعات كبيرة تهتم بقضايا معينة الا أنه قد يرجع بعض الشباب إلى استخدام تلك المواقع بشكل سلبي لأسباب عديدة قد تدفعهم لذلك، منها البطالة و تفشي الأمية والفقر وهي أسباب تساعد على نمو الأفكار الشاذة والمتطرفة والعدوانية بداخلهم[3].

وقد صدر في بريطانيا عام (1978) قانون حماية الطفل والذي جرم في المادة (الأولى) منه، قيام أي شخص في ألتقاط أو أن يسمح بالتقاط أو إنتاج أي صور ضوئية غير حقيقية مهينة لطفل وقام بتوزيعها وعرضها. ويقصد بالصورة الضوئية غير الحقيقية حسب المادة (7) من هذا القانون بمعنى أي صورة، سواء أنتجت بواسطة الرسم بالكمبيوتر أو تبدو على أنها كذلك. وفي عام 1994 وضع المشرع البريطاني تعريفاً ضمن الأمر الخاص بالعدالة الجنائية والنظام العام، فيما يخص الصور المخزنة في الكمبيوتر، إذ أضيفت مادة لقانون الطفل عام 1978 وشمل التعديل تجريم البيانات المخزنة على أسطوانة كمبيوتر أو بأي وسيلة إلكترونية أخرى، بحيث يمكن تحويلها إلى صورة ضوئية،[4] والغاية من ذلك التعديل هو مواجهة استخدام برامج الكمبيوتر في تركيب صور وجوه الأطفال على اجساد البالغين أو غيرهم من الصغار. اما المشرع الأمريكي فقد جرم القانون الأمريكي التقاط صور إباحية

(1) - د. سعيد زيوش ، ظاهرة الابتزاز الالكتروني وأساليب الوقاية منها، بحث منشور، مجلة العلوم الاجتماعية، العدد 22، 2017، ص 81.

(2) - د. ياسر محمد عبدالله، م. احمد مصطفى علي، جرائم العنف الاسري وسبل مواجهتها في التشريع العراقي، بحث منشور، مجلة الرافدين للحقوق، المجلد 15، العدد 55، 2012 ، ص 362.

(3) - د. حسنين شفيق ، الاعلام الجديد والجرائم الالكترونية، دار الفكر والفن، مصر، 2015، ص 41.

(4) - د. عبد الفتاح بيومي ، المصدر السابق، ص 238.

للأطفال، أو الإعلان عن هذه الصور وعرضها دون بيان أو تعريف هذه الصور[1]، وعلى ضوء ذلك صدر في عام 1996 تعديلا تشريعيا للقانون الاتحادي في هذا الخصوص، يوسع من نطاق التصوير الإباحي للأطفال والمجرم، وعرف بأنه كل تصوير مرئي يتضمن صورة أو فيلماً أو فيديواً أو رسماً أو صوراً مصطنعة بطريقة الكمبيوتر والمنتجة بوسيلة إلكترونية أو ميكانيكية أو بأي وسيلة أخرى، وذلك لأي سلوك جنسي مباشر في حال[2]:

1- إذا كان إنتاج الصور أو مقاطع الفيديو تقوم على استخدام طفل في وضع جنسي مباشرة.
2- إذا كان هذا التصوير يبدو كما لو كان هناك طفل في وضع جنسي مباشر.
3- إذا كان هو التصوير قد صنع أو عدل ليظهر طفلا في وضع جنسي مباشر.
4- في حال تم إعلان أو توزيع أو دعاية لتصوير إذ يرى أنه ينطوي على صورة طفل في وضع جنسي مباشر.

وجاء هذا التعديل التشريعي في القانون الأمريكي مخالفا لمبادئ الدستور، وقد أكدته محاكم الاستئناف في الولايات المتحدة؛ لأنه يجرم الصور الإلكترونية التي جمعت بطريق الكمبيوتر رغم أنها تخلو من المشاركة الحقيقية للطفل، فضلاً عن عمومية الألفاظ التي إستخدمها المشرع[3].

فالأسرة كونها ذلك المجتمع الصغير الذي يربي الإنسان، وينشأ من خلاله في أول عهده بالحياة في أحضانه، ويتطبع بأطباعه، ويرى الأشياء بعينه وتعرفها بها عن طريق أحكامه وميوله وإتجاهاته من أنه يستحسن ما يراه حسنا، أو يستقبح لك ما يراه قبيحا بحسب رؤيته، وأن الأسرة هي بمثابة المدرسة الأولى في الخير والشر، وأن الأسرة تحمل المسؤولية بما تلقيه على عاتق أفرادها من مهام ولا يستطيعون التهرب منها، ومن كتب الله له نجاح في أن يتحمل التبعات في بناء الأسرة والقيام بمسؤولياتها سيكون راعياً في القيام بتبعات المجتمع الذي سيستضل بظله[4]. إذ البيت هو المصدر الأول الذي يمد الأمة من خلاله بالرجال والنساء وإذا كان هذا المصدر طيبا صافياً خالياً من الشوائب المفسدة كان إمداده خيراً على الأمة، وهذا ما سيؤثر إيجابا من خلال وجود الأفراد الصالحين الذين يصبحون في مجتمع متماسك، وسيكون هناك تعاون ودعاة فضيلة، ونظام مستقر متماسك على أسس وقيم وأخلاق راسخة[5].

(1) - هورال هبه نبيلة، جرائم الانترنت، أطروحة دكتوراه، جامعة ابي بكر بلقايد، الجزائر، 2014، ص144.
(2) - د. عبد الفتاح بيومي ، المصدر السابق، ص 239.
(3) - المصدر نفسه، ص 240.
(4) - د. علي هاشم عبد الحسن ، المصدر السابق، ص 47.
(5) -حسين فريجة، الجرائم الإلكترونية والإنترنت، بحث منشور، مجلة المعلوماتية، العدد 36، 2011،ص7.

وبناء على ما تقدم سنحاول دراسة هذا الموضوع من خلال دراسة الأمن الأسري في التشريع الإسلامي والقانوني للحماية الأسرية.

أولا: أساس الحماية المقررة للآمن الاسري

1- **الأساس التشريعي الإسلامي للحماية الأسرية:** نلاحظ أن الشريعة الإسلامية قد اهتمت بالأمن الأسري، وكذلك ادراك الوضع الخطير في بناء المجتمعات ومن منطلق أن الأسرة في الشريعة الإسلامية ضرورة دينية، وكذلك إجتماعية، وحرصا منها على حماية الأسرة من التفكك والإنحلال فقد أهتمت بأمورها وقررت لها الضوابط والقواعد اللازمة لها، ومن المعروف أن الأسرة هي الحصن الامين لمواجهة الهيمنة الغربية وغيرها، وهذا ما نلاحظه من إصرار المجتمع الدولي على هدم الاسرة وإستئصالها بدعوى مواكبة التطور، أو بحجة الإستجابة لمتغيرات العصر[1]، ولما كانت الأسرة تتألف من الرجل والمرأة، كان على كل منهما أن يحسن اختيار الأخر، فالعلاقة الزوجية في الإسلام اجتماع سكن واستقرار ومودة ورحمة تذكر الآية الكريمة قوله تعالى: (ومن آياته أن خلق لكم من انفسكم أزواجا لتسكنوا إليها وجعل بينكم مودة ورحمة إن في ذلك لآيات لقوم يتفكرون)[2]. وقوله تعالى (هو الذي خلقكم من نفس واحدة وجعل منها زوجها ليسكن إليها فلما تغشها حملت حملا أن خفيفا فمرت به فلما اثقلت دعوا الله ربهما لئن اتيتنا صالحا لنكونن من الشاكرين)[3]. فجعلة في هاتين الآيتين غاية الزواج وعبر عنها بالنفس الواحدة، أن يسكن كل من الزوجين للآخر ويطمئن ويستريح لوجوده ولا تكون حالة السكن هذه وحالة الاطمئنان والراحة في اجتماع أحد بأخر إلا إذا كان هناك انسجام بينهما، واقترب كل منهما نحو الأخذ بمفاهيمه وسلوكه وطريقته في الحياة وعلى ذلك فإن الأسرة بوصفها الصورة المثلى في تأسيس حياة مطمئنة التي تلبي رغبات الإنسان، لأنها الحضن الطبيعي الذي يتولى حماية افراد العائلة الواحدة بوصفها عاملاً مهما للإستقرار النفسي سواء بالنسبة للزوج أم الزوجة أم الاولاد، وهو ما يساعد على الأحتفاظ بالانسجام بين الزوجين وإدامته، هو أن الحقوق والواجبات الزوجية متكافئة ومتعادلة بحسب طبيعة كل منهما للزوج حقوق وواجبات، وللزوجة حقوق وواجبات وكل واحد من هذه الحقوق والواجبات متكافئ ومتعادل مع الآخر، بمعنى أن التكافؤ والتعادل هنا، أن الحياة الزوجية لتصل إلى غايتها وهي السكن والمودة والانسجام اذ لابد من اسهام الرجل والمرأة فيها سواء بسواء، ولا بد من أفاد كلا منهما معا بهذه العلاقة ولا يضار الرجل بالعلاقة الزوجية فيؤدي ما عليه دون مساهمة من المرأة فيها، ولا تضار المرأة فتؤدي ما عليها دون مساهمة الرجل فيها، وهذا التكافؤ في الحقوق والواجبات هو الذي تشير إليه الآيتان الكريمتان في قوله تعالى: (الرجال قوامون

(1) - د. علي هاشم عبد الحسن ، المصدر السابق، ص 48.
(2) - الآية (21) سورة الروم.
(3) - الآية (189) سورة الاعراف.

على النساء بما فضل الله بعضهم على بعض وبما انفقوا من اموالهم)[1]. وقوله تعالى: (والمطلقات يتربصن بأنفسهن ثلاثة قروء ولا يحل لهن أن يكتمن ما خلق الله في ارحامهن إن كن يؤمن بالله واليوم الآخر وبعولتهن أحق بردهن في ذلك أن أرادوا إصلاحا ولهن مثل الذي عليهن)[2]. والمراد بالتماثل في الحقوق والواجبات هو التكافؤ والتعادل بينهما، ولذلك حث القرآن الكريم على حسن العشرة وذلك بقوله تعالى: (يا أيها الذين آمنوا لا يحل لكم أن ترثوا النساء كرها ولا تعضلوهن لتذهبوا ببعض ما اتيتموهن إلا ان يأتين بفاحشة مبينة وعاشروهن.....)[3]. فهذه الآية تبين أن للرجل على المرأة حق الرياسة وواجب النفقة، وعليها أن تطيعه هو تحفظ غيبته، ولقد قال تعالى: (ولا تتمنوا ما فضل الله به بعضكم على بعض للرجال نصيب مما اكتسبوا وللنساء نصيب مما اكتسبن وأسالوا الله من فضله إن الله كان بكل شيء عليما)[4].

ونلاحظ تأثير التطور التكنولوجي قد أدى إلى تزايد حالات الطلاق في كثير من المجتمعات على الصعيد العربي والعالمي، إذ توجد هناك كثير من الحالات الطلاق والتي أدت إلى إنهيار الحياة الأسرية، بسبب الصداقات من خلال البرامج والتطبيقات على الإنترنت، وذلك عندما تكتشف الزوجة أو الزوج هذا النوع من العلاقات المشبوهة، وقد يستمر أحد الزوجين بتلك الصداقات، ويصل الأمر إلى إنهاء العلاقة الزوجية والطلاق، وهذا ما يسبب تفكك للأسرة والمجتمع، مما يؤثر على حياة الأطفال بسبب الإدمان على تلك المواقع والعلاقات غير المشروعة، وهذا ما يؤدي إلى انهيار الحياة الزوجية، وتزعزع الثقة بين أفراد الأسرة[5].

2- **الاساس الدستوري والقانوني لحماية الأمن الاسري:** إن من المبادئ المتفق عليها في معظم النظم الديمقراطية، هو أن يكون الدستور، الوثيقة الرسمية والقانونية العليا في أي دولة، وذلك بحكم كونه يتضمن الأسس القانونية العامة التي تحدد شكل الدولة فيها، ونظام الحكم، فضلا عن تنظيم الدستور لاختصاصات السلطات العامة فيها، وتحديده لحقوق وحريات الأفراد سواء في الإباحة أو التقيد، لذلك فقد كانت مسألة الأمن الأسري في الدساتير العراقية منذ نشأة الدولة العراقية ولغاية الدستور الحالي لعام 2005 محلاً للحماية سواء بنصه على الأمن الأسري بشكل عام أو حماية المرأة من أنواع التميز أو ما يشمله حماية الطفل، وذلك لخلق بيئة ثابتة ومناسبة في المجتمع أساسه الاسرة، وإذ إن الدستور فضلاً عن تنظيمه للمواضيع الأساسية والمهمة في المجتمع، فإنه يتولى أيضا تنظيم موضوع الحقوق

---

(1) - الآية (34) سورة النساء .
(2) - الآية (228) سورة البقرة .
(3) - الآية (19) سورة النساء .
(4) - الآية (32) سورة النساء .
(5) - د. حسنين شفيق ، المصدر السابق ، ص 310.

والحريات الفردية المتعلقة بأمن الأسرة سواء كانت هذه الحقوق شخصية أم سياسية أم اجتماعية أم اقتصادية، ومن أجل احترام هذه الحقوق والحريات الفردية للأسرة لابد من أن يتم أولا النص عليها في أصل الدساتير بوصفه خير ضامن لهذه الحقوق، لأن النص عليها يضمن عدم تجاوز السلطات في الدولة لهذه النصوص الدستورية[1]، وكما هو معلوم أن النصوص الدستورية تتميز بالسمو والعلو على القوانين، ولكي نضمن عدم تجاوز السلطة العامة لصلاحياتها، لابد من تفعيل موضوع الرقابة على دستورية القوانين، كونها عبارة عن وضع قانوني مهمته التحقق في مدى مطابقة القوانين للدستور والأمن الأسري كونه من الحقوق التي يكفلها المشرع[2].

أما فيما يتعلق بدستور جمهورية العراق لسنة 2005 فقد تضمن مجمل الحقوق والحريات بموجب الباب الثاني من الدستور، إذ جاء في الفصل الأول منه بعنوان الحقوق، وكذلك تضمن الفصل الثاني الحريات، وتفرع منه الفصل الأول الحقوق إلى الفرعين فقد تناول في الفرع الأول الحقوق المدنية والسياسية، أما الفرع الثاني، متضمناً الحقوق الأقتصادية، وكذلك الاجتماعية والثقافية، وأكد الدستور في هذا الفصل على مبدأ تكافؤ الفرص، وكذلك أن لكل فرد الحق في الخصوصية الشخصية ويعد هذا باباً آخر يفتحه المشرع لضمان حماية الأسرة وحفظ أمنها من التدخل في الخصوصية الأسرية أو الفردية وبما لا يتنافى مع حقوق الآخرين والآداب العامة، وكذلك تضمن حرمة المساكن لحفظ كيان الأسرة، والحق لكل عراقي في أن يحصل على جنسية. وأكد الدستور أيضاً أن لكل فرد حرية الفكر والمعتقد بما يضمن ذلك امن أسرته[3].

ونجد أن حماية الأمن الأسري في الدساتير المقارنة قد أكدت معظم الدساتير على حماية الأسرة وأفرادها وجعلتها محور المجتمع في ذلك البلد على أساس أنها تمثل نواة المجتمع وعلى أساس المسكن الذي يجتمعون فيه والتعاون الاقتصادي بما فيما بين افراد الأسرة. ونلاحظ ان الدستور المصري الجديد المعدل 2019 قد نص بموجب المواد (17) على أن المجتمع يقوم على أساس التضامن الإجتماعي وأن الدولة هي من تسير أمور رعاياها فتلتزم بتحقيق العدالة الإجتماعية، وتوفير بيئة خصبة للتكافل الإجتماعي التي تضمن الحياة الكريمة لجميع المواطنين، وكذلك جاء في نص المادة (9) منه، أن الدولة تلتزم في تكافؤ الفرص لجميع المواطنين بلا تميز، وتضمنت المادة (10) منه، وصف الأسرة أساس المجتمع التي تتمثل بقوام الدين والأخلاق الوطنية، وأن من واجب الدولة أن تحرص على تماسك الأسرة واستقرارها، وحفظ القيم السائدة فيها، بوصفها تمثل جانبا رئيسياً من ثقافة

(1) - د. علي هاشم عبد الحسن ، المصدر السابق، ص 63.
(2) - إسحاق صلاح ابو طه، الحرية الشخصية في ضوء مراقبة المراسلات والتنصت على المحادثات الهاتفية، بحث منشور ، مجلة البحوث والدراسات العربية، مصر، العدد 53، 2016، ص 74 .
(3) - ينظر المادة (37) من الدستور العراقي لسنة 2005 .

أي مجتمع فعلى أساسها تحدد وتنظم النشاط الإجتماعي لأفراد الأسرة، في كافة المجتمع، وذلك انطلاقا من أن لكل مجتمع من المجتمعات له فلسفته الخاصة في الحفاظ على قيم أفراد الأسرة فالدولة هي التي تحدد تصرفات أفراد الأسرة بشكل عام وترسم وتحدد الأساليب التي تضمن بقائها ودوام تماسكها. وجاء بنص المادة (11) على أن: الدولة تكفل المساواة بين المرأة والرجل في جميع الحقوق سواء المدنية أم السياسية أم الأقتصادية[1]. أما الدستور الإماراتي لعام 1971 المعدل عام (2009) فقد تضمن وكفل حماية الأمن الأسري وايضاً نص على المساواة والعدالة الاجتماعية بموجب أحكام الدستور، وكذلك نص على توفير الأمن والطمأنينة، والتأكيد على مبدأ تكافؤ الفرص لجميع المواطنين بوصفهم أحد أسس الاسرة وانهم دعامات المجتمع، وقد جاء بنص المادة (15) منه أيضا على ان الأسرة أساس المجتمع التي يكون قوامها الدين والأخلاق وكذلك حب الوطن، وأن القانون هو الذي يكفل كيانها ويصونها ويحميها من الانحراف، ولقد جاء بموجب نص المادة (16) من الدستور ذاته، أن المجتمع الذي نواته الأسرة يحظى برعايته الطفولة والأمومة وذوي الاحتياجات الخاصة[2].

ومما تقدم يرى الباحث أن أساس حماية الأمن الأسري التي يكفلها الدستور بوصفها الحياة الخاصة للأفراد، أصبحت في متناول وسائل التطور التكنولوجي والتقني، وكذلك المسموعة، وهذا ما يشكل خطراً على حرمة الأسرة، والحرية الشخصية للفرد سواء داخل نطاقها أم خارجها، وذلك في ما يستدعي إلى وضع تشريعات تواكب التطور والعولمة التي يعيشها العالم في ظل التطور التكنولوجي، وتكفل حماية الأسرة وأمنها، وهذا مما يستلزم تدخل الدولة من اجل ضمان حياة أفضل للأسرة وأفرادها.

أما على صعيد الحماية القانونية ومدى الجهود التشريعية المقررة لحماية الأمن الأسري، فقد سعت أغلب التشريعات الجنائية لحماية الأمن الأسري في ظل التطور التكنولوجي بإصدار مجموعة من التشريعات الجنائية تحت مسميات مختلفة باسم قانون الجرائم المعلوماتية أو قانون الجرائم الإلكترونية، أو ما يصطلح عليه (قانون جرائم المعلومات)، وجميع هذه الجرائم المستحدثة في الوسط التشريعي التي تصيب الاسرة في امنها، الأمر الذي يوجب على المشرع عند إعداد وصياغة أي قانون يتعلق بإحدى هذا الجرائم يتوجب عليه أن يلتفت إلى أختلاف طبيعة هذه الجرائم عن الاجرام التقليدي، وذلك لتعلقها بأساليب حديثة ترتبط بالبيانات الإلكترونية ، والتعديل عليها وما إلى ذلك، وهذا يعني أن

(1) -ينظر: المواد (9 و 10 و 11 و 17) من الدستور المصري المعدل لعام 2019.
(2) - ينظر المواد (15 و 16) من الدستور الاماراتي المعدل عام (2009) .

شبكة المعلومات الإلكترونية هي من ساعدت في ارتفاع مستوى الجرائم التقليدية نحو مستوى آخر غير الذي شهدناه[1].

وعلى ضوء ما تقدم نجد أن المشرع العراقي، قد شرع بكتابة مشروع قانون الجرائم المعلوماتية، ولكن لم يتم التصويت عليه منذ عام 2011، ونجد أن المشرع المصري قد شرع قانون رقم 175 لسنة 2018 تحت عنوان قانون مكافحة جرائم تقنية المعلومات[2]. أما المشرع الاماراتي فقد اصدر القانون الاتحادي رقم (5) لسنة 2012 تحت اسم قانون مكافحة جرائم تقنية المعلومات[3]، وبالرجوع إلى هذا قانون، فقد جرم المشرع الإماراتي بموجب المادة (2) منه، فعل الدخول إلى المواقع ونظم المعلومات بدون تصريح أو تجاوز التصريح أو البقاء بصورة غير مشروعة، وكذلك عاقب في المادة ذاتها إذا نتج عن فعل الجاني إلغاء أو حذف أو تدمير أو إفشاء أو تغيير أو نسخ أو نشر أو إعادة نشر أي بيانات أو معلومات، وقد شدد المشرع الإماراتي فيما لو كانت المعلومات شخصية. وجاء بنص المادة (10) من القانون الإماراتي على أنه: يعاقب بالحبس أو الغرامة أو أحدهما فيما لو كان الفعل الذي نتج عن اختراق البريد الإلكتروني بالرسائل أو إيقافه، لا سيما وأن كثيرا من الأسر لديها بريد إلكتروني خاص تتداول به فالعبث به يكون بطبيعة الحال موجب العقوبة، أما المادة (14) من القانون نفسه فقد جرمت الأفعال التي تنتج على نظم المعلومات فيما يخص التحريض على إرتكاب الجرائم وبهذا وسع المشرع الإماراتي دائرة الحماية للأسرة في مجال الجرائم الإلكترونية، والتي قد ترتكب بواسطة التحريض الإلكتروني، وكذلك جاء بنص المادة (16) فان المشرع جرم فعل الإبتزاز أو التهديد لحمل الغير القيام بفعل أو الإمتناع عنه بواسطة تقنية المعلومات، وقد عاقب المشرع أيضاً على الأفعال المخلة بالآداب العامة في المواد من (17 – 19) من قانون جرائم تقنية المعلومات، الإعتداء على الآداب العامة أو حتى الإخلال بالبيانات في حالة التخزين أو التهيئة أو حتى إعداد للصور أو البيانات أو المعلومات التي من شأنها تمس كيان الأسرة أو أخلاق المجتمع، ويعد في حكم الاخلال بالآداب العامة إستخدام وسائل تقنية المعلومات أو أي وسيلة أخرى من خلال أخذ الصور الإباحية للأطفال سواء عن طريق التصوير المباشر أو عن طريق الترهيب عبر الإنترنت[4].

اما المشرع المصري فقد جرم الإفعال التي ترتكب لمن يستخدم تقنية المعلومات الإلكترونية في مجال الإعتداء على الأمن الأسري وكيانها ، وعلى ضوء ذلك وضع المشرع عقوبات رادعة تحد من إرتكاب الأفعال التي تمس الامن الأسري، وفي مجال الجرائم التي تمثل إعتداء على حرمة الحياة

(1) - د. علي هاشم عبد الحسن ، المصدر السابق، ص 69.
(2) - ينظر قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018 .
(3) - المادة (2) من قانون مكافحة جرائم تقنية المعلومات الاماراتي رقم (5) لسنة 2012.
(4) - ينظر المواد (10 و 14 و 16 و 17 و 19) من قانون الجرائم التقنية والمعلوماتية الاماراتي.

الخاصة نص المشرع المصري في قانون مكافحة جرائم تقنية المعلومات التي تقرر بأنه يعاقب بالحبس لمدة ستة أشهر أو الغرامة أو بإحداهما كل من إعتدى على أي من المبادئ أو القيم الأسرية في المجتمع المصري، أو قد تكون بإنتهاك حرمة الحياة الخاصة أو حتى بإرسال كثير من الرسائل الإلكترونية دون موافقته أو قد تكون عن طريق نشر المعلومات أو أخبار أو حتى صور وما في حكم ذلك[1]. أما فيما يخص جريمة استعمال برنامج معلوماتي أو تقنية معلوماتية في معالجة المعطيات الشخصية للغير وربطها في محتوى مناف للآداب العامة، فقد أشارت المادة (26) من القانون ذاته فإنه: يعاقب مدة لا تقل عن سنتين وغرامة أو أحداهما كل من تعمد استعمال برنامج معلوماتي أو تقنية معلومات في معالجة المعطيات الشخصية للغير أو ربطها بمحتوى مناف للآداب أو بطريقة من شأنها المساس باعتباره أو شرفه[2].

ويجدر بالإشارة إلى أنه قد برزت على شبكة الإنترنت مواقع كثيرة تحرض على ممارسة الجنس، سواء مع البالغين أو مع الأطفال نظرا لكونها حافلة في المواقع التي تدعو إلى الرذيلة، والبغاء، والدعارة، وتقدم خدماتها للجمهور، دون مقابل[3]، وتقوم هذه المواقع بإرسال رسائل إلكترونية للإعلان عن نفسها، وهذه المواقع يمكن القول إلى انها تُعد من أهم الأسباب التي تدفع إلى التفكك الأسري، ومن ثم إلى تزايد الجرائم الأسرية، كما تقوم هذه المواقع بنشر صور جنسية فاضحة للبالغين والأطفال[4]، والجديد بالذكر أن هذه المواقع لا تحرض على الفسق بالإشارة أو القول، وانما تحرض وتدعو إلى ممارسة الأفعال المخلة بالآداب العامة من خلال نشر الصور والأفلام الجنسية. وتأكيدا على خطورة شبكات الإنترنت والتطور التكنولوجي الحديث، على الاخلاق والأسرة، فقد أوضحت الإحصائيات أن حجم مشكلة المواد الإباحية بوجه عام والمواد والأنشطة الجنسية المتصلة بالأطفال والقصر بوجه خاص، يتزايد بشكل غير عادي فوفقا لتقديرات حديثة انه واحد من كل خمسة اشخاص قد تواصل مع أحد المواقع التي تحرض على المواد الجنسية على الإنترنت[5]، وأن واحداً من كل (33) شخصاً تلقى عرضا لأنشطة جنسية بشكل أو بآخر، وان كل واحدٍ من أربعة اشخاص، وصلته مواد واعلانات جنسية، وأن كل واحد من سبعة عشر شخص تلقى تهديدات أو إبتزاز أو غيرها من

(1) - د. علي هاشم عبد الحسن ، المصدر السابق، ص 73.

(2) - قانون جرائم تقنية المعلومات المصري رقم 175 لسنة 2018.

(3) - د. عاطف محمد ابو هربيد، أ. نجوان نبيل، جريمة استغلال الاطفال جنسيا عبر الانترنت، بحث منشور، مجلة الجامعة الاسلامية للدراسات الشرعية والقانونية، المجلد 30، العدد 1، 2022، ص 8.

(4) - د. الحاج علي بدر الدين، بوعكاز خليل، الاستغلال الجنسي عبر شبكة الانترنت، بحث منشور، اصدار المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، برلين، الجزء الاول، 2020 ، ص331.

(5) - الطاهر بن احمد، المسؤولية الجنائية للحق في حرية التعبير والصحافة، أطروحة دكتوراه، جامعة الحاج لخضر باتنة، كلية العلوم الانسانية والاجتماعية، شريعة القانون، 2015 ، ص 111.

المواد المسيئة، وهذه الاحصائية حصلت خلال عام 2000. وانطلاقا من كون شبكة الإنترنت تحتوي على العديد من المواقع الإباحية المحرضة على ممارسة الجنس سواء مع البالغين أو مع الأطفال، فإن هذا الأمر يستوجب على المجتمع الدولي والإقليمي والمحلي مكافحة هذه الظاهرة والحد من انتشارها من خلال تشريع قوانين رادعة ونشر الوعي والثقافة التي ترسخ القيم النبيلة[1].

وبناء على ما تقدم نجد أن أغلب القوانين المقارنة تضمنت تجريم جميع الافعال المخلة بالآداب العامة، والتي تمس الأمن الأسري بواسطة الإستخدام السلبي للتطور التكنولوجي والذي ولد عنه مجموعة كبيرة من الجرائم الإلكترونية، مما يتطلب من المشرع معالجة هذا الخطر الذي يمس الامن الاسري من خلال تشريع نصوص ناجعة تتمثل بالردع العام والخاص وكذلك اتخاذ خطوات استباقية تتمثل بالوقاية قبل وقوع الجريمة الإلكترونية، وهذا الأمر يتطلب دراسة علمية وفنية شاملة من قبل اشخاص وفقهاء متخصصين في مجال الجريمة الإلكترونية.

ثانيا : الركن المادي للجرائم الإلكترونية الماسة بالأمن الأسري

يتمثل الركن المادي في الجرائم الإلكترونية بالسلوك الذي يقوم به المجرم المعلوماتي، ويطلق عليها أيضاً (السلوك المعلوماتي)، ويقصد به ذلك السلوك أو النشاط الذي يقوم به مجرم محترف في مجال التقنية المعلوماتية لإرتكاب الجريمة الإلكترونية[2]. وعلى هذا الأساس يشترط لتحقيق الركن المادي في الجريمة الإلكترونية، وجود سلوك يرتبط بنظام معلوماتي عبر شبكة الويب العالمية (الإنترنت)، عن طريق إستخدام الحاسوب وهذا يتطلب الماماً من قبل الجاني بإستخدام الحاسوب و تقنيات والأتصال بالأنترنت والدخول إلى المواقع وأيضاً فإن النظام المعلوماتي يلعب دوراً رئيسياً ومهماً في أحداث السلوك المعلوماتي الذي يتحقق من خلال إرتكاب الجريمة المعلوماتية ولذلك لا يمكن تصور وقوع الجريمة الالكترونية دون هذا النظام حتى وان كان هذا النظام هاتفاً محمولاً أو أي جهاز تقني أخر[3]، يمكن من خلاله الدخول إلى شبكة الإنترنت ولكن قبل البدء بالسلوك المعلوماتي التقني والذي يمثل الركن المادي للجريمة فلا بد أن يقوم الجاني بعدد من الأعمال التحضيرية.

أما السلوك الإلكتروني المادي فإنه عادة ما يبدأ بالدخول إلى شبكة المعلومات (الإنترنت)، ومن ثم استخدام لوحة المفاتيح والدخول إلى الموقع المراد إستخدامها أو إرتكاب الجريمة من خلالها وذلك بعد معرفة التفاصيل الخاصة بالموقع محل الأحداث من خلال الحصول على أسم المستخدم والرقم السري، لأن الدخول إلى الموقع يأتي في بادئ الأمر بنشاط مادي محسوس يتمثل بالضغط على أحرف لوحة

(1) - د. محمود أحمد طه ، المصدر السابق ، ص 177.
(2) - د. ابراهيم محمود اللبيدي، السلوك الاجرامي في جرائم الإنترنت، اصدارات مركز الاعلام الامني، البحرين، 2013، ص 4.
(3) - لينا محمد الاسدي، المصدر السابق، ص 167.

المفاتيح أو أرقام وينتج عن ذلك أحداث تصرفات مخالفة للقانون عبر هذا السلوك أو النشاط المادي من خلال تحويل تلك الأرقام أو الأحرف إلى بيانات تعالج داخل النظام المعلوماتي لينتج عنه سلوك تقني ذو تأثير يسبب ضرراً أو خسارة للمجنى عليه في الجريمة الإلكترونية[1].

وبناءً على ذلك فإن السلوك المادي في الجرائم الإلكترونية، يتكون من صورتين (سلوك مادي) يتمثل باي طريقه يتم من خلالها إدخال البيانات، كما في استعمال لوحات المفاتيح والضغط على الأزرار سواء اكانت حروفاً أم أرقاماً. و(سلوك تقني) يتمثل بمعالجة البيانات داخل الحاسوب عن طريق وحدة المعالجة المركزية فهذا السلوك التقني يعد مكملاً للسلوك الإجرامي الإلكتروني وبدونها لا تقع الجريمة ومن خلالها يتحول السلوك المادي السابق إلى ذبذبات كهرومغناطيسية يتأثر بها الموقع المراد الدخول إليه ويستقبل الأخير هذه الإشارات التي يتم من خلالها إرتكاب الجريمة[2]، أما الجريمة الإلكترونية فلا يكفي إحداث السلوك المادي المتمثل بالسلوك الملموس الذي يتم من خلاله إدخال البيانات وإستخدامها بواسطة النظام المعلوماتي والحاسب الآلي، وإنما لابد أن يقترن به سلوك تقني إلكتروني حتى يكتمل السلوك الإجرامي للجريمة الإلكترونية، من هنا نتوصل إلى أن السلوك المعلوماتي في الجريمة الإلكترونية هو سلوك مزدوج مادي وتقني بوصفه أحد عناصر الركن المادي في الجريمة الإلكترونية الحديثة [3].

وخلاصة القول ان الركن المادي يتحقق في جريمة الأمن الأسري، بعد أن يتم نشر أي محتوى غير أخلاقي أو محتوى مخالف للآداب العامة، أو محتوى يهدد القيم الغجتماعية، عن طريق المواقع الإلكترونية وبرامج التواصل الإجتماعي، دون مراعاة ضوابط النشر.

أما النتيجة في الجريمة الإلكترونية، فهي تلعب دوراً مهماً في تحقق هذه الجرائم، فالنتيجة هي الضرر أو الخسارة التي تترتب على السلوك الإجرامي الإلكتروني بشقيه المادي والتقني، فالنتيجة في الجرائم الإلكترونية تكون ذات مدلولين (الأول) المظهر المادية بمعنى هي الآثار المادية الملموس الناتجة عن السلوك في الجريمة الإلكترونية التي حدثت على أرض الواقع كما في سرقة المال المعلوماتي من

(1) - خالد رمضان عبدالعال سلطان، المسؤولية الجنائية عن جرائم الصحافة، دار النهضة العربية، القاهرة، 2002، ص 277.

(2) - **د.** محمود أحمد طه، المصدر السابق ، ص 185 ، وكذلك : د. عاطف محمد ابو هربيد، أ. نجوان نبيل، جريمة استغلال الاطفال جنسيا عبر الانترنت، المصدر السابق، ص 14 و 15.

(3) - آمين أعزان ، الحماية الجنائية للتجارة الالكترونية، أطروحة دكتوراه، جامعة عين شمس، كلية الحقوق، 2011، ص 127 .

صاحبة دون رضاه، فالقانون أخذ بنظر الإعتبار المصلحة العامة ووفر لها الحماية الكافية لمنع وقوع أي إعتداء عليها أو إنتهاكها[1].

وتأسيسا على ما تقدم فإن القانون يتطلب نتيجة معينة في الجريمة الإلكترونية، وغالبا ما يتم مثل ذلك بأحداث أضرار في الأموال أو النفس أو البيانات المخزنة في أنظمة الحاسب الآلي. (الامر الثاني) المظهر القانوني ويتمثل بالمساس بالحق الذي خصص له القانون الحماية، كما في حالة المساس بحقوق الأفراد وخصوصياتهم، من خلال الأطلاع على الرسائل الموجودة في البريد الإلكتروني لأن نتيجة الاخيرة لا تتحقق إلا إذا وجد نص صريح في القانون يعاقب على الافعال التي تقع في ظل الاتصالات والأعمال الإلكترونية التقنية، أما في حالة إنعدام النص القانوني الذي ينظم الأفعال الإلكترونية، فلا يترتب على الفعل أو السلوك المرتكب نتيجة قانونية وإنما سنكون أمام سلوك غير معاقب عليه ولا يوجد عليه جزاء[2].

ثالثا : الركن المعنوي للجرائم الإلكترونية الماسة بالأمن الأسري

الركن المعنوي هو الحالة النفسية للجاني والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني، وبصورة عامة أن الجرائم الإلكترونية من الجرائم العمدية التي يتوفر لها القصد الجرمي لألحاق الاذى والخسارة بالمجنى عليه، سواء كان ذلك في النفس أو المال أو البيانات المخزنة في ذاكرة الحاسوب وغيرها وعلى هذا الأساس لابد أن يتوافر القصد الجنائي للجريمة الالكترونية من قبل الجاني، أي توافر العلم والإرادة[3]. ونجد أن المشرع العراقي قد اشترط لقيام الجريمة العمدية إلى تحقق الركن المعنوي فيها، وذلك من خلال تحقق نص المادتين (33 و 34) من قانون العقوبات العراقي رقم (111) لسنة 1969المعدل، وعلى هذا الأساس إذا كانت الجريمة الإلكترونية من الجرائم العمدية، يتعين أن يكون لدى مرتكبها القصد الجرمي الذي يقوم على العلم والإرادة، وفي حال اذا اتجهت إرادة الجاني إلى ارتكاب الجريمة عالما بمضمون نشاطه الإجرامي قام لديه هذا القصد وتحققت المسؤولية الجزائية عما قام به من نشاط[4].

---

(1) - د. سليمان عبدالله، شرح قانون العقوبات، القسم العام، الجزء الاول، دار المطبوعات الجامعية، 2005، ص105.

(2) - خليل سعيد خليل، القالب التشريعي لجرائم انتحال الصفة والشخصية الالكترونية، بحث منشور، مجلة العلوم الانسانية والادارية، العدد 22، 2021، ص 91.

(3) - د. محمود نجيب حسني، النظرية العامة للقصد الجنائي، دار النهضة العربية، القاهرة، 1988، ص 49 وما بعدها. كذلك ينظر : د. احمد عادل عبدالله المعمري، المسؤولية الجنائية عن سوء استخدام حرية التعبير الصحفي، وزارة الداخلية، قيادة شرطة الشارقة، ادارة مركز بحوث الشرطة، 2017، ص 228.

(4) - لينا محمد ، المصدر السابق، ص 164.

فالركن المعنوي للجرائم الإلكترونية يختلف من جريمة إلى أخرى، مثال على ذلك في جريمة تهديد الأمن الاسري، لابد من اتجاه إرادة الجاني إلاّ أنه على علم بأنه يقوم بنشر محتوى مخالف للنظام والآداب العامة، وإن إرادته متجهة لتحقيق غاية أو غرض عن طريق نشر هذا المحتوى، سواء بالإبتزاز أم القذف غير المشروع أو نشر مواد إباحية، بمعنى لابد أن يتوافر القصد في هذه الجريمة لكي يتحقق الركن المعنوي للجريمة (العمدية)، كما لا يتوفر القصد الجرمي إذا كان الشخص قد إرتكب فعلا عن طريق الخطأ أو أنه كان يعتقد بأن ما قام به فعل مسموح به[1].

وبناء على ما تقدم فإن القصد الجرمي هو ركن أساس ومهم في نطاق الجريمة الإلكترونية، لأن أغلب الدول التي قامت بتشريع قانون خاص بالجرائم الإلكترونية ولم تشر إلى توافر القصد الخاص في إطار الركن المعنوي في الجريمة الإلكترونية، وانما اكتفت بأن يكون الفعل عمدياً. فالركن المعنوي وأن كان يختلف من جريمة إلى أخرى في إطار الجرائم الإلكترونية، إلا أنه يجتمع بخصيصه واحدة، وهو صعوبة إثبات القصد الجرمي في الجرائم الإلكترونية، بسبب يعود إلى طبيعة الأنشطة التي يتعرض لها النظام الإلكتروني بإعتبار هذه الأنشطة غير مادية وغالباً لا تترك آثاراً بعد إرتكابها فهي عبارة عن نبضات إلكترونية منتشرة في الشبكات أو المواقع الإلكترونية إلا أن إثبات القصد الجرمي هي مسألة موضوعية ترجع إلى تقدير محكمة الموضوع، ويتم التوصل إليها عن طريق الأدلة التي يتم الحصول عليها[2].

رابعا : الركن الشرعي للجرائم الالكترونية الماسة بالأمن الاسري

يقصد به الفعل الذي يرتكبه الجاني لا بد أن يخضع لأحد نصوص التجريم الواردة في أي نص تجريمي في القانون، ومن ثم فإن هذا الفعل غير مشروع، ويخضع الجاني للجزاء والعقاب الذي أوردة النص الجنائي، وقد اتجه أغلب فقهاء القانون الجنائي إلى ضرورة وضع النصوص العقابية التي يجرم المشرع من خلالها الأفعال والإنتهاكات التي تقع على المعلومات[3]. فمبدأ الشرعية الجنائية يمنع محاسبة اي شخص جنائيا، ما لم يتوفر النص القانوني، فلا جريمة ولا عقوبة الا بنص، ومتى انتفى النص القانوني الذي يجرم اي فعل، فإن المسؤولية الجنائية تنتفي[4]، وقد يثار سؤال في غاية الأهمية، وهو مدى انطباق النصوص الجنائية التقليدية على الجرائم الإلكترونية؟ وللإجابة على هذا السؤال

(1) - حفصي عباس، جرائم التزوير الالكترونية، اطروحة دكتوراه، جامعة وهران ، احمد بن بلة، كلية العلوم الانسانية والعلوم الاسلامية، الجزائر، 2015، ص 78.

(2) - د. علي هاشم عبد الحسن، المصدر السابق، ص 98.

(3) - د. طالب محمد جواد، د. عبدالجبار ضاحي، جرائم تقنية المعلومات واثباتها، بحث منشور، مجلة كلية الرافدين الجامعة، العدد 28، 2013 ، ص 60 .

(4) - د. تيانتي مريم، ورقة عمل بعنوان، الجريمة الالكترونية بين القيام والتجريم، اصدار المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، برلين، الجزء الاول، 2020 ، ص 43.

يتوجب علينا ان نبين مدى تطبيق مبدأ الشرعية على الجرائم الإلكترونية، حيث إن أغلب التشريعات الجنائية الدولية والإقليمية والمحلية حاولت مكافحة هذه الجرائم الناشئة عن التطور التكنولوجي، من خلال تطبيق القوانين العقابية التقليدية[1]، أو تشريع قوانين اخرى لمواكبة هذا التطور وما نتج عنه من جرائم، إلا أن هذه القوانين التقليدية لم تستطع أن تواجهه هذه الجرائم الإلكترونية، وذلك لاختلاف طبيعتها من حيث التحضير والافعال التي تمتاز بكونها سهلة الإرتكاب عن بعد وسهولة إخفاء الدليل ولا تحتاج لأي جهد بدني، أو أدوات كما في الجرائم العادية، فالحاجة لتدخل المشرع الجنائي لمواجهة ومكافحة الجرائم الإلكترونية، ضرورة ملحة وعلى جميع المشرعين أن يعوا مدى خطورة هذه الجرائم على استقرار الدول من الناحية الإجتماعية والسياسية والأقتصادية والدولية[2].

الفرع الثاني

جرائم الدخول غير القانوني للنظام الإلكتروني

يمكن وصف شبكة الإنترنت على أنها خزان معلوماتي له أبعاد ثلاثة، وهي سرية المعلومات وسلامتها ووجودها، وهذا ما يستوجب تأمين على المعلومات المتنقلة في العالم الافتراضي، فيكون من الأهمية إعادة النظر في مفهوم الأمن ذاته، من النظرة التقليدية أو المرادفة لمكافحة الجريمة، إلى مقاربات تخص التطوير التقني والرقي التكنولوجي لحل عقد الجرائم المتفشية عبر الفضاء الإلكتروني[3]، وإذ إن التطور المعلوماتي والتكنولوجي له مظهر راقٍ للدول ويدخل ضمن سياستها التخطيطية في المعالجات الذكية للجرائم المنبثقة عنها، سواء في المعاملات الأقتصادية أو ما يتعلق بالجانبين الأمني والسياسي، لعوامل لها شأن بالتدفق السريع للمعلومات، وخرق قواعد الزمن والمسافة الأمر الذي يسرع من أختراق الحدود الأمنية للدول، ويشجع على بذل الجهود في توحيد السيادة القومية لمكافحة الإرهاب والجرائم الإلكترونية في العالم الافتراضي[4].

([1])- ينظر: قرار محكمة استئناف بغداد/ الرصافة الاتحادية/ الهيأة التمييزية الجزائية المرقم (807/جزاء/2018 أعلام / 696) والذي تضمن نقض قرار محكمة الاستئناف، وكان مضمون الدعوى هو ارسال صور فاضحة من قبل المتهمة الى المتهم، وقد قررت محكمة التمييز نقض القرار واعادة التحقيق وفق المادة (400) من قانون العقوبات العراقي، وفي حقيقة الامر فان قرار محكمة التمييز كان مبنيا على الاستدلال والاجتهاد لمواجهة النقص التشريعي بسبب عدم اقرار قانون الجرائم الالكترونية والمعلوماتية العراقي.

(2) - د. محمد ممدوح بدير، المصدر السابق، ص 91.

(3) - خالد مشتهى، الجرائم الالكترونية المؤثرة على امن الدولة، رسالة ماجستير، جامعة جندوبة، كلية العلوم القانونية والاقتصادية، تونس، 2021، ص 93.

(4) - د. زورال معزوزة، الإرهاب الإلكتروني نمط الأمن المعلوماتي الجرائم المعلوماتية وأثرها على التنمية الاقتصادية، ورقة عمل، ضمن اعمال المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، بعنوان ، الجريمة المعلوماتية وأثرها على التنمية الاقتصادية، الجزء الاول، برلين، 2020 ، ص307.

ونلاحظ أن التطور السريع في حرية الوصول إلى تسهيلات الإنترنت بطريقة غير منتظمة لذلك الميدان من الأتصالات الدولية، قد أثارت أهتماماً بإمكانية إستخدام شبكات الإنترنت والتكنولوجيا الحديثة بواسطة مهربي المخدرات في تعزيز نشاطاتهم الإجرامية، وأن إستغلال المنظمات الإجرامية للفرص المتاحة من خلال الإنترنت في الواقع غير مختلفة عن غيرها من العديد من الفرص كنتيجة للتدابير من أجل تسهيل القيود على التجارة الدولية والنقل والاتصالات[1]، ومما لا شك فيه أن الإنترنت قوة كامنة في تقديم حرية وصول معلومات دقيقة، ولما كان المجرمون بطبيعتهم سريعين إلى إستغلال أية فرصة تبدو لهم وكانت خدمة الإنترنت قد سهلت العمليات الاجرامية في هذا المجال بشكل كبير، وهناك بعض المواقع الخاصة بالترويج للمخدرات، تستغل بوضوح على سبيل المثال، في نشر صيغ أو تصنيع المخدرات لا سيما أنواع الأمفيتامينات والمنشطات وهي حاليا متوفرة على شبكات الإنترنت، كما أن بعض مواقع الإنترنت تقدم تفاصيل لمصادر توفر المواد الكيميائية وعن الادوات المخبرية المطلوبة لتصنيع المخدرات، كما أن تلك المواقع تسلط الضوء على المصنعين لتلك المواد المخدرة، والذين هم على استعداد لتلقي طلبات المجرمين أو أولئك الموجودين في دول قوانينها وانظمتها لا ترقى إلى معايير دولية لمراقبة انتشار جرائم المخدرات، وهناك مواقع أخرى يمكن أن تستغل تسهيلات الإنترنت الموجودة في تسويق المواد التي تستخدم في إنتاج مادة الحشيش، لا سيما ذلك النوع الذي يحتوي على نسبة عالية من المادة الفعالة (thc) والذي يمكن إنتاجه داخل البيوت الزجاجية بواسطة أساليب وتقنيات الزراعة المائية[2].

ويُعدّ الحاسب الآلي والشبكات المعلوماتية قد أصبحت مستودعاً لكثير من الأسرار البشر مما جعل منها هدفا ومطمعاً لكثير من مجرمي التقنية الإلكترونية، أو المتطفلين الفضوليين الذين يجدون المتعة في إختراق النظام المعلوماتية والأطلاع على ما يحتويه من أسرار والعبث بها، وعلى الرغم من ان التقدم والتطور التكنولوجي والتقني السريع في مجال التكنولوجيا ووسائل الإتصالات يمثل إنعكاسات إيجابية على مختلف جوانب حياة المجتمعات، إلا أنه في الوقت ذاته ونتيجة لإساءة استغلاله من قبل بعضهم، أصبح يشكل تهديداً خطيراً لخصوصية الافراد وأسرار الدول والمؤسسات والشركات، وسهل التطور مهمة المجرم الإلكتروني، وساعد على زيادة قدراتهم في الوصول إلى المعلومات المخزنة إلكترونياً والاطلاع عليها والعبث بها وإفشائها، وزاد من قدرتهم على التخفي ومحو آثار جرائمهم على نحو

(1) - يوسف بو غرارة، الامن السيبراني (الاستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبراني)، بحث منشور، مجلة الدراسات الافريقية وحوض النيل، المركز الديمقراطي العربي، العدد 3، 2018، مصر، ص107.

(2) - سامي حارب المنذري، موسوعة العلوم الجنائية (تقنية الحصول على الاثار والادلة المادية)، الجزء الاول، مركز بحوث الشرطة، الشارقة، 2021، ص 470.

يصعب معه ضبطهم[1]. ومن ثم تمكنهم من الإفلات من القانون والعقاب، ومما يزيد من خطورة فعل الدخول غير القانوني، انه قد يتسبب في خسائر مادية ومعنوية كبيرة للمجنى عليه، وخاصة إذا كان الموقع الإلكتروني أو النظام المعلوماتي يعود إلى احد البنوك أو المؤسسات المالية الحكومية والشركات الخاصة، ومن الأمثلة_ قضية (الجحيم العالمي global hell) وملخص هذه القضية هو قيام مجموعة من الأشخاص باختراق موقع البيت الأبيض والشركة الفدرالية الأمريكية والجيش الأمريكي ووزارة الداخلية الامريكية، وتم ادانة اثنين من أفراد هذه المجموعة، وظهر بعد التحقيقات أن الدافع وراء إرتكاب هذه المجموعة لجريمتهم هو مجرد الإختراق اكثر من التدمير أو التقاط المعلومات، وقد تطلب الوصول إلى هذه المجموعة وقتاً طويلاً بين ملاحقتهم وتتبع آثار أنشطتهم، وكلف التحقيق في هذه القضية مبالغ كبيرة نظراً لما تطلبه من وسائل معقدة في المتابعة[2].

وعلى ضوء ذلك فقد حرصت كثير من الدول على تجريم أفعال الدخول غير القانوني للنظام الإلكتروني والتقني، بموجب تشريعاتها الجزائية، فضلاً عن الاتفاقيات الدولية والإقليمية المتعلقة بالجرائم إلكترونية. ومن هنا برز مفهوم الأمن الإلكتروني يثير مخاوف الدول في سياساتها الأمنية، كأحد المتطلبات والعناصر الضرورية المتكاملة في منظومة الأمن القومي[3].

فالأمن الإلكتروني أصبح ضرورة قومية، وواجب على جميع دول العالم إدراجها ضمن سياساتها العامة، وذلك من خلال وضع سياسة أمنية عامة تتضمن الأمن الوطني العسكرية والأمن الوطني السياسي والأمن الوطني للجهاز الإداري الحكومي، والأمن الوطني الاقتصادي، بالإضافة إلى الأمن الوطني الفكري، والثقافي، والإعلامي وغيرها من المجالات التي تمثل السياسة العامة للدولة[4]. ويقصد بالأمن الإلكتروني (تأمين وحماية) الشبكة المعلوماتية والنظام الإلكتروني بصورة عامة، وعمليات جمع المعلومات، بإستخدام أي وسيلة من الوسائل الإلكترونية[5].

ونلاحظ أن المشرع الفرنسي حاول توفير الحماية اللازمة للبيانات والمعلومات الإلكترونية من خلال تشريع نصوص في قانون العقوبات الفرنسي الجديد، إذ تضمنت المادة (323-3) توفير الحماية اللازمة للمعلومات والنظام الالكتروني من كل صور الإعتداء عليها، سواء بالمحو أو التعديل، أو

(1) محمد كمال محمود ، المصدر السابق، ص 55.

(2) - صباح كزيز ، د. سمير قط، أثر الجرائم الإلكترونية على من واستقرار الدول، قرصنة الموقع الإلكتروني لوكالة الأنباء القطرية نموذجا ، مجلة الناقد للدراسات السياسية، العدد الثالث، 2018، ص 124.

(3) - د. هيام محمد الهادي، بحث منشور بعنوان، تعرض المراهقين للجرائم الالكترونية عبر وسائل الاعلام الرقمي وتأثيرها على ادراكهم للأمن الاجتماعي المصري، المجلة العربية لبحوث الاعلام والاتصال، العدد 30، يوليو، 2020، ص 856.

(4) - د. أميل جبار عاشور ، بحث منشور بعنوان، المسؤولية الجنائية عن جريمة الابتزاز الالكتروني في مواقع التواصل الاجتماعي، مجلة أبحاث ميسان، المجلد السادس عشر، العدد 31، حزيران، 2020 ،ص126.

(5) - د. حازم حسن الجمل، المصدر السابق، ص 10.

ادخال معلومات داخل النظام بطريقة غير مشروعة. فالمادة المذكورة أعلاه، عاقبت كل شخص يقوم غشاً بإدخال بيانات في نظام للمعالجة الآلية للمعلومات، أو حذف أو تعديل (غشا) لمعطيات يتضمنها هذا النظام، وقد حددت هذه المادة العقوبة بالسجن لمدة خمس سنوات وغرامة مقدارها (75000) الف يورو، وكما هو الحال بالنسبة للجريمة المنصوص عليها في المادة (323-1) والمادة (323-2) فأن الجريمة المنصوص عليها في المادة (323-3) تُعد من الجرائم العمدية التي تقوم بالقصد الجرمي العام إذ يتعين أن يعلم الجاني بطبيعة نشاطه وأن تتجه إرادته إلى إدخال أو إلغاء أو التعديل للبيانات وأن يعلم أنه يعتدي على حقوق الغير بمقتضى هذا الفعل[1]. وأيضا تضمنت الفقرة الاولى من المادة (9/432): على معاقبة كل شخص عام مكلف بخدمة عامة بالحبس مدة ثلاث سنوات وغرامة (300,000) فرنك، إذا قام عنده مباشرته لعمله وما بمناسبته بالأمر أو التسهيل أو القيام في غير الحالات المقررة قانونا باختلاس أو إلغاء أو فض المراسلات أو كشف محتواها. كما نصت المادة ذاتها في الفقرة الثانية: على معاقبة كل شخص أو مكلف بخدمة عامة أو بأعمال استغلال خدمة الاتصالات بموجب المادة (23-1 من قانون البريد أو الاتصالات) أو بأعمال تقديم خدمة الأتصالات بالحبس مدة ثلاث سنوات وغرامة (300000) فرنك، إذا قام عند مباشرته لعمله أو بمناسبته بالإمر أو التسهيل أو القيام في غير الحالات المقررة قانونا، بالتقاط أو اختلاس مراسلات تتم أو تنقل أو تحمل بطريق الاتصالات وكذلك بإستعمال أو فض محتواها. ونلاحظ أن المشرع الفرنسي قد نص في المادة (9/432) من قانون العقوبات الفرنسي الجديد، على جريمتين مختلفتين في الفقرة الأولى والثانية من المادة أعلاه، فقد عالجت الفقرة (الأولى) حالة الإعتداء على المراسلات بالمعنى الضيق، أما الفقرة (الثانية) فإنها تتعلق المراسلات عبر خدمة الاتصالات بمستوى أن تكون سمعية عن طريق الهاتف على سبيل مثال) أو بصرية كالإنترنت أو مكتوبة في الفاكس ومن ثم لا تقتصر الحماية على المراسلات الهاتفية التي تتم عبر شبكة الإنترنت، ولهذا يرى جانب من الفقه الجنائي أن هذه النص ينصرف إلى المراسلات الخاصة أو المراسلات التي تتعلق بنظام معالجة البيانات في الحكومة أو القطاع الخاص التي تتم عبر البريد الإلكتروني، كما أن هذه الحماية ليست قاصرة فقط على البيانات الخاصة بل تمتد كذلك إلى أي بيانات أخرى، ولو لم تكون سرية[2] .

أما اتفاقية بودابست لسنة(2001) تضمنت بنص المادة (2) من الإتفاقية المتعلقة بالجريمة الإلكترونية على أنه: (يجب على كل طرف أن يتبنى الإجراءات التشريعية أو إجراءات أخرى يرى أنها ضرورية من أجل غعتبارها جريمة جنائية وفقا لقانونه الداخلي للولوج العمدي لكل أو لجزء من جهاز الحاسب الآلي بدون حق، كما يمكن له أن يشترط أن ترتكب الجريمة من خلال إنتهاك إجراءات

(1) - آمين أعزان ، المصدر السابق ، ص 107.
(2) - ينظر: د. عبد الفتاح بيومي ، المصدر السابق، ص 171 وما بعدها.

الأمن بنية الحصول على بيانات الحاسب أو أية نية اجرامية أخرى، أو أن ترتكب الجريمة في حاسب آلي يكون متصلا عن بعد بحاسب آخر)[1].

ومما تقدم نجد أن إتفاقية بودابست لم تفرض اسلوباً محددا لتجريم الدخول غير القانوني وإنما فسحت المجال أمام الدول الموقعة على الإتفاقية ان تتبنى ما تراه مناسبا من إجراءات لتجريم هذه الأفعال، وفي تحديد محل الدخول غير القانوني، سواء لكل أو لجزء من نظام الحاسب الآلي وسواء كان النظام المعلوماتي متصلاً بشبكات الإتصال، أو متصلاً بذات الشبكة، أي شبكة محلية أو دولية أو أي شبكة خاصة لشركة أو مؤسسة.

ونلاحظ أن بعض التشريعات العربية ومنها قانون مكافحة جرائم تقنية المعلومات العماني لسنة 2011 وقانون مكافحة جرائم تقنية المعلومات الإماراتي لسنة 2012 المعدل، وكذلك قانون العقوبات الجزائري المادة (394)، وبعض التشريعات الأخرى، إشترطت لتحقق جريمة الدخول غير القانوني للنظام المعلوماتي، هو أن يتحقق الوصول إلى المعلومات التي يتضمنها النظام المعلوماتي والمراد الوصول اليها. ومثال على ذلك القانون الفيدرالي الأمريكي لجرائم الحاسبات الآلية المادة (103/ a / الفقرة 1 و 2) وهذه المواد تتضمن عدم العقاب على الدخول المجرد إلى النظام المعلومات بل يتطلب الحصول على المعلومات، إلا أنه يجرم في المادة نفسها الفقرة (3) مجرد الدخول بالنسبة للحاسبات الآلية التي تعمل داخل الحكومة الفدرالية أو تلك التي لا تعمل داخل الحكومة ولكن من شان الدخول غير القانوني إليها التأثير على مصالح الحكومة التي ترتبط بأي صورة بتلك الحواسيب[2].

ومن خلال ملاحظتنا للتشريعات العربية نلاحظ أن نظام مكافحة الجرائم المعلوماتية السعودي لسنة 2007 أخذ بالاتجاه ذاته، إذ جرم الدخول غير القانوني بالمواد (3 – 5 – 7) إلى انه: إشترط أن يكون الدخول غير القانوني لتهديد شخص، أو ابتزازه، لحملة على القيام بفعل أو الامتناع عنه، أو الدخول غير القانوني إلى موقع إلكتروني أو الدخول إلى موقع الكتروني لتغيير تصاميم هذه المواقع أو إتلافه أو تعديله، أو شغل عنوانه بالإضافة إلى الدخول غير المشروع لإلغاء بيانات خاصة أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها، أو تغييرها، أو إعادة نشرها....[3]"

وهناك من يذهب مع الاتجاه الذي يجرم مجرد فعل الدخول غير القانوني والمعاقبة على هذا الفعل، بغض النظر عن وصول المجرم للمعلومات أو البرامج من عدمه، ونؤيد تشديد العقوبة تبعا لطبيعة النظام المعلوماتي والمعلومات التي يحتوي عليها الحاسب الالي، وطبيعة العلاقة بين المجرم والنظام

(1) - ينظر المادة (2) من اتفاقية بودابست المتعلقة بالجريمة الالكترونية. وكذلك ينظر: د. محمد كمال محمود دسوقي ، المصدر السابق، ص 61.

(2) - د. ياسمين بو نعارة الجريمة ، المصدر السابق، ص 292 .

(3) - ينظر: المواد (3 و 5 و 7) من نظام مكافحة الجرائم المعلوماتية السعودي لسنة 2007.

المعلوماتي، ذلك أن مجرد الدخول غير القانوني يعد انتهاكا لحق الغير في خصوصياته المعلوماتية ،كما يُعدّ الشرارة الأولى لإرتكاب الجرائم المعلوماتية، فضلاً عما يترتب عليه من خسائر مادية ومعنوية كبيرة للمجنى عليه نظراً لما يتطلبه وقف هذا الدخول لجهود ونفقات مالية[1].

وعلى ضوء ذلك فانه يسأل جنائياً المهنيون المختصون في خدمة الإنترنت متى أسند إلى أي منهم القيام بنشاط يندرج ضمن الركن المادي لجريمة التنصت على المراسلات والمنصوص عليها في الفقرة الثانية، أي أنه يسأل متعهدي الوصول لخدمة الإنترنت ومتعهدي الإيواء لهذه الخدمة، وكذلك المنتج وناقل المعلومات ومورد المعلومات ومتعهد الخدمات، ومؤلف الرسالة بالإضافة إلى مسؤولية مستخدمي الشبكة ما نسب إليهم إرتكاب الجريمة المذكورة [2].

ويقصد بالدخول غير القانوني للنظام الالكتروني بأنه: (الولوج غير المصرح به أو الدخول بشكل غير مشروع إلى نظام معالجة البيانات بإستخدام الحاسوب إذ يتحقق الدخول غير المشروع إلى نظام المعلومات للوصول إلى المعلومات والبيانات المخزنة داخل النظام المعلوماتي وبدون رضا من المسؤول عن هذا النظام التي يحتوي عليها)، وقد عرف نظام مكافحة الجرائم المعلوماتية السعودي لسنة 2007 في المادة (الأولى) منه الدخول غير المشروع بأنه: (دخول شخص بطريقة متعمدة إلى حاسب الآلي أو موقع إلكتروني أو نظام الالكتروني، أو شبكة الحاسب الآلي غير مصرح لذلك الشخص بالدخول إليها). ويرى آخرون بأن الدخول غير القانوني هو قيام شخص غير مرخص له بإساءة استخدام الحاسب الآلي، أو نظامه، أو الدخول إليه بقصد الوصول إلى المعلومات والبيانات التي يحتويها الحاسب الآلي بهدف الاطلاع عليها، أو لأثبات القدرة على إختراق نظام الحماية الإلكتروني، أو لأي سبب آخر)[3].

ويرى الباحث أن جرائم الإعتداء على الدخول غير القانوني للنظام الإلكتروني، هي مجموعة الجرائم التي تمس النظام الإلكتروني والبيانات الخاصة لجهاز الحاسوب والاجهزة التقنية الحديثة وغيرها من الاجهزة، سواء كانت ترتبط بشبكات الإنترنت ام لا، فالأمن الإلكتروني يتعلق بكل جهاز أو بيانات

(1) - د. ماشاءالله الزوي، الجرائم الالكترونية، بحث مقدم ضمن اعمال المؤتمر الدولي الرابع عشر، بعنوان، المواجهة الجنائية للبريد الالكتروني العدائي المزعج او المضلل، مارس، 2017 ، ص 20.

(2) - د. سحر عبد السميع ، المصدر السابق، ص 126 .

(3) - د. محمود أحمد طه، المصدر السابق ، ص 21 . وكذلك: د. خالد ممدوح ابراهيم، أمن الجريمة الإلكترونية، الدار الجامعية ، الاسكندرية، 2008، ص 84.

الإلكترونية خاصة ام حكومية، فهذه الأجهزة والبيانات لها خصوصية ويجب على المشرع أن يحيطها بنظام حماية[1].

ويؤكد الباحث إلى ضرورة أن يتدخل المشرع الجنائي في العراق، لتشريع نصوص قانونية لتجريم الأفعال غير المشروعة الناتجة عن إستعمال الإنترنت والبيانات الإلكترونية من الاولويات الضرورية، وخاصة في ظل التطور التكنولوجي السريع، والذي تولد عنه ظهور مجموعة من الجرائم الإلكترونية لا حصر لها، وعلى المشرع العراقي أن يحذو حذو المشرع الامريكي والفرنسي والإماراتي لمواجهة هذه الجرائم التي بدأت تفتك بالأمن الإلكتروني وهذا ما يؤثر سلباً على جميع الاصعدة الإجتماعية والأقتصادية والسياسية .

أولاً: الركن المادي لجرائم الدخول غير القانوني للنظام الإلكتروني:

الركن المادي ويقصد به السلوك المادي الخارجي الذي نص القانون على تجريمه [2]. ومن ثم كل ما يدخل في كيان الجريمة، وله طبيعة مادية ملموسة يمكن لمس الحيز الخارجي، وهذا ما حذا ببعضهم إلى تسميته بماديات الجريمة[3]. وعلى ضوء ذلك لا عبرة بما يدور في الاذهان من أفكار، أو رغبات وتطلعات، طالما بقيت في هذا الحيز دون أن تحدث على أرض الواقع. وقد أشار قانون العقوبات العراقي رقم (111) لسنة 1969 المعدل، إلى الركن المادي للجريمة في المادة (28) منه على انه: (سلوك إجرامي بإرتكاب فعل جرمه القانون، أو الإمتناع عن فعل أمر به القانون...) ولقيام الركن المادي للجريمة فلابد من توفر ثلاث عناصر.

العنصر الاول: السلوك الإجرامي - المتمثل في النشاط المادي الخارجي، فلا توجد جريمة دون هذا السلوك، لأن القانون كما شهد لا يعاقب على مخارج نفس الأفكار، وهذا السلوك يختلف من جريمة لأخرى، اما العنصر الثاني: النتيجة - ويقصد بها الأثار المترتبة على السلوك الإجرامي الذي حدد القانون له العقاب وقد ينظر إلى الجريمة على أنها ظاهرة مادية يرمز من خلالها إلى التغير الذي يحدث في العالم الخارجي فينال الجاني بسلوكه من حق أو مصلحة قد احاطها المشرع بالحماية الجنائية. ويتمثل العنصر الثالث: بالعلاقة السببية - ويقصد بها الصلة التي تربط بين السلوك الإجرامي

([1])- ينظر: قرار محكمة استئناف واسط الاتحادية/ الهيئة التمييزية المرقم (211/ت/جنح/2021 بتاريخ 2021/1/22) والذي تضمن جريمة اختراق صفحة الفيس بوك، وانتحال صفة شخصية المشتكي، فقد كان قرار المحكمة مبنيا على الاستدلال بالمادة (292) من قانون العقوبات العراقي، وحقيقة الامر هذا يدل على الاجتهاد من قبل رئاسة المحكمة نتيجة للنقص التشريعي ولعدم اقرار قانون الجرائم الالكترونية العراقي.

(2) - د. علي حسين خلف، د. سلطان عبدالقادر الشاوي، المبادئ العامة في قانون العقوبات، الطبعة 2، العاتك لصناعة الكتب، 2010، ص 138 .

(3) - د. محمد ماضي، التحضير للجريمة في التشريع العراقي، الطبعة الاولى، مكتبة السنهوري، بيروت، 2012، ص 35.

والنتيجة الضارة إذ تثبت بأن الاخيرة هي نتيجة طبيعية للسلوك الإجرامي ولهذا فإن العلاقة السببية هي التي تربط بين عنصري الركن المادي للجريمة وقيامها يؤدي إلى إثبات قيام الجاني بالفعل ومن ثم إنزال العقاب الذي نص عليه القانون. في حين أن تخلف الرابطة أو العلاقة يؤدي إلى مساءلة الجاني عن الشروع في الجريمة في حال إذا كانت الجريمة عمدية، أما إذا لم تكن كذلك فإن الجاني لا يسأل عن الشروع لأنه لا شروع عن الجرائم غير العمدية [1].

أما حالات الدخول غير القانوني إلى النظام الإلكتروني هي : أ- حالة عدم وجود سند قانوني للدخول إلى النظام المعلوماتي وتتحقق هذه الحالة في فرضيتين، (الأولى) قيام شخص غير مالك للنظام المعلوماتي أو مستخدمة الشرعي بالدخول إلى النظام المعلوماتي على غير رضاه ودون الحصول على تصريح منه[2]. (الثانية) دخول غير مالك النظام المعلوماتي أو مستخدمه الشرعي دون الحصول على إذن من السلطة المختصة، على سبيل مثال الحصول على إذن من النيابة العامة بالتفتيش في الحالات المنصوص عليها قانونا. ب- حالة تجاوز التصريح أو الإذن بالدخول إلى النظام المعلوماتي، بمعنى قد يكون للشخص الداخل إلى النظام المعلوماتي سواء من داخل المؤسسة التي تحتوي على النظام أو من خارجها صلاحيات محددة وفقاً لطبيعة عمله أو لطبيعة التصريح الممنوح له، إلا أنه يطمع في الحصول على صلاحيات ومعلومات أكثر[3] .

ومن خلال مراجعتنا لموقف التشريعات العربية لاحظنا أن قانون مكافحة جرائم تقنية المعلومات الإماراتي لسنة 2006 المعدل بالقانون رقم (6) لسنة 2012 أخذ بهذا الإتجاه، إذ جرم في المادة **(2/اولا)** الدخول غير القانوني إلى المواقع الإلكترونية، أو نظام معلوماتي دون الإشارة إلى شبكات المعلومات، إذ المادة المذكورة سلفاً، إلى انه: (1- كل فعل عمدي يتوصل فيه بغير وجه حق إلى موقع أو نظام معلوماتي سواء بدخول الموقع أو النظام أو بتجاوز مدخل مصرح به يعاقب عليه بالحبس وبالغرامة أو بإحدى هاتين العقوبتين).

اما النتيجة في الجرائم الإلكترونية، فهناك سؤال يثار، هل تتحقق النتيجة الاجرامية بمجرد الدخول إلى النظام الإلكتروني والمعلومات، بصرف النظر عن الوصول إلى المعلومات المخزنة داخله، أم أنه يجب الوصول إلى المعلومات التي يحتويها النظام المعتدي عليه؟

---

(1) - د. أحمد عبد الموجود ابو الحمد زكير، المواجهة الجنائية لظاهرة التنمر، المجلة القانونية، المجلة القانونية، المجلد 9، العدد 8، 2021، ص 2654 .

(2) - د. تامر محمد صالح، الحماية الجنائية للحق في المعلومات الرسمية، دار الفكر والقانون، مصر 2021، ص168.

(3) - د. محمد كمال محمود دسوقي ، المصدر السابق، ص 68.

للإجابة عن هذا السؤال تختلف تبعا لأختلاف مواقف التشريعات من جريمة الدخول غير القانوني، فقد ذهبت بعض التشريعات إلى الاكتفاء بمجرد الدخول إلى نظام المعلومات كان يقوم شخص ما بتشغيل جهاز الحاسب الآلي والتصفح فيه، أو تمكنه من كسر برامج الحماية ورموز التشفير الخاصة بالحاسب الآلي أو الشبكات والوصول إلى مناطق داخل النظام المعلوماتي على النحو الذي يمكنه التجوال داخل النظام المعلوماتي، سواء نجح الجاني في الوصول إلى المعلومات أو البرامج المخزنة داخل النظام محل الجريمة، أم لا[1].

والعلة من تجريم هذا الفعل في تقديرنا لكون فعل الدخول غير القانوني هو لضمان توفير الحماية اللازمة للمعلومات والنظام من الوصول إليها ويصبح هذا النظام عرضه للدخول والخطر، والمساس بسلامتها، كون هذه الجريمة من الجرائم التي تمثل عدواناً محتملاً على الحق المحمي.

ثانيا: الركن المعنوي لجرائم الدخول غير القانوني للنظام الالكتروني

الركن المعنوي له أهمية كبيرة في تحديد نطاق المسؤولية عن الجريمة إذ أن العدالة تقتضي إنزال العقوبة على الشخص الذي يكون على صله نفسية بمادياتها وبصور عامة فإن الركن المعنوي أو النفسي له صورتان نص عليها المشرع العراقي، (الأولى) القصد الجرمي- وهو ما جاء في نص المادة (33) من قانون العقوبات رقم 111 لسنة 1969 المعدل ويقصد به هو توجيه الفاعل إرادته إلى ارتكاب الفعل المكون للجريمة هادفا إلى نتيجة الجريمة التي وقعت أو نتيجة أخرى[2].

وعلى هذا الأساس فالقصد الجرمي يتكون من (علم وإرادة) وذلك من خلال اتجاه الإرادة إلى تحقيق النتيجة الجرمية وكل واقعة يستمد منها الفعل دلالته الإجرامية، بالإضافة إلى إتجاه الإرادة إلى تحقيق الفعل الإجرامي، وكذلك لابد من توافر العلم بعناصر الجريمة [3]، فالقصد الجرمي لا يقوم بإرادة تتجه إلى تحقيق الفعل الإجرامي وحسب وإنما لابد من توافر العلم بعناصر تلك الواقعة وتصورها بوقت سابق. (الثانية) الخطأ - قد لا يقصد الفاعل تحقيق النتيجة التي تترتب على سلوكه، إذ تتجه إرادة الفاعل للفعل دون النتيجة[4]. وقد أشار المشرع العراقي إلى هذه الصورة في المادة (35) إلى الجريمة غير العمدية، اذ يكون معيار الخطأ هو الركن المعنوي في هذه الجرائم، وفي إطار تحديد هذا الخطأ ظهر هناك اتجاهان، **الاتجاه الأول** (الشخصي) والذي يقوم على أساس سلوك المتهم الذي صدر عنه الخطأ في ظروف معينة على سلوكه المعتاد **الاتجاه الثاني (الموضوعي)** الذي يقوم على أساس

(1) - د. محمد كمال محمود دسوقي ، المصدر السابق ، ص 76.
(2) - المادة (33) قانون العقوبات العراقي رقم 111 لسنة 1969 .
(3) - د. ابراهيم محمود اللبيدي، السلوك الاجرامي في جرائم الانترنت، اصدارات مركز الاعلام الامني، البحرين، ص 5.
(4) - د. تامر محمد صالح، المصدر السابق ، ص 175 .

الشخص العادي، ويقوم على قياس السلوك الواقعي للمتهم بسلوك شخص مجرد وفي بعض الأحيان قد تقع الجريمة المعلوماتية عن طريق الخطأ دون أن يقصد الفاعل ارتكابها كما في حال الدخول إلى بعض المواقع المحظورة أو القيام بخطوة ما في مسرح الجريمة يؤدي إلى محو الدليل دون أن يقصد بذلك[1].

ويمكن القول أنه تُعد جريمة الدخول غير القانوني للنظام الإلكتروني، هي من جرائم الأمن الإلكتروني، فوفقا لما ذهبت اليه اتفاقية بودابست المتعلق بالجريمة الإلكترونية وغالبية التشريعات من الجرائم العمدية، التي يجب أن يكون الجاني قد أقترفها وهو على علم بحقيقتها الواقعية وبعناصرها القانونية، ويتخذ فيها الركن المعنوي صورة القصد الجرمي بعنصرية (العلم والإرادة) أي بمعنى أن يكون الجاني على علم بمكونات الجريمة ولديه الإرادة لإرتكاب أفعال هذه الجريمة. فجريمة الدخول غير القانوني للنظام المعلوماتي ويتحقق القصد الجرمي بتعمد الجاني إستخدام وسائل وأساليب مختلفة تمكنهم من كسر شفرة الدخول وكلمة السر وهو إحداث تغيرات في نظام الحماية الخاصة بالنظام الإلكتروني، بقصد الدخول إلى هذا النظام وهو يعلم بأنه غير مصرح له بالدخول إليه بداية أو أنه يدخل إلى مناطق داخل النظام المعلوماتي المصرح له بالدخول إليه لا يشملها هذا التصريح ويقوم بالاطلاع على المعلومات والأسرار التي يحتويها ذلك النظام، ويتحقق القصد الخاص الجنائي في الجرائم الإلكترونية والمعلوماتية في جريمة البقاء غير القانوني أو الدخول غير القانوني للنظام الإلكتروني من خلال تعمد الجاني بقائه عند اكتشافه أنه دخل إلى النظام الإلكتروني أو إلى أنظمة غير مصرح له بالدخول إليها أو البقاء داخلها والاطلاع عليها وعلى ما تحتويه هذه الانظمة من أسرار وبرامج[2]. وعلى هذا الأساس يكون القصد الجرمي مطلوباً في جريمة الدخول غير القانوني للنظام الإلكتروني وقد يكون قصداً عاماً أو خاصاً، وهو ما يتضح من موقف التشريعات المختلفة وبيان ذلك يكون كالاتي:

1- **القصد العام في جريمة الدخول غير القانوني**: يراد به القصد الجرمي العام وهو إتجاه إرادة المجرم إلى إرتكاب الفعل المجرم مع توافر العلم بأركانها، التي يتطلبها القانون وينحصر في حدود تحقيق الهدف من الجريمة ويكتفي القانون بربط القصد الجرمي بالغرض الذي يسعى إليه الجاني لتحقيقه

(1) - د. محمود محمود مصطفى، شرح قانون العقوبات العام، الطبعة الاولى، دار النهضة العربية، القاهرة، 1984 ص 415.

(2) - محمد جمال الدسوقي المصدر السابق، ص 79.

بغض النظر عن الباعث الذي يدفعه فالقصد العام هو الأصل العام الكافي لقيام الجريمة في الجرائم العمدية[1].

وعلى هذا الأساس فإن القصد العام في الجرائم الإلكترونية والدخول غير القانوني للنظام المعلوماتي يتطلب أن يكون الجاني على علم بأن الدخول إلى نظام المعلومات كان دخول غير مشروع لا يستند إلى حق قانوني أو تصريح من مسؤول النظام يخوله الدخول إلى هذا النظام أو الأطلاع على ما يحتويه من معلومات أو بيانات أو برامج، كما يقتضي القصد الجرمي اتجاه إرادة الجاني حين يأتي فعله بقصد تحقيق النتيجة الإجرامية التي سوف تترتب على فعله[2].

2- **القصد الخاص في جريمة الدخول غير القانوني:** القصد الخاص هو نفسه القصد العام من إذ توافر أركانه الا أن المشرع يتطلب في الجريمة حصول نتيجة اجرامية معينة، أو وقوعها بباعث خاص، أو كانت الجريمة تستلزم ذلك بحسب طبيعتها ولو لم يتطلبه المشرع صراحة في نص التجريم، وبالنسبة لجريمة الدخول غير القانوني إلى النظام المعلوماتي فقد تتطلب بعض التشريعات توافر القصد الخاص إلى جانب القصد العام، وقد رتب بعضها على توافر القصد الخاص تشديد العقوبة. ففي أستراليا نجد أن المشرع نص على تشديد العقوبة متى ارتكب المجرم فعل الدخول غير المشروع بنية الأضرار بالغير[3].

وتأسيساً على ما تقدم فالمجرم الإلكتروني كغيرة من المجرمين يلجأ إلى وسائل وأساليب مختلفة في إرتكاب الجريمة وفي سعي مستمر إلى تطوير الوسائل المتاحة له، وقد يلجأ إلى إستحداث وسائل وأساليب جديده وهو ما يتوافق مع طبيعة الصراع والتنافس المستمر بين صانعي البرامج الإلكترونية، فالمجرم المعلوماتي يسعى دائما للبحث عن الثغرات الأمنية أو خلق تلك الثغرات في البرامج الإلكترونية والنظم المعلوماتية من قبل المجرم المعلوماتي، في مقابل السعي الدائم من جانب صانعي البرامج لسد ومعالجة الثغرات التي يمكن أن ينفذ من خلالها المجرم المعلوماتي وتطوير برامج الحماية اللازمة لذلك[4]. ففي بعض الحالات قد لا يتطلب إرتكاب جريمة الدخول غير القانوني سوى قيام الجاني بضغط زر تشغيل الحاسب الآلي حتى يتمكن من الدخول إليه والتجوال داخله والاطلاع على ما يحتويه من معلومات، وقد يلجا الجاني إلى التجربة العشوائية للوصول إلى كلمات السر أو لكسر شفرتها، إذ يقوم بتجربة كل الطرق الممكنة للوصول إلى كلمة السر، وفي الوقت الحالي هناك عدد

(1) - د. عبد الفتاح بيومي ، المصدر السابق، ص 132 .
(2) - علي عدنان سلمان الركابي ، المصدر السابق، ص 80 .
(3) – نقلاً عن د. سعد معن إبراهيم وحسام حازم أحمد الجبوري ، التحريض في وسائل النشر وكيفية مواجهته امنيا، مكتبة القانون المقارن، الطبعة الاولى، 2021، ص 60 .
(4) - د. خالد ممدوح ابراهيم، أمن الجريمة الالكترونية، المصدر السابق، ص 45.

كبير من المواقع الإلكترونية على شبكات الانترنت توفر برامج لكسر كلمات السر أو الشفرة، أو يقوم المجرم باستغلال الثغرات الأمنية الموجودة في نظام الحاسوب وشبكات الانترنت و يمكن من خلالها النفاذ، وتعد الابواب الخلفية الموجودة في النظام المعلوماتي والبرامج من أبرز صور الثغرات الأمنية التي يستغلها الجاني لاقتحامه والوصول إلى المعلومات المخزنة. وقد يلجأ الجاني إلى اسلوب إنتحال شخصية أحد المستفيدين الشرعيين للحصول على كلمة السر، كأن يقوم الجاني بالأتصال بأحد المستخدمين الشرعيين وإقناعه بانه خادم الموقع يقوم بعرض رسالة مزورة عليه يطلب منه إعادة إدخال الاسم وكلمة السر[1].

ويرى الباحث أن جرائم الامن الإلكترونية لا تتطلب توفر القصد الخاص لتحقق الجريمة الإلكترونية وانما يكفي توفر القصد العام المتمثل باتجاه ارادة المجرم إلى إرتكاب الفعل المجرم مع توافر العلم بأركانها، فالقصد العام في الجرائم الإلكترونية وجريمة الدخول غير القانوني للنظام المعلوماتي يتطلب أن يكون الجاني على علم بأن الدخول إلى نظام المعلومات كان دخولاً غير مشروع لا يستند إلى حق قانوني أو تصريح من مسؤول النظام يخوله الدخول إلى هذا النظام أو الاطلاع على ما يحتويه من معلومات أو بيانات أو برامج.

ثالثا : الركن الشرعي لجرائم الدخول غير القانوني للنظام الإلكتروني

المقصود بالركن الشرعي هو الصفة غير المشروعة وهذه الأخيرة تتحقق نتيجة إنطباق نص التجريم الموجود في القانون العقابي على سلوك أو فعل الذي يرتكبه الجاني، بمعنى أن الركن الشرعي للجريمة هو ما يسمى (بمبدأ قانونية الجرائم والمعلومات) وعلى هذا الأساس فإن الركن الشرعي يختلف عن الركنين المادي والمعنوي للجرمية[2].

ونجد أن الولايات المتحدة الأمريكية قد شرعت قانوناً خاصاً لحماية الحاسوب والبيانات الإلكترونية، وذلك في عام (1976) وفي عام (1985) وعلى ضوء ذلك قد حدد معهد العدالة القومي فيها خمسة أنواع رئيسية لهذه النوع من الجرائم وهي: 1- جرائم الحاسوب الداخلية. 2- جرائم الاستخدام غير المشروع عن بعد، شبكات المعلومات الإلكترونية. 3- جرائم التلاعب بالحاسوب. 4- دعم التعاملات الاجرامية للنظم والشبكات الالكترونية. 5- سرقة البرامج الجاهزة والمكونات المادية .

(1) - د. سحر سعد عبد السميع ، المصدر السابق، ص 132 وما بعدها .

(2) - حسين مجباس حسين العزاوي، جرائم القذف والسب عبر القنوات الفضائية والانترنت وموقف القانون العراقي منها، مطبعة السيماء، بغداد، 2016، ص 102 .

وصدر في عام 1986 قانون آخر يعرف فيه جميع المصطلحات الضرورية لتطبيق جرائم النظم المعلومات والشبكات الإلكترونية، وعلى أثر ذلك قامت الولايات المتحدة الأمريكية بدورها بإصدار تشريعاتها الخاصة بها للتعامل مع هذه الجرائم التي تواكب التشريعات الإتحادية المذكورة[1].

أما المشرع العراقي فقد تناول مبدأ المشروعية من خلال الدستور العراقي لسنة 2005 في المادة (19/ثانيا) والتي تنص على أن (لا جريمة ولا عقوبة الاّ بنص، ولا عقوبة إلا على الفعل الذي يعده القانون وقت اقترافه جريمة، ولا يجوز تطبيق عقوبة أشد من العقوبة النافذة وقت ارتكاب الجريمة)[2]. وايضا نجد ان المشرع الجنائي العراقي قد أشار إلى مبدأ المشروعية من خلال قانون العقوبات العراقي رقم 111 لسنة 1969، وجاء بنص المادة (1) منه على أن: (لا عقاب على فعل أو امتناع إلاّ بناء على قانون ينص على تجريمه وقت أقترافه، ولا يجوز توقيع عقوبات أو تدابير إحترازية لم ينص عليها القانون)[3].

وتأسيساً على ما تقدم فأن المشرع العراقي يحاول أن يطبق القوانين التقليدية على الجرائم الإلكترونية الحديثة، لعدم إقرار مشروع قانون الجرائم الإلكترونية لغاية اليوم ، وهذا ما يسبب إشكالية كبيرة في ضبط الجريمة الالكترونية وايضا يسبب نقصاً تشريعياً واضحاً، ويؤدي من ثم إلى صعوبة مكافحة الجريمة الإلكترونية، بالإضافة إلى صعوبة التفتيش الإلكتروني عن ادلة الاثبات وضبط المجرم. لذا نرى أن الوقت مناسب وعلى المشرع الجنائي العراقي إقرار مشروع قانون الجرائم الإلكترونية، رغم تأخره لمدة طويلة، ولكن قد يكون لهذا التأخير إيجابيات كثيرة، ومنها أن يحيط المشرع بكافة الجرائم الإلكترونية والمعلوماتية، من خلال البحث ودراسة القوانين المقارنة على الصعيد العربي والغربي، والتي قد أثبتت فاعليتها في مواجهة ومكافحة الجرائم الناشئة عن التطور التكنولوجي.

(1) - د. محمد ممدوح بدر ، المصدر السابق، ص 91.
(2) - المادة (19) من الدستور العراقي لسنة 2005 .
(3) - المادة (1) من قانون العقوبات العراقي رقم 111 لسنة 1969 .

الباب الثاني

مظاهر تأثير التطور التكنولوجي على السياسة الجنائية الإجرائية

الباب الثاني

مظاهر تأثير التطور التكنولوجي على السياسة الجنائية الإجرائية

ظهرت هناك مجموعة من الصعوبات حددها قانونيون والتي تعطل إثبات الجرائم الإلكترونية، بسبب غياب الدليل الجنائي، وصعوبة تتبع المتهمين بسبب قدرتهم على إخفاء أي إثبات يؤكد تورطهم في القضية أو وجودهم خارج حدود الدولة، وكذلك أن المتهمين في الجرائم الإلكترونية على إلمام بطبيعة الأجهزة التي يتعاملون معها، وكيفية تطبيق الجريمة من دون ترك أي دليل يثبت تورطهم، لذلك يتوجب تطوير السياسة الجنائية، مع تطور الجريمة الإلكترونية، التي تتطور مع تقدم الأجهزة التي تتعامل معها، وأن تشرع قوانين حديثة لسد الثغرات التي تواكب تطور الأجهزة التقنية وما ينتج عنها. وعلى ضوء ذلك سنقسم دراستنا في هذا الباب إلى فصلين نخصص الفصل الاول لدراسة الدور الإلكتروني في السياسة الجنائية، أما الفصل الثان سيكون لبحث أثر التطور التكنولوجي على إجراءات التحقيق والمحاكمة.

الفصل الأول

الدور الإلكتروني في السياسة الجنائية

تعدّ الجرائم الإلكترونية من أكثر القضايا القانونية حداثة وإثارة لمخاوف رواد المواقع ومنصات التواصل والشركات والبنوك التي تعدّ هدفاً ثميناً للهجمات السيبرانية ومرتكبي الجرائم الإلكترونية. كما باتت تأخذ منحى أكثر رواجاً مع التقدم التكنولوجي الكبير الذي أدخل أبعاداً جديدة إلى مفهوم الجريمة، ومع تداخل المعلوماتية والأجهزة الحاسوبية في مختلف الأنشطة الحياتيّة، أصبحت الجرائم الرقمية أكثر خطورة وحساسيّة، فضلاً عن تعقيداتها، ووسائل التخفّي في إرتكابها.

ونجد هناك مجموعة من الدول قد أطّرت الجرائم الإلكترونية في أحكام وقوانين تعنى بمكافحة الجريمة المعلوماتية، تفصّل في أحكامها طبيعة هذه الجرائم وآلياتها، وسلوكيات مرتكبيها وأهدافهم والعقوبات المستحقة وتعويضات ضحايا الجرم الإلكتروني، وتشكّل رادعاً قانونيّاً للحدّ منها، في المقابل هنالك صعوبات عدّة ومتجددة تواجه القائمين على مكافحة الجرائم الإلكترونية من إذ اكتشافها والتحقيق، وجمع الاستدلالات اللازمة لإثباتها وكيفية مباشرة إجراءات الدعوى الجنائية فيها أمام المحاكم.

وقد ظهرت مجموعة من الصعوبات حددها قانونيون والتي تعطل إثبات الجرائم الإلكترونية، بسبب غياب الدليل الجنائي، وصعوبة تتبع المتهمين بسبب قدرتهم على إخفاء أي إثبات يؤكد تورطهم في القضية أو وجودهم خارج حدود الدولة، وغياب التزام الشركات ألمزودة لخدمات التواصل الاجتماعي بتوفير تسهيلات للجهات القضائية بهدف الحصول على معلومات وبيانات تخص المتهمين، وعدم وجود قوانين تحمي البيانات الشخصية لمستخدمي الإنترنتعالمياً. وركزوا على تحدٍّ يرتبط بصعوبة الاحتفاظ الفني بدليل الجريمة المعلوماتية، إذ يستطيع المجرم المعلوماتي، في أقل من ثانية، أن يمحو أو يحرف أو يغير البيانات والمعلومات الموجودة في الكمبيوتر. وأكدوا أن المجنى عليه، خصوصاً في جرائم الإبتزاز الإلكتروني، يتكتم على الجريمة ولا يبلغ السلطات المختصة عنها، خوفاً من التشهير، وعندما يكون المجنى عليه مصرفاً، أو مؤسسة مالية، أو مشروعاً صناعياً أو تجارياً ضخماً، لا يبلغ عن تلك الجريمة والسبب في ذلك يرجع إلى أن الإبلاغ عن تلك الجرائم ربما يؤدي إلى إحاطة المجرمين عمداً بنقاط الضعف في أنظمتها، ورغبة منها في تفادي الخسائر التي قد تلحق بها من جراء هذا البلاغ وتأثير ذلك في ثقة العملاء بها.

فالجرائم التي كانت ترتكب في الأزمنة السالفة لم يعد لها وجود في الوقت الراهن و العكس صحيح، فارتكابها يختلف باختلاف البيئة التي تقع فيها وكذلك باختلاف المستوى العلمي والثقافي، وفي بعض

الأحيان الجانب الديني. خاصة بعد ظهور المعنى الحديث للدولة، إذ نتج عنها ظهور مجتمع دولي تربط بينه الكثير من الصلات التجارية أو السياسية أو حتى العسكرية. هذا التطور على المستوى الدولي لم يمر هو الآخر بسلام على الإنسانية جمعاء، فالجريمة ومن ورائها المجرمون استغلوا هذا الوضع ليجعلوا للجريمة طابعا يتعدى كل الحدود.

ولذا سوف نقسم دراستنا في هذا الفصل إلى مبحثين، نتناول في الاول دراسة ماهية الوسائل الإلكترونية الحديثة في السياسة الجنائية، ونخصص المبحث الثان، لدراسة مظاهر تأثير التطور التكنولوجي على الاثبات الجنائي.

المبحث الأول

الوسائل الإلكترونية وأثرها في الإثبات الجنائي

تعددت الوسائل الإلكترونية في ظل التقدم التكنولوجي والتقني، وهذا التعدد يزداد تنوعاً ونموا وتداخلاً مع مرور الوقت، ومن هذه الوسائل الإلكترونية: المحطات التلفزيونية، والكابل الرقمي، والصحافة الإلكترونية، ومنتديات الحوار، والمدونات، والمواقع الشخصية، والمؤسسات التجارية، ومواقع الشبكات الاجتماعية، ومقاطع الفيديو والصور والصوت، والاذاعات الرقمية، ومواقع الإنترنت والبريد الإلكتروني، بالإضافة إلى الهواتف المتنقلة وغيرها الكثير من الوسائل الإلكترونية التي أصبح التعامل معها في الحياة اليومية أمراً لا بد منه. وعلى ضوء ذلك سنحاول دراسة وتبيان مفهوم الوسائل الإلكترونية في مطلب أول، ونخصص المطلب الثاني لدراسة صور الدليل الإلكتروني وإشكالية قبوله.

المطلب الأول

مفهوم الوسائل الإلكترونية

تزايدت جرائم الأنترنت بعد التطور التكنولوجي الذي يعيشه العالم في الوقت الحالي، مما أدى إلى ظهور الوسائل التقنية الحديثة ووسائل التواصل الاجتماعي وغيرها وأجهزة الحاسوب مما أضاف أعباء جديدة على عاتق اجهزة التحقيق، لما يتطلبه التصدي لهذه الجرائم من قدرات فنية لم يألفها المحققون، ولم يعتادوا عليها، مما أدى إلى ضرورة توفير الإمكانيات والمهارات المطلوبة في هذا المجال، بالإضافة إلى ذلك فإن إجراءات التحقيق وجمع الأدلة في هذه الجرائم تتميز بطابع خاص من حيث الإجراءات ومن حيث طبيعة الأدلة المتحصلة من هذه الإجراءات.

الفرع الأول

التعريف بالوسائل الإلكترونية

الوسائل الإلكترونية هي" منظومة من الشبكات الإلكترونية التي تسمح للمشترك فيها بإنشاء مواقع خاصة بها، ومن ثم ربطها عن طريق نظام اجتماعي إلكتروني مع أعضاء آخرين لديهم أهتمامات والهوايات نفسها"[1] ويعرفها بعضهم على أنها: هي "مجموعة من الأجزاء متكاملة مع بعضها بعضهم بهدف تشغيل مجموعة من البيانات الداخلة وفقا لبرنامج موضوع مسبق للحصول على النتائج المطلوبة"[2]. وهناك من يتوسع في تعريف مضمون الوسائل الالكترونية على أنها: كل جهاز إلكتروني يستطيع أن يقوم بأداء العمليات الحسابية والمنطقية لتعليمات المعطاة له بسرعة كبيرة تصل إلى عشرات الملايين من العمليات الحسابية في الثانية الواحدة وبدرجة عالية الدقة وله القدرة على التعامل مع كم هائل من البيانات وكذلك تخزينها واسترجاعها عند الحاجة إليها[3]. وأيضا من يعرفها بأنها: "مجموعة من الأجهزة أو المواقع على شبكة الإنترنت العالمية تتيح التواصل بين الأفراد في بيئة مجتمع افتراضي يجمعهم الاهتمام أو الانتماء لبلد أو مدرسة أو فئة معينة في نظام عالمي لنقل المعلومات والمعارف". وأيضا هناك جانب من الفقه يعرفها على أنها : "مواقع تتشكل عن طريق الانترنت، تسمح للأفراد بتقديم لمحة عن حياتهم العامة، واتاحة الفرصة لاتصال بقائمة المسجلين والتعبير عن وجهة نظر الافراد أو المجموعة عن طريق عملية اتصال وتختلف طبيعة التواصل من موقع لآخر"[4].

أما المشرع الفرنسي فقد عرف الوسائل الالكترونية بأنها: "بروتكول اتصال مفتوح أو ربط بيانات وتبادلها باي شكل يصل إلى الجمهور دون قيد على أي محتوى تبادلي من قبل مقدمي الخدمات التقنية". أما القانون الإماراتي رقم (5) لسنة 2012 فقد عرف الوسائل الإلكترونية على أنها "مكان إتاحة المعلومات الإلكترونية على الشبكة المعلوماتية ومنها مواقع التواصل الاجتماعي والصفحات الشخصية والمدونات". أما القانون الكويتي رقم (63) سنة 2015 فقد عرفها: "أنها مكان إتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان محدد، وإلكتروني، وهو كل ما يتصل بتكنولوجيا المعلومات وذو قدرات كهربائية أو رقمية أو مغناطيسية، أو بصرية أو كهرومغناطيسية أو وسائل

(1) - التوجي محمد عثمان عبد القادر، السياسة الجنائية لمكافحة الإشاعة عبر مواقع التواصل الاجتماعي، بحث منشور، مجلة الاجتهاد الدراسات القانونية والاقتصادية، المجلد 9 ، العدد 4، 2020، صفحة 200.

(2) - نسرين عبد الحميد نبيه الجريمة المعلوماتية والمجرم المعلوماتي ، ص 184 .

(3) - علي عدنان سلمان الركابي ، جريمة الارهاب المعلوماتي، مكتبة السنهوري، 2020، ص 95.

(4) - د. زيد محمود سلمان، موضوعات الارهاب في مواقع التواصل الاجتماعي وعلاقتها بإشاعة الخوف لدى الجمهور، أطروحة دكتوراه في فلسفة الاعلام، جامعة بغداد، 2018، ص 67.

أخرى مشابهة، سلكية أو لا سلكية، وما قد يستحدث من تقنيات في هذا المجال". وهناك من يعرف الوسائل الإلكترونية على أنها "وسائل التواصل الاجتماعي الإلكترونية وهي المواقع على شبكة الإنترنت تسمى (sociaux reseaux) وهي الشبكات الاجتماعية التي تتيح التواصل بين مستخدميها في بيئة مجتمع افتراضي يجمعهم وفقا لاهتماماتهم أو انتماءاتهم الاجتماعية والثقافية والتجارية حيث يتم ذلك عن طريق التواصل المباشر في إرسال الصور أو مقاطع الفيديو وغيرها"[1].

ويرى الباحث أنه يمكن تعريف الوسائل الإلكترونية على أنها: (كل برنامج أو تطبيق الإلكتروني أو جهاز تقني أو موقع إلكتروني أو برامج إتصال، يتم من خلال تلك البرامج والتقنيات تبادل جميع البيانات والمعلومات مهما كانت طبيعتها ونوعها).

أولا : تعريف الدليل الإلكتروني.

1- الدليل لغة : هو المرشد وما يتم به الإرشاد، وما يستدل به، والدليل هو الدال ايضا، والجمع أدلة جمع دلالة [2]. وأيضاً ورد في مختار الصحاح ان الدليل ما يستدل به، وقد دله على الطريق أي أرشده، يدله بالضم، دلالة يفتح الدال وكسرها، ودلولة بالضم والفتح أعلى ويقال أدل، والاسم الدال بتشديد اللام، فلان يدل فلانا أي يثق بع، وقال ابو عبيد: الدال قريب المعنى من الهدى وهما في السكينة والوقار في الهيئة والمنظر وغير ذلك[3].
2- الدليل اصطلاحاً : هو معلومة يقبلها العقل والمنطق يتم الحصول عليها بإجراءات قانونية ووسائل فنية أو مادية أو قولية، ويمكن إستخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة أو فعل، أو أي شيء أو شخص له علاقة بجريمة أو جاني أو مجنى عليه[4]. أو هو الوسيلة التي يستعين بها القاضي للوصول إلى الحقيقة التي يبتغيها[5]. وهناك من يعرف الدليل على أنه: هو كل ما يؤدي إلى إظهار الحقيقة في المسائل الجزائية[6].

---

(1) - دينا عبدالعزيز فهمي، الحماية الجنائية من إساءة استخدام مواقع التواصل الاجتماعي، دار النهضة العربية، 2018 ،ص 19.
(2) - د. جميل صليبا، المعجم الفلسفي، الطبعة الاولى ،دار الكتاب اللبناني، بيروت، 1970 ، ص23.
(3) - محمد بن أبي بكر بن عبدالقادر الرازي، مختار الصحاح، المطبعة الاميرية، القاهرة ، 1338 ،ص209.
(4) - د. رامي متولي القاضي ، المصدر السابق، ص 322.
(5) - د. ابو العلا النمر، الادلة الجنائية في ضوء الفقه واحكام النقض الجنائي، دار الصداقة، 1991، ص 3. وكذلك : د. محمد الامين البشري، التحقيق في الجرائم المستحدثة، الطبعة الاولى، الرياض، 2004، ص 229.
(6) - د. ضياء عبدالله الجابر، ناصر خضر الجوراني، القناعة القضائية في الاثبات الجنائي، بحث منشور، مجلة جامعة كربلاء، المجلد الثالث، العدد الثالث عشر، 2005 ، ص171.

3- تعريف الدليل الالكتروني قانونا: هو الدليل الجنائي ذو طبيعة رقمية[1]. وأيضاً فقد عرف الدليل الإلكتروني من قبل مجموعة العمل القياسية (swgde) وقالوا بأن الدليل الإلكتروني: (هو كل معلومة ذات قيمة اثباتية يتم حفظها أو نقلها في شكل رقمي)[2]. وأيضاً جاء تعريف الدليل الإلكتروني من قبل المنظمة الدولية للدليل الرقمي (ioce) وقالوا بأن الدليل الإلكتروني: (هو المعلومة المحفوظة أو المنقولة في شكل ثنائي والتي يمكن الاعتماد عليها في المحكمة). وايضاً قامت رابطة كبار ضباط الشرطة (acpo) بتعريف الدليل الالكتروني: (بأنه البيانات والمعلومات ذات القيمة الذاتية التي تخزن أو تنقل بواسطة الحاسوب)[3]. أما الفقيه براين (brian carrier) عرف الدليل الإلكتروني بأنه (بيانات رقمية من شأنها أن تدعم أو تدحض فرضية حول وقائع رقمية أو بيانات رقمية). أما الفقيه كازاي (casey eagham) عرف الدليل الإلكتروني بأنه: (أي بيانات يخزنها جهاز حاسوب أو يمكن نقلها بواسطته من شأنها أن تدعم أو تدحض نظرية حول كيفية وقوع جريمة أو تكتشف عنصراً جوهرياً فيها كالقصد الجنائي والاعذار القانونية)[4].

وبعض الفقهاء يعرف الدليل الإلكتروني بأنه: الدليل المأخوذ من أجهزة الكمبيوتر والأجهزة التقنية الأخرى ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة وهو مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور والأصوات والأشكال والرسوم وذلك من أجل الربط بين الجريمة و المجرم والمجنى عليه، وبشكل قانوني يمكن الاخذ به أمام أجهزة انفاذ وتطبيق القانون[5]. وهناك من يعرف الأدلة على انها: جميع البيانات الرقمية التي يمكن أن تثبت أن هناك جريمة قد ارتكبت أو توجد علاقة بين الجريمة والمتضرر منها والبيانات الرقمية هي مجموعة الأرقام التي تمثل مختلف المعلومات بما فيها النصوص المكتوبة والرسومات والخرائط والصوت والصورة[6]. وهناك أيضاً من يعرف الدليل الرقمي : (يمكن أن يكون أي معلومة محررة أو مخزنة في شكل معالج رموز وأرقام إذ يستخدمها الحاسوب في إنجاز مهمة ما). وذهب بعضهم لتعريف الأدلة الرقمية بأنها: (مجموعة المجالات، أو النبضات المغناطيسية، أو الكهربائية التي يمكن تجميعها وتحليلها بإستخدام

(1) - أمير فرج يوسف، الاثبات الجنائي للجريمة الالكترونية والاختصاص القضائي بها، مكتبة الوفاء القانونية، الاسكندرية، الطبعة الاولى، 2016 ، ص287.

(2) - د. ميسون خلف أحمد الحمداني، مشروعية إلكترونية في الاثبات الجنائي، بحث منشور ، مجلة البحوث والدراسات العربية، المجلد 18، العدد 65 ، 2016 ، ص 196 .

(3) - د. خالد ممدوح ابراهيم، المصدر السابق، ص 177 .

(4) - د. مفيدة مباركة ، المصدر السابق، ص 555.

(5) - د. سحر سعد عبد السميع ، المصدر السابق، ص 283 .

(6) - د. علي هاشم عبد الحسن ، المصدر السابق، ص129. وكذلك: د. مليكة أبو ديار ، المصدر السابق، ص106 .

برامج وتطبيقات خاصة تظهر في شكل صور، أو تسجيل صوتي ومرئية)[1]. ويعرف الدليل الإلكتروني بانه: (الدليل المأخوذ من الانظمة التكنولوجية الإلكترونية سواء من الحاسب الآلي أو أي نظام إلكتروني رقمي أو من شبكات الإتصال عبر إجراءات قانونية وفنيه من أجل تقديمها للقضاء بعد استنباطها وتفسيرها على شكل نصوص مكتوبة لإثبات أو نفي وقوع الجريمة)[2].

4- التعريف التشريعي للدليل الالكتروني

جاء تعريف الدليل الإلكتروني من قبل الإتفاقيات الدولية والأوروبية، إذ إستدرك المشرع الأوروبي القصور التشريعي في تعريف الدليل الإلكتروني ومن خلال هذه الإتفاقية الخاصة بتبادل المعلومات والأدلة الرقمية المسماة (evidence)، فقد عرف المشرع الاوربي الدليل الإلكتروني على أنه: (الدليل الرقمي يشمل أي معلومات ومخرجات الأجهزة التناظرية أو البيانات في شكل رقمي، ذات قيمة اثباتية محتملة تتم معالجتها أو توليدها أو تخزينها أو نقلها بواسطة أي جهاز إلكتروني) . ويلاحظ على هذا التعريف انه ورد دقيق الصياغة من الناحية اللغوية والقانونية ولقد كان التعريف موسعاً شاملاً لجميع أنواع المعلومات أياً كان نوعها ووضعها خشية توصل التقنية إلى معلومات حديثة تجعل التعريف لا يتجاوب مع التطورات الحاصلة في مجال التكنولوجيا الحديثة والإتصالات. فقد كان التعريف يشمل جميع المعلومات غير محددة، وهو ما يتجلى من عبارة ذات قيمة إثباتية محتملة. وكلمة محتملة في نظر بعضهم تترتب عليها مسائل قانونية مهمة ، فمن جهة تفضي إلى تفادي تضييق دائرة الادلة المعلوماتية بحصرها في تلك التي تتمتع بالقوة الاثباتية دون غيرها أو تلك التي يرجح أن تكون كذلك، في وقت تحول دون التعميم المجرد للمعلومات، إذ ليست كل المعلومات التي قد توجد بحوزة المتهم، بالمفهوم التقليدي للحيازة- ما لم يكن له إرتباط بالواقعة الجرمية أو يفيد فيها إظهار الحقيقة[3].

أما المشرع المصري فقد تطرق إلى تعريف الدليل إلكتروني من خلال القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات ، وقال: (أي معلومات إلكترونية لها قوة أو قيمة ثبوتية مخزنة أو منقولة أو مستخرجة أو مأخوذة من أجهزة الحاسب أو الشبكات المعلوماتية وما في حكمها يمكن تجميعها وتحليلها بإستخدام أجهزة أو برامج أو تطبيقات تكنولوجيا خاصة)[4]. ونلاحظ أن هذا التعريف يفتقر إلى الدقة في الصياغة إذ ورد التعريف عاما ليس قاصراً على الدليل الإلكتروني في

(1) - أمير فرج يوسف، المصدر السابق، ص 288.
(2) - د. علي هاشم ، المصدر السابق، ص 129 .
(3) - لهوى رابح، الشرعية الإجرائية للأدلة المعلوماتية المستمدة من التفتيش، أطروحة دكتورة جامعة بابنه 1 كلية الحقوق والعلوم السياسية قسم الحقوق 21 20 ، ص 12.
(4) - محمود علي محمود علي ، المصدر السابق، ص 23 .

مجال الإثبات الجنائي كما يعاب عليه اشتراط قوة إثباتية للمعلومات لخلع صفة الدليل عليها. **أما المشرع اللبناني** فقد تعرض لتعريف الدليل الإلكتروني من خلال المادة (121) من القانون رقم (81) لسنة 2018 الخاص بالمعاملات الإلكترونية والبيانات ذات الطابع الشخصي وعرف الدليل على أنه: (الآثار المعلوماتية والتي هي من قبيل الأدلة الرقمية أو المعلومات هي البيانات التي يتركها الأشخاص بصورة إرادية أو لا إرادية على الأنظمة التقنية وقواعد البيانات والخدمات المعلوماتية والشبكات المعلوماتية تتضمن الأدلة المعلوماتية والتجهيزات المعلوماتية والبرامج والبيانات و التطبيقات والآثار المعلوماتية وما يماثلها)[1].

ويرى الباحث أنه يمكن تعريف الدليل الإلكتروني الرقمي على أنه : هو مجموعة البيانات والتي تتكون نتيجة المجالات أو النبضات المغناطيسية أو الكهربائية، التي يمكن تجميعها وتحليلها بإستخدام برامج وتطبيقات إلكترونية خاصة ينتج عنها بيانات، كالصور أو تسجيلات صوتية أو مرئية وغيرها، تؤدي إلى معرفة الحقيقة وتكون لها قيمة اثباتية محتملة).

ثانيا : خصائص الدليل الالكتروني

يتميز الدليل الرقمي الإلكتروني بمجموعة من الخصائص تميزه عن الأدلة الجنائية التقليدية، فهي أدلة غير ملموسة، ولا تدرك بالحواس العادية، ولإثبات هذا النوع من الادلة لتكون لها قوة الحجية في الأدانة أو البراءة ، يتطلب وجود الخبراء في المجال الفني والتقني للحفاظ على هذه الادلة من التلف أو الحذف، وسنحاول أن نبين بعض هذه الخصائص والمميزات بمجموعة من النقاط كما يأتي :

1- الدليل الإلكتروني دليل علمي[2]: أي أنه يتكون من بيانات ومعلومات ذات هيئة إلكتروني غير ملموسة لا تدرك في الحواس العادية بل يتطلب إدراكها الإستعانة بأجهزة ومعدات وأدوات الحاسبات الآلية واستخدام نظم برامجية حاسوبية، فهو يحتاج إلى مجال تقني يتعامل معه وهذا يعني أنه كدليل يحتاج إلى بيئته التقنية التي يتكون فيه لكونه من طبيعة تقنية المعلومات[3].
2- الدليل الإلكتروني دليل تقني بمعنى هو مستوحاة من البيئة التي يعيش فيها وهي البيئة الرقمية أو التقنية وتتمثل هذه التقنية الاخيرة في إطار الجرائم الإلكترونية في العالم الافتراضي وهذا العالم كامن في أجهزة الحاسب الآلي والأجهزة التقنية الحديثة والخوادم والمضيفات والشبكات بمختلف أنواعها، فالأدلة الرقمية ليست مثل الدليل العادي فلا تنتج التقنية سكينا يتم بها أكتشاف القاتل، أو اعترافا مكتوبة، أو بصمة اصبع وإنما تنتج التقنية نبضات رقمية تصل إلى درجة تخيلية في شكلها وحجمها

(1) - لهوى رابح ، المصدر السابق، ص 13.
(2) - ابراهيمي جمال، المصدر السابق، ص 161.
(3) - أمير فرج يوسف، المصدر السابق، ص 291.

ومكان تواجدها غير المعلن، فهي ذات طبيعة ديناميكية فائقة السرعة تنتقل من مكان إلى آخر عبر شبكات أتصال بالأنترنت[1].

3- الدليل الإلكتروني يصعب التخلص منه: وهذا يعني أنه من أهم خصائص الدليل الالكتروني بل أنه يمكن عدّهذه الخاصية مميزة يتمتع به الدليل الرقمي عن غيره من الادلة التقليدية، إذ يمكن التخلص بكل سهولة من الاوراق والأشرطة المسجلة إذا حملت في ذاتها إقراراً بإرتكاب شخص لجرائم وذلك بتمزيقها وحرقها[2]، كما يمكن أيضا التخلص من بصمات الاصابع بمسحها من موضعها، بالإضافة إلى أنه في بعض الظروف يمكن التخلص من الشهود وقتلهم أو تهديدهم بعدم الذهاب لأداء الشهادة هذا الامر بالنسبة للأدلة التقليدية، أما بالنسبة للأدلة الرقمية فأن الحال غير ذلك إذ يمكن إسترجاعها بعد محو الملفات وإصلاحها بعد اتلافها وإظهارها بعد إخفاءها، مما يؤدي إلى صعوبة التخلص منها، وذلك عن طريق تهيئة أو إعادة تهيئة أو تشغيل القرص الصلب أو باستخدام الأمر (فورمات) سواء كانت هذه البيانات صور أو رسومات أو كتابات أو غيرها[3].

4- الدليل الإلكتروني قابل للنسخ: حيث يمكن إستخراج نسخة من الأدلة الجنائية مطابقة للأصل ولها القيمة العلمية ذاتها، وهذه الخاصية لا تتوفر في أنواع الأدلة الأخرى التقليدية، مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل من الفقد أو التلف أو الحذف أو التغيير عن طريق النسخ طبق الاصل من الدليل[4].

5- يمتاز الدليل الإلكتروني بالسعة التخزينية العالية: أي أن ملفات التصوير أو مقاطع الفيديو الرقمية يمكن تخزين المئات منها في مكتبة رقمية صغيرة [5].

الفرع الثاني

صعوبة فهم الدليل المتحصل من الوسائل الإلكترونية

إن من جملة المشاكل التي تطرحها الجريمة الإلكترونية ، هو ما يقع على القاضي الجنائي من حيث تقديره لأدلة الإثبات فضلا عن التثبت منها، وكذلك الاقتناع بها من أجل أن لا يدان بريء، أو يفلت

(1) - فيروز عوض عبدالكريم، إجراءات التحري وضبط في الجريمة الإلكترونية، اطروحة دكتوراه، جامعة شندي ، كلية الدراسات العليا والبحث العلمي قسم القانون، 2017 ، ص 75 .

(2) - عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الاثبات، دار الجامعة الجديد، الاسكندرية، 2010 ، ص 62.

(3) - لهوى رابح ، المصدر السابق، ص 32.

(4) - د. ميسون خلف أحمد الحمداني، مشروعية الادلة الالكترونية في الاثبات الجنائي، بحث منشور، مجلة البحوث والدراسات العربية، المجلد 18، العدد 2، 2016، ص 200 .

(5) - عائشة بن قارة مصطفى ، المصدر السابق، ص 34.

الجاني من العقاب . لذا سنبحث هذا الموضوع من خلال بيان مدى تفسير وقبول الدليل الإلكتروني في التشريعات المقارنة.

أولا : صعوبة فهم وتفسير الدليل الإلكتروني

إذا كانت الإدانة في الحكم الجنائي تبنى على الجزم واليقين فأن الحصول على الدليل الرقمي وحجيته أمام القضاء أمر تكتنفه الكثير من الإشكاليات، وذلك نتيجة لبعض الصعوبات:

1- الدليل الإلكتروني دليل يمكن إخفاؤه : إذا كانت الرقابة على الإنترنت ضعيفة فإن مرتكبي جرائم الإرهاب، أو الجرائم الإلكترونية عبر الفضاء الإلكتروني من التسلل والعبث في النبضات والذبذبات الإلكترونية التي تسجل عن طريق المعلومات والبيانات بغرض إحداث تغيرات في البيانات والمعلومات والتلاعب في منظومة الحاسب الآلي ومحتوياتها. كما يمكن بمجرد القيام بدس برامج خاصة من برنامجه فلا يشعر بها القائمون بتشغيل، الأمر الذي يمكن معه المجرمين أن ينجحوا في إخفاء ما قاموا به ومحو الدليل مما يتعذر من إعادة عرض أعمال التسلل والدخول، وذلك من خلال اخفاء أدلة الجريمة عبر الفضاء الإلكتروني و تشفير جهاز الحاسب الآلي أو تشفير القرص الصلب الخارجي أو تشفير المعلومات الموجودة على القرص الصلب الخارجي[1]، بالإضافة لعدم وجود أي بيانات تدل على صاحب أو مستخدم القرص الصلب الخارجي، وكذلك من ضمن الطرق المستخدمة في اخفاء الدليل الالكتروني قيام المجرم بخطوات تضليلية لإخفاء المواقع الارهابية، كما يمكن اخفاء الدليل الإلكتروني من خلال الاستعانة بفلاش ميموري (ذاكرة خارجيه) يتم نقل كل نشاط إجرامي فيها مما يسهل معه أن يتخلص منها وقت الضرورة[2].

2- غياب الدليل ضد متهم معين: وقد يتوصل المحقق لوجود جريمة إلكترونية، ولكن يصعب الوصول إلى مرتكبيها رغم وصول المحقق لأدلة على إرتكاب الجريمة، فقد لا تفصح الأدلة عن صلة شخص معين بالجريمة المرتكبة نظراً لان معظم نظم الحاسب الآلي لا تسمح للمراجعين والفنيين بالتتابع العكسي لمسار مخرجاتها، بالإضافة إلى صعوبة تتبع الآثار الإلكترونية ومراجعة وفحص الكم الهائل من البيانات والمعلومات الموجودة في الانظمة .

3- الكتابة على المساحة الفارغة للقرص الصلب وتضليل المحقق: قد يلجأ الجناة في الجرائم الإلكترونية إلى إستغلال المساحة الفارغة في القرص الصلب في تخزين أدلة إرتكابهم هذه الجرائم مما يعرقل عمل المحقق[3].

---

(1) - لهوى رابح، المصدر السابق، ص 38.
(2) - د. محمود رجب فتح الله، المصدر السابق ، ص 73.
(3) - د، محمود صالح العدلي ، المصدر السابق، ص 1239و 1240.

ثانيا : مدى قبول الدليل الإلكتروني

يُعد دليل الإثبات الإلكتروني حسب طبيعته قابلاً للتحريف، أو الإتلاف، أو التدمير، من خلال سوء المناولة أو الفحص بطريقة غير سليمة، ولهذا السبب ينبغي إتخاذ أحتياطات خاصة من أجل توثيق هذا النوع من أدله الإثبات وجمعه والحفاظ عليه وفحصه، وقد يؤدي عدم القيام بذلك إلى جعل هذا الأدلة غير صالحة للإستعمال أو يفضي إلى إستنتاجات غير دقيقة. ومع شيوع التطور التكنولوجي الحديث مثل الشبكات المخفية للهوية و التشفير عالي الدرجة، والعملات الأفتراضية في الجرائم التي تشمل أدلة جنائية إلكترونية، وهذا ما يوجب على المحققين أن إعتماد استراتيجية جديدة، وعلى سبيل المثال يمكن لسلطات إنفاذ القانون أن تعمل على تدعيم الشركات مع وجود فرق البحث الأكاديمي التي تركز على إستحداث منهجيات تقنية في مجالات مثل تحديد سمات المعاملات التي تجري بالعملات الأفتراضية ودراستها. وربما يتعين أيضاً على المحققين أن ينظروا في كيفية إستخدام أساليب التحري الخاصة مثل المراقبة والعمليات المستمرة وإستخدام المخبرين وتسليم المراقب في حالة بيع سلع غير مشروعة عبر الإنترنت جنبا إلى جنب مع التحريات الخاصة بالإنترنيت وتقنيات التحليل الجنائي الرقمي[1].

وتأسيساً على ذلك ترتبط عملية إثبات الجريمة بصفة عامة بإقامة الدليل، وذلك بالنظر إلى نوع الجريمة وإلى الإجراءات التي يتم إتباعها للحصول على الدليل، وهذه الخطوات هي المتبعة في في كل الجرائم، بما فيها الجرائم المرتكبة عبر الإنترنت، غير أنه في هذه الأخيرة تكون عملية استخلاص الدليل معقدة وتحتاج إلى ذوي الخبرة، وأن الحصول على الدليل عملية صعبة للغاية، لكون الأدلة في الجرائم الإلكترونية تتميز بخصوصية معنوية بالإضافة إلى ذلك فالإجراءات المتبعة في إثبات الأدلة أثبتت قصورها، فإذا كانت ذات فائدة في الجرائم التقليدية فهي غير مجدية في جرائم إنترنت في أغلب الأحوال، خاصة في ظل الطابع العالمي للجريمة الالكترونية، وذلك لعدة أسباب منها غياب الدليل المادي وسهولة إخفاء الدليل الإلكتروني، بالإضافة إلى قصور الإجراءات الجنائية لكونها من الجرائم العابرة للحدود[2].

(1) - ينظر: مؤتمر الأطراف في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية ، المصدر السابق، ص 4.

(2) - د. محمد ممدوح بدير، المصدر السابق، ص 175.

المطلب الثاني

أنواع الدليل الإلكتروني وإشكالية قبوله

تتنوع الأدلة الإلكترونية باختلاف نوع المعلومات والبيانات والأرقام ونوع الجريمة والوسائل التقنية الحديثة التي إرتكبت بها الجريمة في عالم افتراضي، فالدليل الإلكتروني لا يظهر بصورة ونوع واحد، بل له العديد من الأشكال والصور ولقد اختلف الفقهاء والباحثين في تقسيم تلك الأدلة. وهذا ما سبب إشكالية في مدى قبول وفاعلية تلك الادلة الإلكترونية ومدى مشروعيتها. وعلى ضوء ذلك سنقسم هذا الموضوع لفرعين، نتكلم في الفرع الاول عن أنواع الادلة المتحصلة من الوسائل الإلكترونية، ونخصص الفرع الثاني لدراسة إشكالية قبول الأدلة المتحصلة من الوسائل الإلكترونية .

الفرع الأول

أنواع الأدلة المتحصلة من الوسائل الإلكترونية ووسائل اثباتها

تطورت وسائل التحقيق الجنائي في عصر التكنولوجيا تطوراً ملموساً يواكب حركة الجريمة وتطور أساليب إرتكابها، فبعد أن كان الطابع المميز لوسائل التحقيق، العنف والتعذيب للوصول إلى الدليل، أصبحت المرحلة العلمية الحديثة القائمة على الإستعانة بالأساليب العلمية والتقنية وإستخدام شبكة الإنترنت هي الصفة المميزة والغالبة، ويرجع ذلك إلى حدوث طفرة علمية في مجال التكنولوجيا والمعلومات والإتصالات وإستخدام الوسائط المعلوماتية في شتى مجالات الحياة فكلما اكتشف العالم شيئاً حديثاً وجد هذا الاكتشاف طريقة إلى مجال الإثبات الجنائي والتدليل[1].

أولا : أنواع الدليل الإلكتروني

الإثبات في الجريمة الإلكترونية، يمتاز بخصيصة حديثة أفرزتها تقنية التبادل الاإكتروني من خلال ما تقدمه من بيانات ذات طبيعة غير تقليدية، فالأدلة الرقمية الجنائية لم يسبق أن جرى الإثبات التقليدي على إعتمادها، بل كانت الأدلة الكتابية والورقية هي المعتمدة في الأغلب، وعلى ضوء ذلك فإن الإثبات الجنائي يهدف إلى قبول الأدلة الإلكترونية، بوصفها صورة من صور الأدلة التي تعتمد لدى القضاء سواء بصورة كتابية أم بيانات رقمية، وتشمل هذه الأدلة جميع المستخرجات الإلكترونية أيا كان مصدرها، سواء كان الإنترنت، أم التلكس، أم الفاكس، أم أي برنامج، أو تطبيق إلكتروني[1].

---

(1) - د. علي هاشم عبد الحسن، الحماية الجزائية للأمن الأسري من التطور التكنولوجي ، المصدر السابق، ص127.

(1) - د. حسن فضالة موسى، التنظيم القانوني للإثبات الالكتروني، الطبعة الاولى، مكتبة السنهوري، بغداد، 2016 ، ص 40.

فالأدلة التقليدية تختلف عن الأدلة الرقمية، وكل منهما يختلف عن الآخر في سلامته ودرجة مقبوليته، وطبيعته، إذ إن إرتكاب الجريمة الإلكترونية يترك بصمة رقمية وعلى خلاف الأدلة المادية في الجرائم التقليدية، فهذه البصمات الرقمية غير المرئية، أو أنها مرئية أفتراضياً، وذات طبيعة متقلبة، ويمكن العثور على الأدلة الرقمية في ذاكرة تخزين المعلومات[1]. وهي قد تكون وحدات تخزين دائمة مثل (cd , and servers, hard desks) أو وحدات تخزين مؤقتة مثل (random access memory) وغيره. وهذه البصمات تأخذ إحدى ثلاثة أشكال: ملفات فعالة، ملفات مؤرشفة ، وملفات ممسوحة. **النوع الأول** الملفات الفعالة وهي عبارة عن ملفات يمكن الوصول إليها بسهولة ويسر ولا تحتاج إلى خبرة ومعامل جنائية، وعادة هي متاحة وغير محمية بكلمة السر، ويتم استعادتها دون اللجوء إلى المعامل. **أما النوع الثاني** من الملفات وهي الملفات المؤرشفة ، وهي المعلومات المخزنة في وحدات التخزين دائمة مثل (cd, flopy disk, network servers and the internet) مماثلة للنوع الأول، يمكن الوصول إليها بسهولة ويسر دون اللجوء إلى الخبرة والمعامل الجنائية لضبطها أو نسخها وهي أقل تقلباً من النوع الأول ،كونها موجودة في وحدة التخزين دائماً ويمكن طباعتها بسهولة. **أما النوع الثالث** من الملفات وهي المعلومات التي يتم مسحها والتي يمكن استرجاعها، ولكن بإستخدام تكنولوجيا هندسة المعلومات المتطورة، وهي على خلاف الاعتقاد السائد بأن المعلومات التي يتم مسحها وتفريق سلة المهملات منها ينعدم وجودها، بل هي تبقى مخزنة أوتوماتيكيا ولمدة مؤقتة في خوادم، وهي تبقى هناك حتى يتم تخزين ملفات جديدة فوق تلك الممسوحة، هذه الانواع الثلاثة تختلف طبيعتها حسب المكان الذي تخزن فيه، وحسب درجة تقلبها ويجب التعامل معها بحذر حتى لا يتم تدميرها أو تغيير طبيعتها، إذ إن المعلومات المخزنة سهل فقدها[2].وتأسيساً على ذلك سنقسم الأدلة الإلكترونية إلى قسمين هما:

1- أدلة لها حجية الإثبات: وهذا النوع من الأدلة الإلكترونية يمكن إجمالها كالآتي :

أ- الأدلة الرقمية الخاصة بأجهزة كمبيوتر- وهي السجلات التي تم انشاؤها بواسطة الحاسب الآلي تلقائيا، وتُعد هذه السجلات من مخرجات الألة التي لم يسهم الفرد في إنشائها مثل سجلات الهاتف وفواتير أجهزة الحاسب الآلي[1].

ب- الأدلة الرقمية الخاصة بالإنترنت[2].

---

(1) - د. محمد كمال شاهين، الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي، دار الجامعة الجديدة، 2018 ، ص 368.

(2) - مصطفى عبد الباقي، التحقيق في الجريمة الإلكترونية و إثباتها في فلسطين، المصدر السابق، ص 292.

(1) - د. لورنس سعيد الحوامدة، حجية الادلة الرقمية في الاثبات الجنائي، بحث منشور، مجلة البحوث الفقهية والقانونية، العدد السادس والثلاثون، 2021، ص 904.

(2) - فيروز عوض الكريم صالح، إجراءات التحري والضبط في الجريمة الالكترونية، المصدر السابق، ص74 .

ت- البيانات التي يتم إدخالها بواسطة أشخاص بصورة مكتوبة ، ولم يتم حفظها داخل الجهاز الرقمي، ومن أمثلتها رسائل البريد الإلكتروني ومواقع التواصل الإجتماعي وغيرها[1].

ث- الادلة الرقمية الخاصة بروتوكولات تبادل المعلومات – وهي السجلات التي يتم حفظها بالإدخال، وجزء منها تم إنشاؤها بواسطة الآلة، ومن أمثلتها، تلك البيانات التي يتم إدخالها إلى الآلة وتتم معالجتها من خلال برنامج خاص، كإجراء العمليات الحسابية على تلك البيانات[2].

ج- الأدلة الرقمية الخاصة بشبكات الإتصال العالمية للمعلومات. وفقا للإتفاقية الاوربية لمكافحة الجرائم الإلكترونية، فقد جاء بنص المادة (1) منها: يقصد بالبيانات المتعلقة بالمرور (donnees relatives au trafic) مجمل البيانات التي تتعامل مع الإتصال والتي تمر من خلال نظام معلوماتي، أو يتم إعدادها بواسطة هذا الاخير والذي يُعد عنصراً في سلسلة الإتصال بالإشارة إلى مصدر الإتصال، مكان الوصول، خط السير، الساعة، التاريخ، الحجم، مدة الإتصال، نوع الخدمة[3].

2- أدلة لم تعد لتكون وسيلة إثبات: وهذا النوع من الأدلة الإلكترونية ينشأ دون إرادة الشخص، أي أن هذه الأدلة هي أثر يتركه الجاني دون أن يكون راغباً في وجوده، ويسمى هذا النوع من الأدلة بالبصمة الرقمية، وهي ما يمكن تسميته أيضا بالأثار المعلوماتية الرقمية، وهي تتجسد في الآثار التي يتركها مستخدم الشبكة الإلكترونية بسبب تسجيل الرسائل المرسلة أو التي يستقبلها، أو كافة الإتصالات التي تتواجد من خلال الحاسب الآلي أو الشبكة المعلوماتية العالمية [4]. وفي واقع الأمر إن مثل هذه الأدلة لم يعد أساساً للحفظ من قبل من صدر عنه، غير أن الوسائل التقنية الخاصة تمكن من ضبط هذه الأدلة ولو بعد فترة زمنية من انشاؤها[5].

وعلى أساس ذلك فإن التمييز بين هذين النوعين من الأدلة مهم وله ضرورة في الإثبات الجنائي وذلك من خلال :

أ- النوع الثاني من الأدلة الإلكترونية هو الأكثر أهمية، لكونه لم يعد أصلاً ليكون أثراً لمن صدر عنه ولا يمكن الاخذ به في الإثبات الجنائي، ولكن من الممكن الأخذ به للكشف عن الجريمة فقط[1].

ب- يتميز النوع الأول من الأدلة الإلكترونية بسهولة الحصول عليه لكونه قد أعد أصلاً ليكون دليلاً على الوقائع التي يتضمنها ، ومن ثم يمكن الإستناد اليه للإثبات الجنائي[2] .

---

(1) - لهوى رابح، المصدر السابق، ص 54.
(2) - د. ميسون خلف حمد الحمداني، المصدر السابق، ص 198.
(3) - لهوى رابح ، المصدر السابق، ص 50.
(4) - محمد بن ناصر بن علي الرقيشي ، المصدر السابق ، ص 41.
(5) - الحسن الطيب عبد السلام الأسمر ، المصدر السابق، ص 60 .
(1) - عائشة بالقارة ، المصدر السابق، ص 41 .
(2) - أمير فرج يوسف، المصدر السابق، ص 290.

ت- النوع الأول من الأدلة الرقمية الجنائية أعد ليكون وسيلة إثبات لبعض الوقائع، أي أنه عادة ما يؤخذ به للإحتجاج به لاحقا، وهو ما يقلل من إمكانية فقدانه، على عكس النوع الثاني من الادلة الإلكترونية، إذ انه لم يعد ليحفظ ، ما يجعله عرضه للفقدان لأسباب كثيرة إذ إن هذا النوع من الأدلة لم يعد اساساً للحفظ من قبل من صدر عنه، غير أن الوسائل الفنية الخاصة تمكن من ضبط هذه الأدلة ولو بعد فترة زمنية من نشوئها فالاتصالات التي تسجل عبر الإنترنت والمراسلات الصادرة عن الجهات التي يتلقاها يمكن ضبطها بواسطة تقنية خاصة بذلك [1].

ومن الجدير بالذكر فقد عدّ (المشرع الاردني)، أن المواقع الإلكترونية كالمطبوعات، إذ يسري عليها قانون المطبوعات والنشر، وقد عرف الديوان الخاص بتفسير القوانين، المطبوعات بأنها: كل وسيلة نشر دونت فيها المعاني أو الكلمات أو الأفكار بأي طريقة من الطرق بما فيها الوسائل الإلكترونية أو الرقمية أو التقنية. وقد أبدت محكمة التمييز الأردنية في احدى أحكامها، إذ خلصت إلاّ أن (الموقع الإلكتروني هو وسيلة من الوسائل التي يتم فيها تدوين الأفكار والمقالات ونشرها، ومن ثم فإن المواقع الإلكترونية تعتبر من المطبوعات وفقا لتعريف المطبوعات الوارد في قانون المطبوعات والنشر و تخضع لأحكامه). وعلى اساس ذلك فأن الأدلة الرقمية تلعب دوراً كبيرا في إثبات الجرائم في الدول المتقدمة مع تنامي ظاهرة الجرائم الإلكترونية وتطور وسائل مؤسسات انفاذ القانون في الإثبات[2].

وتتمثل أشكال الدليل الرقمي (الإلكتروني) على ثلاثة أشكال رئيسية وهي (الصور الرقمية والتسجيلات والنصوص المكتوبة)، فالصور الرقمية وهي عبارة عن تجسيد للحقائق المرئية حول الجريمة، وفي العادة تقدم الصورة، أما في شكل ورقي، أو في شكل مرئي بإستخدام الشاشة المرئية، والواقع أن الصورة الرقمية تمثل تكنلوجيا بديلة للصورة الفوتوغرافية التقليدية، والتي تبدو أكثر تطوراً لكنها ليست بالضرورة أفضل من الصور التقليدية[1]. أما التسجيلات الصوتية فهي التي يتم ضبطها وتخزينها بواسطة آلة رقمية وتشمل المحادثات الصوتية على الإنترنت والهاتف وباقي الأجهزة التقنية الحديثة. أما النصوص المكتوبة وتشمل النصوص التي يتم كتابتها بواسطة الآلة

(1) - ابراهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، اطروحة دكتوراه، جامعة مولود معمري – تيزي وزو، كلية الحقوق والعلوم السياسية، 2018، ص 130.
(2) - د. سحر سعد عبد السميع ، المصدر السابق، ص 285 .
(1) - د. علي هاشم عبد الحسن، المصدر السابق، ص 137 .

الرقمية ومنها الرسائل عبر البريد الإلكتروني، والهاتف المحمول، والبيانات المسجلة بأجهزة الحاسب الآلي[1].

ثانيا : وسائل الحصول على الدليل الإلكتروني

لكي تكون الأدلة لها قوة الإثبات والحجية عنده إصدار الحكم القضائي. فلابد أن تكون هناك طريقة صحيحة وسليمة لإستخراج تلك الأدلة الإلكترونية، ومن هذه الطرق هي: مصادر الحصول على الدليل الإلكتروني: إذ إن الحصول على الدليل الالكتروني يكون من خلال اللجوء إلى الطريقة التي ارتكبت فيها الجريمة و تنحصر تلك الادلة في المتهم المشتبه به المجنى عليه ومقدم خدمة الإنترنت، وهذه الأدلة على سبيل المثال وليس الحصر، إذ إن التطور العلمي والتقني والتكنولوجي قد أسفر عن أنواع جديدة من هذه الأدلة. منها الكمبيوتر الخاص بالمتهم المشتبه به: مما لا شك فيه أن المجنى عليه هو المصدر الكاشف والنتيجة التي يترتب عليها ما قام به المشتبه من جرائم والمجنى عليه قد يكون شخصاً طبيعياً أو مؤسسة خاصة أو عامة أو مؤسسة مالية أو هيئة حكومية وغيرها، ومن ثم فان فحص مثل تلك الأجهزة يمكن المحقق من معرفة الدخول وتتبع مصدر المشتبه فيه. وكذلك مقدم خدمة الإنترنت: يمكن الإستعانة أيضا في كشف الأدلة الإلكترونية بعدة جهات أخرى مثل مقدم خدمة الإنترنت مثل شركة Yahoo أو Google أو msn فإن مثل تلك الشركات يتم تسجيل البيانات الخاصة بمستخدميها ، ومن ثم يمكن اللجوء إليها للتعرف على هوية المجرم المشتبه فيه، وكذلك البريد الإلكتروني على شبكة الإنترنت وذلك إذ انه عن طريق البريد الإلكتروني يمكن التعرف على البيانات الشخصية ومنه نستطيع تحديد هوية المشتبه فيه عن طريق صندوق الرسائل الواردة إليه والمرسلة منه ، ومن ثم يتم تحديد مكانه وموقعة[2].

بالإضافة إلى البرامج المستخدمة في جمع الأدلة، هناك عادة ما توجد أدلة الإلكترونية في مخرجات الطابعة والتقارير والرسوم وفي أجهزة الكمبيوتر وملحقاتها وفي الأقراص المرنة والصلبة وأشرطة تخزين المعلومات، وفي أجهزة المودم والبرامج و أجهزة التصوير مواقع الويب والبريد الإلكتروني، ولذلك تستخدم عدة طرق أو أدوات تُسهم في جمع الأدلة الرقمية ومنها (برنامج إذن التفتيش) - وهو برنامج قاعدة بيانات يسمح بإدخال كل المعلومات المهمة المطلوبة لترقيم الادلة، وتسجيل البيانات منها ويمكن لهذا البرنامج أن يصدر إشارات بإستلام الأدلة المضبوطة لتحديد مكان دليل معين أو تحديد ظروف ضبط هذا الدليل. وكذلك قرص بدء تشغيل الكمبيوتر ، وهو قرص يسمح للمحقق من تشغيل الحاسب الآلي، إذا كان نظام التشغيل فيه محمياً بكلمة مرور، ويجب أن يكون القرص مزوداً

(1) - د. سحر سعد عبد السميع ، المصدر السابق، ص 286.
(2) - باقر غازي حنون ، المصدر السابق، ص 201 .

ببرنامج مضاعفة المساحة. وأيضاً برنامج النسخ (lap link)، وهو برنامج يمكن تشغيله من قرص مرن ويسمح بنسخ البيانات من الحاسب الآلي الخاص بالمتهم ونقلها إلى قرص آخر، سواء على التوازي، أم على التوالي، وهو برنامج متطور يفيد للحصول على نسخة من المعلومات قبل أي محاولة لإتلافها من جانب المتهم[1]. وكذلك برنامج كشف الدسك – ومن خلال هذا البرنامج يمكن الحصول على محتويات القرص المرن، مهما كانت أساليب تهيئة القرص. وايضاً يوجد برنامج الإتصالات – وهذا البرنامج يستطيع ربط جهاز الكمبيوتر الخاص بالمحقق بجهاز حاسب المتهم لنقل ما يحتويه من معلومات ، وبيانات ويحفظها في جهاز نسخ المعلومات ومن ثم إلى القرص الصلب، ويمكن القول أن هذه الطريقة تُعد من أهم الطرق التي يلجأ اليها المحقق لجمع الادلة الإلكترونية[2].

وتجدر بالإشارة إلى أن بعض التشريعات المقارنة، أتاحت للسلطات القضائية صلاحيات واسعة تدخل ضمن القواعد الإجرائية والتي تخول القائم بها للوقاية من الجرائم الإلكترونية، إذ تمكن هذه الصلاحية السلطات القضائية من تعقب الجناة والوصول إلى الادلة التي تدينهم، وتتمثل هذه الإجراءات، بمراقبة الاتصالات الإلكترونية و تجميع وتسجيل محتواها. وتفتيش المنظومات المعلوماتية بوصفها الأداة التي تخزن فيها المعطيات المعلوماتية [3]. وأيضا تفتيش منظومة تخزين المعلومات على غرار قواعد البيانات ، إذ تمثل مصدرا مهماً للمعطيات. وكذلك حجز المعطيات المعلوماتية التي تفيد في الكشف عن الجرائم أو مرتكبيها ويتم حجزها بأخذ نسخة عنها وتخزينها في دعامة إلكترونية. والمنع من الوصول إلى المعطيات المعلوماتية التي تفيد في الكشف عن الجرائم ومرتكبيها متى تعذر نسخة على دعامه إلكترونية. بالإضافة إلى المنع من الوصول إلى المعطيات المعلوماتية التي تفيد في الكشف عن الجرائم أو مرتكبيها والتي يُعد محتواها جريمة بحد ذاتها على غرار المواد الاباحية الضارة[1].

ثالثا : صعوبة الوصول إلى الدليل الإلكتروني

إن حفظ الأدلة الإلكترونية في جهاز الحاسب الآلي والأجهزة التقنية الحديثة، من العمليات المعقدة التي تحتاج إلى إجراء فني دقيق للحفاظ على صحة البيانات التي يحتوي عليها الحاسب الآلي ، وهذا

(1) - ينظر : د. خالد ممدوح ابراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، 2009، ص 214 وما بعدها.
(2) - باقر غازي حنون ، المسؤولية الجنائية الناشئة عن الابتزاز الالكتروني، رسالة ماجستير، جامعة البصرة، كلية القانون، 2020، ص 203.
(3) - د. عفيفي كامل عفيفي ، المصدر السابق، ص 473.
(1) - د. مفيدة مباركية ، الادلة الجنائية الرقمية والحق في الخصوصية، بحث منشور، مجلة المعيار، المجلد 25، العدد 58، 2021، ص 562.

الأمر يتطلب بالضرورة قيام الخبير التقني بالكشف بداية على صحة المعلومات والبيانات الموجودة في الحاسب الالي، سيما من حيث الخلل والعطب، مثال على ذلك الفيروس العدواني يُعد مثالاً واقعياً، فالأخير يمكن أن يسبب خللاً وعطلا لبعض البيانات في جهاز الحاسب الآلي، وفي هذه الحالة يتم التشكيك في صحة الأدلة الموجودة في الحاسوب[1]. وقد تتعدد عملية حفظ الأدلة داخل جهاز الحاسوب بأساليب متعددة تتمثل في أبسط مظاهره بإستخدام أسلوب الحفظ العادي، وأقوى مظاهرها في عمليات حجز الحاسوب على الدليل الموضوع فيه، ذلك أن الدليل الرقمي هو في ملف يحتوي على بيانات رقمية تعطي مظهراً معلوماتياً محدداً وغير قابل للتحويل إلى مظهر آخر، إلاّ بإجراء تعديلات رقمية في البيانات المذكورة[2]، أما بالنسبة لعملية حفظ الأدلة في العالم الرقمي، فإنه يتطلب من الخبير التقني القيام برصد موقع الإنترنت أو المعلومات التي تشير إلى الجريمة، والتي تكون في مظاهر مختلفة الأشكال كما لو كانت جريمة من جرائم القذف والسب في غرفة المناقشة ففي هذه الحالة الاخيرة يتم الرجوع إلى ذاكرة الخادم الذي يتولى ربط هذه الغرف عبر العالم الرقمي، لكي يمكن التوصل إلى تحديد موضوع السب والقذف وتاريخه، وإذا كانت الجريمة من جرائم النشر عبر الإنترنت، فقد يكتفي مجرد اللجوء إلى ذاكرة الحاسب الآلي المستخدم هنا دون الحاجة إلى تحديد الخادم. وتستدعي عملية حفظ الأدلة في العالم الرقمي لزوم قيام الخبير التقني بعرض الأدلة أمام المحكمة وعلى جهات التحقيق، وفي مثل هذا الأمر يجعل عمل الخبير يستمر لمرحلة المحاكمة وأحيانا يتطلب منه ذلك القيام بعمله لمرحلة ما بعد المحاكمة كما هو الشأن حال عرض الدليل المقدم إلى محكمة الموضوع أمام الجهات القضائية أو أمام جهة قضائية أعلى كالاستئناف أو النقض لدرء المشاكل التي يمكن أن تنجم عن حفظ الأدلة في العالم الرقمي[1]. وأما بالنسبة لعملية الحصول على مخرجات الحاسب الآلي والإنترنت بقصد تقديمها إلى المحكمة كدليل فهي تعد من أهم الموضوعات التي تعرض لها الفكر القانوني سواء من حيث قابليتها القانونية أو من حيث منهجية الدليل الذي تم تخريجه وعلى ضوء ذلك يقوم الخبير بتخريج هذه المخرجات إلى العالم المادي بطرق مختلفة أبرزها في العمل هي الطباعة وذلك بتحويلها إلى نسخ ورقية عوضا عن كونها رقمية أو نقدية والخبير في ذلك لا يكتفي بمجرد نسخ لبعض المعلومات وإنما يحتاج أيضا إلى تخريج النبض الرقمي إذ يقوم بتخريج كافة البيانات الرقمية حين طباعة هذا الدليل[2]. وايضا من الصعوبات التي تواجه المشرع أو

(1) - د. عمر محمد بن يونس، مذكرات في الاثبات الجنائي عبر الانترنت، بلا، 2006 ، ص12.

(2) - هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الالات الحديثة، اسيوط، 1994، ص 16.

(1) - د. عبدالفتاح بيومي حجازي، مبادئ الاجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، الإسكندرية،2006، ص 79.

(2) - د. حسين بن سعيد الغافري، ، المصدر السابق، ص 460 وما بعدها.

المحققين أو أعضاء الضبط القضائي هو ضخامة كم البيانات الواجب التحقيق فيها. وتعرف البيانات بأنها (مجموعة من بطاقات تشمل بيانات معدلة ومنظمة تسمح باقتطاع البيانات حسب رغبة المستعمل)، ومصطلح قاعدة أو بنك البيانات شاع استعماله وربما يعني لمعظم الناس بأنه نوع من الحاسب تجمع فيها كل أنواع المعطيات الخاصة يتم الرجوع إليها عند الحاجة[1]، ولذلك يشكل الكم الهائل للبيانات التي يجري تداولها في الأنظمة المعلوماتية إحدى الصعوبات البارزة التي تعيق التحقيق في الجرائم التي تقع عليها أو بواسطتها، إذ عادة ما يتطلب البحث عن الأدلة في حاسب واحد، الاطلاع والفحص الدقيق لكل المعطيات التي تتضمنها الاف الملفات المخزنة في ذاكرة الحاسب الآلي يكلف المحقق وقت وجهد كبيرين، وهو ما قد ينعكس سلباً على مردود سلطات البحث والتحقيق من ضجر وملل، ويؤدي بهم إلى التخلي عن مواصلة البحث والتحقيق. ويزداد الأمر أكثر تعقيداً حينما يكون محل البحث هو الشبكة المعلوماتية (الإنترنت) ، إذ يصبح الأمر في غاية الصعوبة عندما يكون أعضاء الضبط القضائي لا يمتلكون الخبرة الفنية والتقنية على إعتبار أن إجراءات التفتيش والضبط في هذا الفضاء الأفتراضي يستدعي من المحقق تصفح عدد هائلٍ من المواقع وصفحات الإنترنت وفحص عددٍ ضخم من البيانات، مما يسبب له إرهاقاً شديداً قد يدفعه إلى الخروج عن ضوابط البحث والتفتيش القانونية، للبحث عن الدليل، ما يجعل القضاء والمحققين لا يكترثون بالدليل الإلكتروني المتحصل من هذه العملية لإفتقاده لشروط المشروعية والمصداقية التي تجعله جديراً بالثقة[2]. وقد تزايدت صعوبات الاثبات وإستخلاص الدليل الإلكتروني بسبب ظهور أساليب جديدة لتطوير البرامج الضارة والتي أصبحت جماعات الجريمة المنظمة تلجأ إلى أساليب تشبه أساليب (الكي جي بي)[1] لاستقطاب الاجيال الجديدة من المتسللين لكتابة البرامج الضارة. وأن الانتشار الكبير للإنترنت في الحياة العملية أظهر الحاجة في وضع الحلول العملية للمشاكل الناتجة عن إستخدام الإنترنت في ضوء القواعد العامة للقانون، إضافة إلى أهمية توجيه نظر المشرع للتدخل ولوضع قواعد خاصة لتنظيم إستخدام الإنترنت في بعض المجالات الحيوية واستخلاص القواعد

---

(1) - فايز خليفة أحمد بن يعروف، المواجهة التشريعية والأمنية للجرائم المتصلة بمواقع التواصل الاجتماعي، وزارة الداخلية أدارة مركز البحوث، الشارقة، 2019 ، ص 198 .

(2) - صغير يوسف، الجريمة المرتكبة عبر الانترنت، رسالة ماجستير، جامعة مولود معمري وزو، كلية الحقوق والعلوم السياسية، 2013 ، ص 128 .

(1) - هو اختصار لمصطلح يخص جهاز المخابرات الروسي، استعمل اثناء فترة الاتحاد السوفيتي والحرب الباردة، وتعني لجنة أمن الدولة، ويتمثل دور هذا الجهاز بمراقبة المجتمع وحماية المسؤولين الكبار في الدولة. انظر : https://ar.wikipedia.org/wiki/%D9%84%D8%AC%D9%86%D8%A9_%D8%A3%D9%85%D9%86_%D8%A7%D9%84%D8%AF%D9%88%D9%84%D8%A9_(%D8%A7%D9%84%D8%A7%D8%AA%D8%AD%D8%A7%D8%AF_%D8%A7%D9%84%D8%B3%D9%88%D9%81%D9%8A%D8%AA%D9%8A) تم زيارة الموقع بتاريخ 2022/9/15.

الرئيسة في هذا المجال والتي يمكن للمشرع أن يستهدي بها إذا ما أراد يوما تنظيم مجال من مجالات استخدام الإنترنت بقواعد خاصة كالإثبات، وكذلك بيان الأحكام القانونية لإستخدام الإنترنت في بعض المجالات[1].

أما (فرنسا) فقد أكدت في سياق نداء باريس من أجل فرض الثقة والأمن في الفضاء السيبراني إلى جانب أكثر من (60) دولة أخرى، وعدة مئات من المنظمات الدولية وممثلي المجتمع المدني والقطاع الخاص ، دعمها لفضاء إلكتروني، مفتوح وآمن ومستقر وميسر وسلمي يكون فيه القانون الدولي منطبقا بما في ذلك حقوق الإنسان. وفي هذا المجال أشارت فرنسا بأنها شرعت نظاماً وطنياً قوياً في مجال مكافحة الجريمة الإلكترونية، من حيث القانون المطبق حاليا، والتدابير الوقاية المتخذة، والموارد المخصصة للمحققين والقضاة لمكافحة هذه الظاهرة بفعالية، وقد اقتبست هذه الآلية جزئياً من أحكام اتفاقية مجلس أوروبا المتعلقة بالجريمة الإلكترونية. وبناء على ذلك فالتحدي الدائم لمكافحة الجريمة الإلكترونية يتمثل في التكييف مع التكنولوجيا الجديدة، لا سيما العملات المشفرة التي تخضع لتنظيم جزئي فقط، مما يؤدي إلى مخاطر كبيرة تتمثل في إخفاء هوية أصحاب التدفقات المالية، ومع وجود وتطور الشبكة الخفية، ونظام التشفير والإنترنت وغيرها، وجميع هذه الأشياء يصعب إثبات الأدلة فيها[2].

أما (العراق) فقد ركز المشرع العراقي على قضايا الأمن العام، وأكد على أن شركات الإنترنت الكبرى تقدم الخدمات وفرصاً كبيرة للتنمية الإجتماعية والأقتصادية، ولا تكون المنصات القائمة على الإنترنت مناسبة للتنمية الإجتماعية والأقتصادية، إلاّ عندما يعرض مستخدموها أنفسهم بصدق، بيد أنهم عندما يستخدمون اسماً مجهولاً أو مزيفاً، وهو أمر شائع جدا في وسائل التواصل الإجتماعي، فقد يسيئون إستخدام هذه الخدمات ويقومون بأنشطة إجرامية مثل نشر خطاب الكراهية، ورسائل التهديد والإبتزاز، ويشكل ذلك تحدياً صعباً في مجال الأمن العام بالنسبة لحكومات البلدان النامية.

وأشار العراق أيضاً إلى وجود بعض التحديات الأخرى التي تواجه مكافحة إستخدام تكنولوجيا المعلومات، والجرائم الإلكترونية، وذلك من خلال عدم وجود إتفاقية عالمية، بشأن الجريمة الإلكترونية وصعوبة فهم الأدلة الرقمية أو فهم جزء منها، وسهولة إتلافها أو إخفائها، وكون الجرائم الإلكترونية تتجاوز الحدود الجغرافية، إلى جانب وجود مسافة جغرافية بين المجرم والضحية،

(1) - عبدالله دغش العجمي، المشكلات العملية والقانونية للجرائم إلكترونية ، رسالة ماجستير، جامعة الشرق الاوسط، كلية القانون، 2014، ص 113.

(2) - ينظر : التقرير الصادر عن الامم المتحدة/ الجمعية العامة ، الدورة الرابعة والسبعون، مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الاجرامية، 2019، ص 32.

وافتقار السلطات المختصة إلى التدريب المناسب وبناء القدرات اللازمين لمكافحة الجريمة الإلكترونية، وكون الخبرة والدراية في مجال التحقيق في هذه الجرائم من قبل المنظمات غير الحكومية و الكيانات الحكومية الأخرى، لا تستخدم على نحو كاف، وعدم توفر بنية تحتية إلكترونية كافية لمكافحة الجريمة الإلكترونية، وهذا ما يسبب صعوبة في مكافحة الجرائم الإلكترونية بسبب عدم الوصول إلى أدلة رقمية جنائية لها قوة الاثبات في القانون[1].

وتجدر بالإشارة إلى أن أهم وأبرز الصعوبات التي تواجه المحققين والجهات القضائية للوصول إلى الأدلة الإلكترونية التي تفيد في كشف الجريمة هو عدم تحقق التعاون الدولي، ولهذا الموضوع أهمية بارزة في مجال مكافحة الجريمة الالكترونية، وذلك بعد أن أصبحت الاخيرة تتخطى حدود الدول والتي لم تقف حائلا أمامها، وأبرز وأوضح مثال على ذلك الجرائم الإلكترونية. وعلى الرغم من كون التعاون والتنسيق بين أعضاء المجتمع الدولي يتقدم وبشكل مشجع بشأن مكافحة الجرائم الإلكترونية بصورة عامة، إلاّ أنه ليس بالمستوى الذي يسمح بإيجاد نظام جنائي فعال يوازي التقدم التكنولوجي الذي يشهده العالم إذ أن الوسائل والتدابير المتخذة في هذا المجال وعلى الرغم من جديتها إلا أنها لا ترتقي إلى مستوى التحدي ومكافحة هذه الجرائم ومنها الجرائم العابرة للحدود. من جانب آخر وجدت العديد من العراقيل التي تحول دون إتمام عملية التعاون الدولي في هذا المجال، ومنها القلق الذي يراود الدول من القانون الجنائي الدولي، وذلك بسبب اختلاف السياسة الجنائية بين الدول واختلاف المجتمعات، وفي الوقت الحاضر يتم التنسيق بين الدول ذات الأنظمة الجنائية المتعددة، وذلك من خلال اتخاذ عدد من التدابير لتطوير التعاون الأمني والقضائي وبشكل يسمح لكل دولة الاحتفاظ بخصوصيتها[1]. فيما يرى بعضهم بأنه مباح عبر الانترنيت، فيراه بعضهم الآخر بأنه غير مباح، ومن ثم يطبق التجريم عليه، ويرجع السبب في ذلك إلى طبيعة النظام القانوني السائد لكل دولة أو إلى أختلاف البيئة والعادات والتقاليد والأديان والثقافات من دولة إلى أخرى، بل من مجتمع إلى اخر. ومن ثم اختلاف السياسة التشريعية[2]. ولعل هذا الأختلاف قد أتاح الفرصة لمرتكبي الجرائم الإلكترونية على تنظيم أنفسهم لإرتكاب الجرائم بشكل عابر للحدود الدولية، ومن بين الصعوبات التي تقف أمام التعاون الدولي بشأن الجرائم الإلكترونية هو غموض المفاهيم القانونية أو أختلافها، والسبب في ذلك هو عدم الإتفاق على مفهوم واحد للجريمة الإلكترونية إذ إن الاختلاف في تعريف الفعل المجرم يُعد سببا في فشل الجهود الدولية في إيجاد إتفاقية دولية لمكافحتها بل فلم تضع الأنظمة القانونية في الدول صيغة محددة لإساءة استخدام الحاسوب أو نظم المعلومات عبر الشبكة العالمية

(1) - ينظر: تقرير صادر عن الامم المتحدة/ الجمعية العامة، الدورة الرابعة والسبعون، المصدر السابق، ص45.
(1) - ينظر: لينا محمد الاسدي ، المصدر السابق، ص 251 وما بعدها.
(2) - د. رامي متولي القاضي ، المصدر السابق، ص 259.

الإنترنت، فضلا عن اختلاف النظام الإجرائي الجنائية التي يتم اتباعها في البحث والتحري والتحقيق في الجرائم في الإجراءات الجنائية التي يثبت فائدتها في دولة ما، وقد تكون غير ذي فائدة في دولة أخرى، وقد لا يسمح للجهات المختصة بالتحقيق بأجرائها أصلا. كما يلعب غياب المعاهدات الثنائية، أو الجماعية بين الدول التي تحارب من خلالها الجريمة الإلكترونية دوراً مهماً، وفي حال انعقادها فإنها تكون قاصرة على تحقيق الهدف المرجو منها، والسبب في ذلك هو التقدم المستمر والسريع لنظم وبرامج الحاسوب وشبكة الويب العالمية، ويواكبها نتيجة لذلك الجريمة الإلكترونية مما يؤدي إلى تلكؤ عمل المشرع والجهات المختصة في هذا المجال، وفي هذه الحالة إذا كان الامر يتعلق بالجريمة الإلكترونية مع بطء وتعقيد الإجراءات الاخيرة، فهذا الامر ينعكس وبشكل سلبي على الجرائم المتعلقة في الحاسوب والإنترنت، وذلك نظراً لطبيعة الإنترنت وما يتميز به من سرعة فائقة وتطور كبير[1].

وتأسيساً على ما تقدم ، يمكن إجمال أهم الاسباب التي تمثل صعوبة إثبات الدليل الإلكتروني في الجرائم الإلكترونية هي :

أ- عدم ترك الجاني لأي آثار للدليل الرقمي الالكتروني، يدل على ارتكابه لفعله الاجرامي، فالجرائم التي تتم بواسطة إدخال الرموز والارقام هي رموز دقيقة ويصعب اكتشافها وإثباتها ، لهذا عادة ما يتم اكتشافها بالصدفة.

ب- الجريمة الإلكترونية، لا تترك آثاراً ملموسة وبذلك لا تترك شهوداً يمكن الإستلال بأقوالهم ولا بأدلة مادية يمكن فحصها، لأنها تقع في بيئة أفتراضية يتم فيها نقل المعلومات وتناولها بواسطة نبضات الإلكترونية غير مرئية.

ت- إن وسيلة التنفيذ فيها 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.

ث- يصعب العثور على الدليل الرقمي الجنائي للجريمة وذلك راجع إلى إستخدام الجاني وسائل فنية وتقنية معقدة لا يستغرق الاّ ثواني معدودة يتم فيها محو الدليل والتلاعب به.

ج- الدليل الإلكتروني يتطلب خبرة وتحكما في التكنولوجيا المعلوماتية عند متابعتها ولذلك لا يستطيع رجال الضبط القضائي التعامل بأحترافية ومهارة أثناء البحث والتحري.

(1) - لينا محمد الاسدي ، المصدر السابق، ص 253.

الفرع الثاني

إشكاليات قبول الأدلة المتحصلة من الوسائل الإلكترونية كدليل

يواجه الدليل الإلكتروني في ظل نظام الإثبات الجنائي، العديد من المشاكل خاصة في ما يتعلق بالقواعد التي تخص مضمون الأدلة كقاعدة استبعاد شهادة السماع ، ومادام الدليل الالكتروني الجنائي في أصله يمثل شهادة سماع، وهذا بإعتبار أنه يتكون من جمل وكلمات وصور وغيرها، أدخلها شخص إلى جهاز الحاسب الآلي، سواء تمت معالجة البيانات أم لا، هذا الأمر من شأنه أن يخلق اعتراضاً على قبول المستندات المطبوعة التي يخرجها الحاسوب في الإثبات أمام القضاء الجنائي[1]، أما فيما يخص القواعد المتعلقة بكيفية تقديم الادلة للقضاء، وكذلك تحديد مدى قبول هذه الأدلة في الاثبات الجنائي، هناك قاعدة الدليل الأفضل أو المحرر الأصلي ولو تم تطبيق هذه القاعدة على الدليل الإلكتروني لتم إستبعاده كوسيلة إثبات في هذا النظام ،وهذا الامر أدى إلى تخوف رجال الضبط القضائي والمدعين العموميين والقضاة، من أن تكون مخرجات الطباعة والمخزنة على الحاسوب غير أصلية ولا تُعد هذه النسخة الحقيقية، والسبب وراء هذا الأمر هو أنه غالبا ما يتم عرض الدليل الإلكتروني أمام القضاء في شكل مستندات مطبوع أو كيانات معروض على شاشة الكمبيوتر[2]. كما أن الأصل في الدليل الإلكتروني عبارة عن مجرد شعارات إلكترونية ونبضات ممغنطة لا ترى بالعين، وهذا مما لا يتيح للقاضي وضع يده على الدليل الاصلي، وما يتم تقديمة للمحكمة من وثائق تم إخراجها من الحاسب الآلي إلاّ نسخاً عن الاصل مما يجعله دليلا ثانوياً لا اصلياً، وهذه النسخ لا تقدم البيانات التي يتضمنها الدليل الأصلي، ومثال على ذلك فالوثيقة المطبوعة من وثائق لا تظهر جميع التعديلات والملاحظات في حالة وجود تغيير في الدليل الاصلي، وكما أن الدليل الأصلي في بعض العمليات التي تتم من خلال الحاسوب قد لا تعود موجودة كما هو الحال في التحليلات أو الإسقاطات المعالجة[1].

أولا : شروط وضوابط الحصول على الدليل الإلكتروني

يشترط في الدليل الإلكتروني الجنائي عموماً لقبوله كدليل إثبات أن يتم الحصول عليها بطريقة مشروعة، وذلك يقتضي أن تكون الجهة المختصة بجمع الادلة قد إلتزمت بالشروط التي يحددها القانون في هذا الشأن، على عكس إثبات الجرائم المرتكبة عبر الإنترنت، إذ لا تقف الصعوبة فيها عند التعذر للوصول إلى الأدلة التي تكفي لإثباتها، وإنما تمتد هذه الصعوبة لتشمل إجراءات الحصول

(1) - طوني ميشال عيسى، التنظيم القانوني لشبكة الانترنت، الطبعة الاولى، 2001، ص 337.
(2) - خالد ممدوح ابراهيم، ابرام العقد الالكتروني، دار الفكر الجامعي، الإسكندرية، 2008، ص 245.
(1) - د. ميسون خلف أحمد الحمداني ، المصدر السابق، ص 202.

على هذه الأدلة، فإذا كان من السهل على الجهات التحري أن تتحرى عن الجرائم التقليدية عن طريق المشاهدة والتتبع والمساعدة فإنه قد يصعب عليها القيام بهذا التحري وبهذه الطرق بالنسبة إلى الجرائم الالكترونية [1].

وتأسيساً على ما تقدم فإنه لا يمكن الأخذ بالأدلة الرقمية الجنائية كدليل براءة أو بالإدانة من قبل قاضي محكمة الموضوع إلاّ وفق شروط معينة ثابتة، وتتمثل هذه الشروط : في أن تكون هذه الأدلة يقينية ، وهذا يستوجب أن تقترب نحو الحقيقة الواقعية قدر المستطاع وأن تبتعد عن الظنون والتخمينات، ويترتب على ذلك أن كافة المخرجات والوسائل الإلكترونية من مخرجات ورقية أو إلكترونية أو أقراص مغناطيسية أو مصغرات فيلميه تخضع لتقدير القاضي الجنائي، ويجب أن يتم استنتاج الحقيقة بما يتفق مع اليقين القانوني، ويبتعد عن الشك والاحتمال، والقاضي يمكن أن يصل إلى يقينية المخرجات المتقدم ذكرها عن طريق المعرفة الحسية التي تدرك الحواس من خلال معرفة هذه المخرجات وفحصها[2]، كذلك أن يكون الدليل الإلكتروني ذا علاقة بموضوع الجريمة الإلكترونية: وهذا الشرط أشار إليه قانون الإثبات الفيدرالي الأمريكي بمبدأ العلاقة الكاشفة إذ يتطلب القانون الأمريكي ضرورة أن يكون هناك علاقة من نوع ما بين الدليل الإلكتروني وبين الواقعة محل الدعوى وشرط ثبوت العلاقة الكاشفة في الدليل إلكتروني يتطلب شرط آخر وهو مطابق الدليل الإلكتروني المستخرج من الكمبيوتر للأصل الموجود بداخلة، وإلاّ يكون هناك إدعاء أو دفع بأن البيانات غير صحيحة بسبب عدم دقة عمل الكمبيوتر، ومناقشة الأدلة الإلكترونية تطبيقا لمبدأ شفوية المرافعة، وهذا الأمر يتطلب فيما إذا كانت مخرجات الوسائل الإلكترونية تعد ادلة إثبات قائمة في أوراق الدعوة التي ينظرها القاضي فإنه يجب عليه مناقشتها أمام الخصوم ويترتب على ذلك أن هذه المخرجات سواء كانت مطبوعة أم بيانات معروضة على شاشة الحاسب، أم كانت بيانات مدرجة في حاملات، تتخذ شكل أشرطة أو أقراص الذاكرة المحمولة في القرص الصلب أو الميموري تكون محل المناقشة عند الإعتماد عليها كأدلة امام المحكمة. كما يجب أن تكون الأدلة المتحصلة من الوسائل الإلكترونية مشروعة: بمعنى تتوافق الأدلة مع مشروعية التوافق والتقيد بأحكام القانون في إطار مضمونها العام، وهذا الأمر يتطلب تقرير ضمانة أساسية وجدية للأفراد لحماية حريتهم وحقوقهم الشخصية، ضد تعسف السلطة بالتطاول عليها في غير الحالات التي يرخص فيها قانون، وذلك من أجل حماية النظام الاجتماعي وبالقدر نفسه تحقيق حماية مماثلة للفرد ذاته. ولذلك فلا بد

(1) - محمد ممدوح بدير، المصدر السابق، ص 182.
(2) - باقر غازي حنون ، المصدر السابق ، ص 187.

لصحة الإجراءات التي يقوم بها عضو الضبط القضائي أن تغلف بمبدأ المشروعية مما يثمر عن الدليل نتائج صحيحه وسليمه[1].

ولقد حسمت الإتفاقية الاوربية موضوع الأدلة الغلكترونية والجرائم المعلوماتية، لعام 2001 بإقرارها صراحة صلاحية المكونات المنطقية والوسائل الغلكترونية لان تكون محلا للضبط وذلك من خلال الفقرة (3) من المادة (19) والتي تنص على انه: (يجب على كل طرف تبني الإجراءات التشريعية التي يراها ضرورية من اجل تخويل هيئاتها التشريعية المختصة سلطة ضبط أو الحصول بطريقة مشابهة على البيانات والادلة الرقمية التي لها علاقة بالجريمة الإلكترونية وفقا للفقرتين، (1 و 2) [2]، فبالرجوع إلى هذه الفقرة نجدها تخول سلطات البحث والتحري طريقتين لضبط المعلومات الرقمية، التي كانت موضوع التفتيش، أو الولوج بطريقة مشابه عملاً بالفقرتين (1 و 2) من المادة (19) ، تتحقق الأولى عن طريق نسخ وتحميل البيانات والمعطيات محل البحث على دعامة تخزين مادية، (كالأقراص الممغنطة، بطاقات الذاكرة، فلاش دسك)، وتكون هذه الأخيرة قابلة للضبط والوضع في احراز مختومة حسب ما هو مقرر في قواعد تحريز وضبط الدليل التقليدية المنصوص عليها في قوانين الإجراءات الجزائية[1]، وهي الطريقة المقصودة في المادة أعلاه بمصطلح الضبط (saisir)، أما الطريقة الثانية فتتضمن تدابير جديدة مستحدثة خصيصا لضبط الادلة الجنائية الالكترونية، وهي المعبر عنها في هذه المادة بمصطلح (الحصول بطريقة مشابه على البيانات الإلكترونية) والتي تكون بإستعمال تقنيات وتدابير الحماية الفنية والتقنية، كتقنيات التشفير والترميز ببرامج منع الكتابة وإستخدام خوارزميات (تجزئة) للملفات المشفرة، من أجل منع الأشخاص المرخص لهم باستخدام المنظومة المعلوماتية، والوصول إلى المعطيات والبيانات الاصلية التي تحتويها هذه المنظومة أو القيام بنسخها، ويكون ذلك في حالة ما اذا إستحال لأسباب تقنية ضبط هذه البيانات الالكترونية وفق الطريقة الاولى[2].

---

(1) - د. امحمد أبو زينة آمنة، إجراءات التحري الخاصة في مجال مكافحة جرائم المعلوماتية، بحث منشور، مجلة جيل لحقوق الإنسان، 2017 ، ضمن اعمال مؤتمرات الملتقى الوطني، اليات مكافحة الجرائم الالكترونية في التشريع الجزائري ، ص 63 .

(2) - ينظر: المادة (19/ 3) من الاتفاقية الاوربية الخاصة بالأدلة الالكترونية والجرائم المعلوماتية، لعام 2001.

(1) - د. هلالي عبدالله، حجية المخرجات الكمبيوترية في المواد الجنائية، دار النهضة العربية، القارة، 1997، ص91.

(2) - يراجع ، ابراهيمي جمال، اليات التحقيق في الجرائم الالكترونية، اطروحة دكتوراه، جامعة مولود معمري – تيزي ووز، كلية الحقوق والعلوم لسياسية، الجزائر، 2018، ص 47 وما بعدها .

ثانيا : مشروعية الدليل الإلكتروني

يقصد بالمشروعية الجنائية، مدى إمكانية إستخدام الوسائل العلمية الحديثة في سبيل الحصول على الأدلة الجنائية[1]، والقول بمشروعية إستخدام هذه الوسائل التقنية ، يعني أن الدليل المثبت منها يكون صحيحاً ويجوز الإستناد إليها عند الحكم[2]. أما القول بعدم المشروعية فهو يعني الإمتناع عن اللجوء إليها أو الإستناد إلى الأدلة المستمدة منها عند الحكم، تأسيسا على القاعدة التي تقضي (ان ما يبنى على الباطل فهو باطل ولا ينتج أثراً). ولذا أن مضمون المشروعية فيما يتعلق بالأدلة الجنائية وإجراءات الحصول عليها في الواقع يُعد مفهوماً ضيقاً للشرعية في هذا المضمار، ويمكن أن نشبه الشرعية هنا، بمثلث ذي ثلاثة أضلع، تدور في فلكه إجراءات جمع الأدلة وإثباتها، إلى أن تصبح صالحة لإنتاج أثارها القانونية، واضلاع هذا المثلث تمثل اسس الشرعية الإجرائية، وأول هذه الأضلاع وأهمها هو أن تدور الادلة الجنائية في فلك القانون، بأن تكون وليدة إجراءات قانونية سليمة. وثاني هذه الأضلاع هو ان تكون هذه الأدلة قائمة على أساس علمية ثابتة ومستقرة[3]. وثالثها أن تكون وليدة إجراءات تتفق مع مبادئ الأخلاق. ويكون الدليل باطلاً إذا ما تحصل عليه عن طريق مخالفة للقانون. ولهذا الموضوع أهمية بالغة لما يترتب عليه بطلان الدليل، وما يترتب عليه من آثار، فإذا كان الدليل الباطل هو الدليل الوحيد فلا يصح الإستناد عليه في إدانة المتهم. وبطلان الدليل يشمل جميع الآثار المترتبة عليه مباشرة، فإذا شاب التفتيش عيباً فهذا ينعكس على الدليل ويبطله، ويشمل أيضا اعتراف المتهم الذي صدر نتيجة له، وهذا ما يتناسب مع مبدأ المشروعية والمبادئ العامة، وإن لم يرد به نص صريح في قانون أصول المحاكمات الجزائية[1].

وهذا يعني أن التفتيش عن الدليل الإلكتروني يجب أن يكون وفق القانون، بمعنى يكون الدليل الإلكتروني باطلاً إذا تم الحصول عليه عن طريق مخالف للقانون، ولقد أخذ هذا الموضوع أهمية بالغة، لما يترتب على إبطال الدليل من آثار إذا كان الدليل الباطل هو الدليل الوحيد، فلا يصح الإستناد عليه في إدانة المتهم. وعلى ضوء ذلك فإن إستخراج الدليل الإلكتروني الجنائي، يتوقف على ثلاثة شروط مهمة، يجب الحصول على الدليل الإلكتروني بصورة مشروعة غير مخالفة لأحكام

---

(1) د.رؤف عبيد ، مبادئ الإجراءات الجنائية في القانون ، دار الفكر العربي ، 1977 ، ص170 .

(2) - د. لورنس سعيد الحوامدة، حجية الأدلة الرقمية في الاثبات الجنائي ، بحث منشور، مجلة البحوث الفقهية والقانونية، العدد السادس والثلاثون ، 2021 ،ص 907.

(3) - د. احمد يوسف الطحاوي، الادلة الالكترونية ودورها في الاثبات الجنائي، دار النهضة العربية، القاهرة، 2015، ص 34 .

(1) - د. محمد فالح حسن، مشروعية استخدام الوسائل العلمية الحديثة في الاثبات الجنائي، الطبعة الأولى، بغداد، 1987 ،ص 35 وما بعدها.

الدستور أو أحكام القانون[1]. وذلك لكون أهم أهداف القانون هو صيانة كرامة الإنسان وحماية حقوقه، إذا تتضمن الدساتير الحديثة نصوصا تنظم القواعد الأساسية في الاستجواب والتوقيف والحبس والتفتيش وغيرها، إذ يتقيد المشرع بها عند وضع قانون الاجراءات الجزائية. فهناك نصوص دستورية تفرض على المشرع الجنائي عند وضع قانون الإجراءات الجنائية الالتزام بها وعدم الخروج عنها[2]، وكذلك فإن إجراءات الحصول على الأدلة الجنائية الإلكترونية يجب أن تكون ضمن الإطار العام الذي حدده الدستور، وإلاّ فإن الدليل المتحصل عليه بطريقة مخالفة للأحكام الواردة في الدستور، يكون باطلاً بطلاناً مطلقاً، لتعلقه بالنظام العام، ويجوز لكل ذي مصلحة التمسك به، كما أن للمحكمة أن تقضي به من تلقاء نفسها وقد إستقرت محكمة النقض المصرية على أن التفتيش عن الادلة، هو من المسائل الموضوعية التي يوكل الأمر فيها إلى سلطة التحقيق تحت اشراف محكمة الموضوع متى كانت المحكمة قد اقتنعت بجدية الإستدلالات التي بنى عليها إذن التفتيش وكفايتها لتسوغ إصداره[3].

وفي إطار مشروعية الأدلة الإلكترونية نجد أنه قانون الإجراءات الجنائية الفرنسي رغم أنه لم يتضمن أي نصوص تتعلق بمبدأ الأمانة أو النزهة في البحث عن الحقيقة لأن الفقه والقضاء كانا بجانب هذا المبدأ، سواء في مجال البحث عن الجرائم تقليدية أم في مجال البحث في جرائم الحاسب الآلي والإنترنت، كان يستخدم أعضاء الضبط القضائي طرقا معلوماتية في أعمال التنصت على المحادثات الهاتفية، ويذهب رأي من الفقه الفرنسي إلى أن القضاء قد قبل إستخدام الوسائل العلمية الحديثة في البحث والتنقيب عن الجرائم تحت تحفظ أن يتم الحصول على الأدلة الجنائية الرقمية ومن بينها الأدلة المتحصلة من الحاسب الآلي والإنترنت بطريقة شرعية ونزيهة. وهذا ما نجده مطبقاً في كل من سويسرا وبلجيكا[1].

ونجد أن قانون الشرطة والإثبات الجنائي الإنجليزي لعام (1984 م) تضمن تحديد الشروط الواجب توفرها في مخرجات الحاسب الآلي لكي يتم قبولها أمام القضاء، وتضمن كذلك توجيهات في كيفية تقدير وتقييم البيانات المستخرجة عن طريق الحاسب الآلي، فأوصت المادة (11) منه: بمراعات كل الظروف عنده تقييم البيانات الصادرة عن الحاسب الآلي المقبولة في الاثبات طبقا للمادة (69) من القانون نفسه، وبوجه خاص مراعاة (المعاصرة) والتطور بمعنى ما إذا كانت المعلومات المتعلقة بأمر قد تم تزويد الحاسب الآلي بها في وقت معاصر لهذا الامر أم لا، كذلك مسألة إذا كان أي

(1) - د. ابو العلا النمر، المصدر السابق، ص 167.
(2) - د. محمود نجيب حسني، الدستور والقانون الجنائي، دار النهضة العربية، القاهرة ، 1992، ص 7.
(3) - د. سحر سعد عبد السميع ، المصدر السابق، ص 293.
(1) - ابراهيمي جمال، المصدر السابق، ص 146.

شخص من المتصلين على أي نحو بإخراج البيانات من الحاسب الآلي لديه دافع لإخفاء الوقائع أو تشويهها، وقد نصت المادة (69) على ثلاثة شروط أساسية لاستخراج الدليل الإلكتروني وهي: " يجب أن لا يوجد اساسا معقول للإعتقاد أن البيان خاطئ أو غير دقيق بسبب الإستعمال الخاطئ أو غير الدقيق. وكذلك أن تكون جميع المكونات المادية للحاسب الآلي كانت تعمل بدقة وعلى نحو متوافق كما ينبغي. بالإضافة أيا من الشروط المحددة التي تدخل في متطلبات القبول المتعلقة بالموضوع يجب أن تخضع لتقدير المحكمة والقضاء"[1]، ونجد أنه قد قضت محكمة الاستئناف الجنائي في إنجلترا بذلك إذ بينت في حكمها كيفية التعامل مع الأدلة المستخرجة من الحاسب الآلي ويتلخص الحكم فيما يأتي: (يبدو إلى هذه المحكمة أنه من الخطأ رفض أو إنكار أي مزايا أو صلاحيات مقررة وفقا لقانون الإثبات يمكن بمقتضاها التوصل عن طريق التقنيات الجديدة والوسائل الحديثة التأكد من صحة وصدق التسجيل الإلكتروني، إذ يمكن التثبت من ذلك وكذلك يمكن التعرف بوضوح على الاصوات المسجلة، والمستخلص أيضا هو ان الدليل وثيق الصلة بالموضوع من جهة أخرى ويمكن قبوله ومن ثم تؤيد المحكمة قبول هذه الاشرطة والتسجيلات، ويجب أن ينظر لها بعين الإعتبار إلى مثل هذه الأدلة، وتقدير قيمته في ضوء جميع الظروف بالنسبة لكل قضية)[2]. وهناك من يقول إن الدليل الإلكتروني لا يمكن الركون إليه إلاّ على سبيل الإستدلال ولا يمكن الجزم على الأدلة الإلكترونية، وذلك لما تشكله هذه الأدلة من طبيعة تتميز بمتغيرات سريعة يمكن التحكم بها[1].

اما موقف المشرع الأمريكي فقد اختلف في مسألة إستخدام أجهزة المراقبة والتنصت التلفوني في الإجراءات الجنائية كوسائل علمية حديثة للكشف عن الجريمة، فبعضهم يراها إجراءات مشروعة لا تدخل تحت حماية الدستور، وهناك إتجاه آخر عدها إجراءات غير مشروعة، وقد برز رأيان في قضاء المحكمة الفدرالية العليا على مرحلتين المرحلة السابقة على صدور قانون الاتصالات الفيدرالي لعام (1934) والمرحلة اللاحقة لصدور القانون الاخير، ففي المرحلة الأولى ما قبل صدور قانون الاتصالات الفيدرالي لعام (1934) واجهت هذه المرحلة رفض المحكمة الفيدرالية كفالة الحماية الدستورية بموجب التعديل الدستوري الرابع للمحادثات التليفونية وما ينتج عنها من أدلة إثبات تفيد في الكشف عن الحقيقة، وذهب إلى تقرير مشروعية مراقبة المحادثات التليفونية بواسطة السلطات

(1) - نقلا عن : د. سحر سعد عبدالسميع، المصدر السابق ، ص 297.
(2) - د. اشرف عبدالقادر قنديل، الاثبات الجنائي في الجريمة الالكترونية، دار الجامعة الجديد، الاسكندرية، 2015، ص 29.
(1) - د. مخلص محمود حسين ، المصدر السابق، ص 198.

العامة[1]، بمعنى أن المشرع الأمريكي قد أعطى أهمية كبيرة للأدلة الإلكترونية المستخلصة من مراقبة المحادثات التليفونية بواسطة السلطات العامة، وقد إستندت المحكمة العليا في قبول هذا الدليل على أساس أن الحماية الدستورية لم تتناول الحق العام في السرية، وإنما شملت أيضا حق الحماية المقررة للأشخاص والمنازل والأوراق من القبض والتفتيش دون سبب معقول، وأن المكالمات التلفونية بوصفها شيئا غير مادي لا تندرج تحت هذه الحماية.

أما المرحلة الثانية: وهي المرحلة ما بعد صدور قانون الاتصالات الفيدرالي لعام (1934) كان صدور قانون الإتصالات الفيدرالي والذي نص في المادة (605) على حظر إلتقاط المحادثات الهاتفية أو إفشائها على المستوى الإتحادي ومستوى الولايات أثره الفعال في تطوير قضاء المحكمة العليا واتخاذها موقفاً مخالفاً لقضائها السابق، إذ تواترت أحكام المحكمة الفيدرالية على القضاء بعدم مشروعية مراقبة المحادثات التلفونية حتى لو كان القانون الداخلي للولاية قد يجيزها[2]. وهناك من وصف هذا الأمر بانه يُعد تعدياً على الخصوصية والحق العام بمعنى أن الدليل المستخلص من مراقبة هذه المحادثات والإتصالات الهاتفية يُعد غير مشروع، ولا يمكن الأخذ بهذا الدليل وفي حكم اخر للمحكمة الفيدرالية العليا، ذهبت إلى عدم مشروعية قوانين الولايات التي أجازت مراقبة المحادثات التليفونية بعد الحصول على إذن قضائي لآنها لم تضع الضوابط القانونية التي تكفل عدم انتهاك الحقوق والحريات الفردية. جاء في حيثيات الحكم ان الكونجرس قد قرر بصورة واضحة حظر التنصت على المحادثات التليفونية بموجب نص المادة (605) من قانون الإتصالات الفيدرالي لعام (1934) فهو لا يسمح للمشرع في الولايات إصدار تشريعات تتعارض مع قانون الإتصالات الفيدرالي[1].

أما (المشرع الفرنسي) فقد عالج موضوع مدى مشروعية مراقبة المحادثات الهاتفية ومدى مقبولية الدليل المستخلص منها، في قانون الإجراءات الجنائية الفرنسية لأول مرة بمقتضى القانون رقم (643) في عام 1970 بموجب المادتين (80 و 81) والتي أقرت مشروعية الدليل المتحصل من مراقبة المحادثات الهاتفية وفقا لشروط معينة، إلا أن مخالفة هاتين المادتين لنص المادة (الثامنة) من الاتفاقية الأوروبية لحقوق الإنسان، دعا المشرع الفرنسي إلى إصدار القانون رقم (646 – 91)

(1) - د. محمد امين الخرشة، مشروعية الصوت والصورة في الاثبات الجنائي، دار الثقافة للنشر، عمان، 2011، ص60.

(2) - د. حازم حسن الجمل، الحماية الجنائية للأمن الإلكتروني ، الطبعة الاولى، دار الفكر والقانون، 2015، ص70 .

(1) - مبروك ساسي، مشروعية الصوت والصورة في الاثبات الجنائي، اطروحة دكتوراه، جامعة الحاج لخضر باتنة 1 ، كلية .الحقوق والعلوم السياسية، 2017 ، ص 119 .

لعام 1991 ، لتنظيم مشروعية مراقبة المحادثات الهاتفية في جميع وسائل الإتصال الحديثة في صورها المختلفة، وذلك كأثر على حكم المحكمة الأوروبية لحقوق الإنسان والذي صدر عام 1990 وينص هذا القانون على أن الجهة المختصة بإصدار أمر المراقبة هو قاضي التحقيق الذي يندب أحد أعضاء الضبط القضائي مباشرة هذا الإجراء، ولا يجوز لأعضاء الضبط القضائي مراقبة المحادثات الهاتفية بدون وجود إذن من قاضي التحقيق حتى ولو كان ذلك في حالة التلبس بالجريمة كما حددت المحكمة العليا الفرنسية حدود قاضي التحقيق في الجرائم التي تخضع لإمكانية إجراء مراقبة للمحادثات الهاتفية[1]، وأصدرت حكماً بأن قرار إجراء التنصت لا يجوز إلاّ في الجنايات والجنح الخطيرة التي تمثل اعتداء على النظام العام، وقاضي التحقيق هو من يقدر تلك الخطورة بالنظر إلى ظروف القضية التي يذكرها في قراره، كما نص المشرع الفرنسي في القانون ذاته بموجب المادة (100 / 1)، على القاضي أن يأمر بالتنصت في مواد الجنايات ومواد الجنح التي تكون عقوبتها السجن سنتين فأكثر. وجاء بنص المادة 100 /2 من قانون الإجراءات الجنائية الفرنسي على أن مدة المراقب الهاتفية تكون أربعة أشهر كحد أقصى قابلة للتجديد بالشروط نفسها الواردة في قرار المراقبة الأول، مما يعني أن المراقبة تكون مستمرة طالما كان التحقيق يستلزم ذلك كما أن نص القانون ذاته على ضمانات للمتهم عند تعرضه للمراقبة محادثات الهاتفية وفق المادة (100 / 3 و 5/100) منها[1].

وتأسيساً على ما تقدم ولكي يكون الدليل الإلكتروني المستمد من البيانات محلا مقبولاً لإثبات الجرائم الإلكترونية يلزم توافر شروط معينة: يجب أن يكون قد توافرت شروط وضوابط المشروعية وصحته[2]. وكذلك يجب أن تكون الادلة الإلكترونية غير قابل للشك : بمعنى يشترط في الادلة المستخرجة من الحاسب الآلي وشبكة الإنترنت أن تكون غير قابل للشك حتى يمكن الحكم بالإدانة أو البراءة، ذلك أنه لا مجال لفحص قرينه البراءة و افتراض عكسها الاّ عندما يصل اقتناع القاضي إلى حد الجزم واليقين، ويمكن التوصل إلى ذلك من خلال ما يعرض من الأدلة الإلكترونية والمصغرات التصويرية وغيرها من الاشكال الإلكترونية التي تتوافر سواء عن طريق الوصول المباشر، أو كانت مجرد عرض لهذه المخرجات المعالجة بواسطة الحاسب الآلي على الشاشة الخاصة به، وهكذا يستطيع القاضي من خلال ما يعرض عليه من مخرجات إلكترونية وما ينطبع فيه من تصورات وأحتمالات بالنسبة لها، أن يحدد قوتها الإستدلالية على التأكد من نسبة أي من جرائم الاعتداء حصل

(1) - د. محمد امين الخرشة، مشروعية الصوت والصورة في الاثبات الجنائي، المصدر السابق،ص 85 و 86.
(1) - د. ابراهيم عبد نايل، الحماية الجنائية لحرمة الحياة الخاصة في قانون العقوبات الفرنسي، دار النهضة العربية، 2000، ص 123 .
(2) - د. خالد ممدوح إبراهيم الجرائم المعلوماتية المصدر السابق ، ص187.

على منظومة التوقيع الإلكتروني أو غيرها من الاعتداء أو التهديد على شخص معين من عدمه[1]. وأيضا إمكانية مناقشة الأدلة الإلكترونية المستخرجة من الحاسب الآلي والإنترنت: وهذا يعني مبدأ وجوب مناقشة الدليل الجنائي بصفة عامة أن القاضي لا يمكن أن يؤسس قناعته الخاصة، إلاّ على العناصر الاثباتية التي طرحت في جلسات المحاكمة و خضعت لحرية مناقشة أطراف الدعوى، وهذا يعني أن الأدلة المتحصلة من جرائم الحاسب الآلي والإنترنت سواء كانت مطبوعة بيانات معروضة على شاشة الحاسب الآلي أم كانت بيانات مدرجة في حاملات بيانات، أم اتخذت شكل أشرطة أو أقراص صلبة أو مصغرات فيلمية، كل هذه ستكون محل للمناقشة عند الأخذ بها كأدلة إثبات أمام المحكمة، وعلى ضوء ذلك، فإن كل دليل يتم الحصول عليه من خلال بيئة تكنولوجيا المعلومات يجب أن يعرض في الجلسة ليس من خلال ملف الدعوى في التحقيق الابتدائي، لكن بصفة مباشرة أمام القاضي. وهذه الأحكام تنطبق على كافة الأدلة المتحصلة من الحاسبات الآلية والتقنية[2].

ثالثا : حجية الدليل الإلكتروني

يُعدّ الإثبات الجنائي من المبادئ القانونية التي لا تقبل من الطرق والوسائل، إلاّ تلك التي حددها القانون[1]، وإعتبار بعضاً منها يتمتع بالقوة الثبوتية الكاملة، لإثبات جميع التصرفات القانونية والوقائع المادية، إلاّ أن دخول تكنولوجيا المعلومات إلى عالمنا ، وقيام ثورة علمية في مجال نقل المعلومات وتبادلها عبر الإنترنت، أدى إلى ظهور تحديات جديدة لم يستطيع القضاء تجاوزها بالحلول التقليدية التي رسمها المشرع. وعلى الرغم من ما يتميز به الدليل الإلكتروني إلاّ أن هناك تحديات حقيقية تواجه وتضعف من أهميته كتعارض قواعد الإثبات الإلكتروني مع بعض أدلة الإثبات التقليدية، أو تعارض قواعده مع المبادئ الأساسية التي ترتكز عليها مبادئ الاثبات التقليدية، ومن ذلك قاعدة عدم جواز اصطناع الخصم دليلا لنفسه، ولا يقتصر الأمر عند هذا الحد بل هناك تحديات ذات جوانب فنية لا قانونية تتعلق بمدى توافر الأمن القانوني وإلى أي حد يمكن للأفراد وضع ثقتهم في التعامل الإلكتروني وذلك بسبب تعرض أدله الإثبات الالكتروني إلى مخاطر متعددة[2].

---

(1) - ممدوح حسن مانع العدوان، نادر عبدالحليم السلامات، مشروعية وحجية الدليل المستخلص من التفتيش الالكتروني في التشريع الجزائي الاردني، بحث منشور، مجلة علوم الشريعة والقانون، المجلد 45، العدد 4، ملحق 2، 2018، ص 63.

(2) - نوفل علي عبدالله، وخالد عوني خطاب، المصدر السابق ، ص 409.

(1) - عبد المنعم محمد إبراهيم رضوان موضع الضرر في البنيان القانوني للجريمة، اطروحة دكتورة، جامعة القاهرة، كلية القانون، 1993، ص 42 .

(2) - د. حسن فضالة موسى ، المصدر السابق ، ص 160 .

وفي هذا الصدد فقد أختلفت الأنظمة في مدى الإثبات الجنائي وتقدير حجية هذه الأدلة المستخلصة من الوسائل الإلكترونية عامة ومن التفتيش خاصة[1]، وهذه الأمر يقودنا إلى تساؤل مهم، وهو ما مدى مشروعية الأخذ بالدليل الرقمي المستخلص من التفتيش الإلكتروني؟ وهل للدليل المستخلص من الوسائل الإلكترونية من خلال التفتيش يتمتع بقوة الحجية؟ وللإجابة عن هذه التساؤلات هناك ثلاثة أنظمة لكل منها موقفاً من قبول الأدلة الإلكترونية وهي: (نظام الادلة القانونية أو النظام المقيد): ووفقا لهذا النظام فالمشرع هو من يحدد الأدلة بشكل عام وبشكل حصري، والتي يجوز للقاضي اللجوء إليها في الإثبات وهو يحدد القيمة القانونية لكل دليل، ويكون دور القاضي محدداً بفحص الأدلة للتأكد من توافر الشروط التي حددها القانون، فلا سبيل للإستناد إلى أي دليل لم ينص القانون عليه صراحة ضمن أدله الإثبات، كما أنه لا دور للقاضي في تقدير القيمة القانونية للدليل، ولذا يسمى هذا النظام بنظام الإثبات القانوني أو المقيد. أما (نظام الاثبات الحر): إذ يتمتع القاضي الجنائي في ظل هذا النظام بحرية مطلقة في شأن إثبات الوقائع المعروضة عليه، فلا يلزمه القانون بالأدلة للإسناد إليها في تكوين قناعته، فله أن يبني هذه القناعة على أي دليل وأن لم يكون منصوص عليه[2]، بل أن المشرع في مثل هذا النظام لا يلتزم بالنص على أدلة الإثبات، فكل الأدلة تتساوى قيمتها الإثباتية في نظر المشرع، والقاضي هو الذي يختار من بين ما يطرح عليه ما يراه صالحا للوصول إلى الحقيقة، وهو في ذلك يتمتع بمطلق الحرية لقبول الدليل أو رفضه إذا لم يطمئن إليه، فالمشرع لا يتدخل في تحديد القيمة القانونية للدليل وعلى الرغم من توافر شروط الصحة في الدليل إلاّ أن القاضي يملك أن يرد تحت مبرر عدم الاقتناع، وللقاضي دورٌ في تحديد سلامة المنهجية المتبعة والطرق الفنية المتخذة في تحديد الدليل الإلكتروني. والنظام الثالث هو (نظام الإثبات المختلط): ويعتمد هذا الإتجاه أو النظام على أن يحدد القانون أدلة معينة لإثبات بعض الوقائع أو يشترط في الدليل شروطاً في بعض الأحوال، أو يعطي القاضي الحرية في تقدير الأدلة، ونجد مثلاً المشرع الياباني، حصر أدلة الإثبات بأقوال المتهم وأقوال الشهود والقرائن والخبرة، وأشترط للإثبات بواسط مستخرجات ومتحصلات الوسائل الإلكترونية أن يتم تحويلها إلى صور يمكن قراءتها أو مرئية يمكن طباعتها[1].

ونجد أن (المشروع الأمريكي) قد حسم أمر حجية الدليل الإلكتروني من خلال النص عليه صراحة في القانون الخاص للولايات المتحدة الأمريكية، إذ نص قانون الحاسب الآلي لسنة (1984) الصادر في ولاية (Iowa) على أن مخرجات الحاسب الآلي تكون مقبولة بوصفها ادلة إثبات بالنسبة لبرامج وبيانات الحاسب الآلي المخزنة بداخلة، ونص أيضا قانون الإثبات الصادر عام (1983)

(1) - د. احمد فتحي سرور، الوسيط في قانون الاجراءات الجنائية، دار النهضة العربية، القاهرة، 2016، ص587.
(2) - ابراهيمي جمال، المصدر السابق، ص 151 .
(1) - ممدوح حسن مانع ، المصدر السابق، ص 65.

في ولاية كاليفورنيا على النسخ المستخرجة من البيانات التي يحتويها الحاسب الآلي تكون مقبولة بوصفها أفضل الأدلة المتاحة في مجال الإثبات. وهذا ما أكده القضاء الأمريكي في أحكام مختلفة تخص الأدلة الإلكترونية المتحصلة من أجهزة الحاسب الآلي يجب أن تكون مقبولة كأدلة إثبات مادام الكمبيوتر تولد عنه معلومات بصورة سليمة وكان القائم عليه تتوافر فيه الثقة والطمأنينة[1].

أما (المشرع العراقي) فقد تناول موضوع الإثبات ومدى قناعة المحكمة عند تقديم الادلة أثناء نظر الدعوى، إذ جاء بنص المادة (213) من قانون أصول المحاكمات الجزائية رقم (23) لسنة 1971 المعدل، على أنه : (أ- تحكم المحكمة في الدعوى بناء على اقتناعها الذي تكون لديها من الادلة المقدمة في أي دور من أدوار التحقيق أو المحاكمة، وهي الإقرار، وشهادة الشهود ومحاضر التحقيق والمحاضر والكشوف الرسمية الاخرى وتقارير الخبراء والفنيين والقرائن والأدلة الاخرى المقررة قانونا. .....)[2]. وعلى ضوء نص هذه المادة يمكننا القول إن المشرع العراقي قد فعل حسنا عندما وسع من مفهوم دليل الإثبات، وقد اعطى سلطة تقديرية للمحكمة لبناء قناعتها عند دراسة الدليل المقدم اليها، ومن الممكن الأخذ بالدليل الإلكتروني، في حال تم تقديمة من قبل خبراء فنيين مختصين بهذا الشأن، وللمحكمة السلطة التقديرية للأخذ بالدليل الإلكتروني أو التقرير الفني المقدم من قبل الخبراء، في حال اقتناعها به.

ونجد أن المشرع العراقي قد أحاط بموضوع الأخذ بأدلة الإثبات مهما كان نوعها ومصدرها، إذ جاء بقانون الإثبات العراقي رقم (107) لسنة 1979 والمعدل بالقانون رقم 46 لسنة 2000، ضمن الباب الثاني ، الفصل الاول، الفرع الثالث منه (السندات العادية)، وجاء بنص المادة (27/ ثانيا) على أنه: " يكون للبرقيات حجية السندات العادية أيضاً إذا كان أصلها مودعا في مكتب الاصدار موقعا عليه من مرسلها....."[1].

وتأسيساً على ذلك فان مفهوم البرقية يدخل ضمن مفهوم التكنولوجيا الحديثة والتقدم العلمي، وهي عبارة عن رسالة ترسل بواسطة جهاز لا سلكي ، وقد عدها المشرع العراقي كدليل اثبات وأعطاها قوة السندات العادية[2]، وأيضاً نجد أن المشرع العراقي قد اكد على حجية هذه الادلة من خلال نص المادة (104) من القانون نفسه، والتي تنص على انه: " للقاضي ان يستفيد من وسائل التقدم العلمي

(1) - باقر غازي حنون ، المصدر السابق، ص .199
(2) - ينظر: المادة (213) من قانون اصول المحاكمات الجزائية العراقي رقم 23 لسنة 1971 .
(1) - المادة (27) من قانون الاثبات العراقي رقم (107) لسنة 1979 المعدل .
(2) - د. أدم وهيب النداوي، الموجز في قانون الاثبات ، مكتبة مدينة العلم، دون سنة نشر، ص 94. وكذلك:ينظر : د. حسن فضالة موسى، التنظيم القانوني للإثبات الالكتروني، المصدر السابق، ص 149 .

في إستنباط القرائن القضائية". ومفهوم هذا النص القانوني، يؤكد بإعطاء السلطة التقديرية للمحكمة والقاضي الإخذ بالأدلة الإلكترونية، في حال توصلت المحكمة لقناعة وإستنباط القرائن القضائية.

المبحث الثاني

أثر التطور التكنولوجي على الإثبات الجنائي

بعد أن كانت وسائل الإثبات الجنائي التقليدية هي من يفرضها المشرع لإثبات أي فعل مجرم، إلاّ أن التطور التكنولوجي والتقني الحديث، قد أظهر لنا مجموعة كبيرة من أدلة الإثبات غير التقليدية، كالبيانات الرقمية الإلكترونية، والصور ومقاطع الفيديو والأرقام، وغيرها العديد من الادلة الرقمية والتي تدخل ضمن نطاق التكنولوجيا الحديثة المتمثلة بإستعمال أجهزة الإتصالات والبرامج والتطبيقات الإلكترونية في الوقت الحالي، وهذا ما أدى إلى توجه بعض الدول إلى مواكبة هذا التطور التكنولوجي وتغيير في سياستها الجنائية لمكافحة الجريمة الإلكترونية، والإعتماد على الأدلة الإلكترونية في الإثبات الجنائي، من خلال إجراء المعاينة والتفتيش على مكان وموقع الجريمة وتفتيش الأجهزة التقنية الحديثة التي تحتوي على مجموعة من البيانات، التي تفيد في الكشف عن الجريمة والمتهم، لذا فقد إرتأينا أن نقسم دراستنا لموضوع مظاهر تأثير التطور التكنولوجي على الإثبات الجنائي من خلال تقسيم هذا المبحث لمطلبين، نتناول في المطلب الاول دراسة أثر التطور التكنولوجي في المعاينة الإلكترونية، ونخصص المطلب الثاني لدراسة أثر التطور التكنولوجي على تفتيش الجريمة الإلكترونية.

المطلب الأول

أثر التطور التكنولوجي في المعاينة الإلكترونية

يحتاج التحقيق في جرائم الإنترنت إلى مشاهدة وفحص الأدلة الجنائية، وهي غالبا ما تتميز بالسهولة في الإستخدام والبعد عن التعقيد لأن الكثير من مستخدمي الحاسوب يستخدمونها كبرامج عرض الصور وبرامج فك الملفات المضغوطة، ولذلك ينبغي على أعضاء الضبط القضائي والمحققين والقضاة، عند إجراء المعاينة أن يكونوا على وعي جيد بجرائم الحاسوب والإنترنت، حتى يتمكنوا من مواجهة هذه الجرائم. وعلى المحقق اتباع أساليب حديثة ومتغيرة، إذ يعالج كل أسلوب منها في إحدى الحالات المعينة أو يلجأ إلى إستعمال عدة إساليب في حالات أخرى، ولذلك فإنه يحتاج للوسائل المادية والمعنوية ليستخدمها في تنفيذ التحقيق والمعاينة لأن التحقيق في جرائم الإنترنت يحتاج إلى معرفة تامة وإدراك بالوسائل التي تثبت وقوع الجريمة والوصول إلى الجاني ونسبتها إليه.

الفرع الأول

المعاينة في الجرائم الإلكترونية

يحتاج إثبات الجرائم الإلكترونية إلى دليل إلكتروني رقمي، كوسيلة لأثبات الواقعة الجرمية، كالإختراق والتعدي على البيانات والمعلومات والأنظمة التقنية، وهذا الامر يحتاج إلى إستخدام طرق علمية وعملية حديثة لإستحصال تلك الأدلة والتي لها إرتباط مباشر بوقوع الجريمة الالكترونية، وهذا الامر يتطلب إستخدام طرق غير تقليدية لإثبات الدليل الرقمي، مما يستدعي الإستعانة بأشخاص ذوي صفة وخبرة فنية في المجال التقني، يمتلكون المهارة الفنية والتقنية اللازمة لإستخلاص الأدلة والحفاظ عليها من التعرض للتلف، أو المحو، لان الفصل في الدعوى الجزائية في هذه الحالة يتوقف على الرأي الفني الذي يبرّئ أو يدين المتهم. فالدليل العلمي الإلكتروني هو النتيجة التي تسفر عن إجراء المعاينة والتفتيش اثناء البحث في كل ما له علاقة بالجريمة التي إرتكبت[1].

أولا : المعاينة لغة : عاينت الشيء: أي نظرت إليه رأيته عياناً، على وزن فاعل مفاعلة وفعالاً[1]، إذ قال الأزهري: رأيت فلاناً عياناً، أي مواجهة، ويقال: عينت فلاناً، أي أخبرته بمساويه في وجهه، ولقيته عيانا: معاينة بعينك، لم يشك في رؤيته إياه[2]. وقال أبن فارس : ورأيت الشيء عياناً، أي معاينه، ويقولون: لقيته عين عنه، أي عياناً. وصنعت ذلك عمد عين، إذا تعمدته والأصل في العين النظرة، أي أنه صنع ذلك بعين كل من راه[3].

ثانيا : المعاينة اصطلاحاً : عرفت المعاينة من جانب الفقه بتعريفات عدة منها من يقول بأنها: رؤية بالعين لمكان أو شخص أو شيء لإثبات حالة، وضبط كل ما يلزم كشف الحقيقة[4]. وأيضاً عرفت بأنها: إثبات الحالة التي يكون عليها مسرح الجريمة بعد انتقال المحقق إليه، واثبات ما به من آثار وحالة الأشخاص المتواجدين به، والتحفظ على كل ما من شأنه أن يغير في كشف الحقيقة[5]. وأيضاً يقصد بالمعاينة بأنها الإجراء الذي يتضمن وصف مكان الحادث بما فيه من أشياء وأشخاص ، والفحص الدقيق لكافة المحتويات بهدف كشف مخلفات وأثار الجاني بالمكان والتي تشير إلى

---

(1) - د. حجازي عبد الفتاح بيومي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، 2005 ،ص 49.

(1) - انظر: لسان العرب، ابن منظور، ج4، ص 3196، وايضا. تاج العروس، الزبيدي، ج35، ص 452.

(2) - ينظر : تهذيب اللغة الازهري، ج3، ص 131.

(3) - معجم مقاييس اللغة، زكريا ، ج4 ، ص 199.

(4) - د. محمد ممدوح بدير ، مكافحة الجريمة المعلوماتية عبر شبكات الانترنت، الطبعة الاولى، مركز الدراسات العربية، 2019 ، ص 120 .

(5) - د فضيلة عاقلي ، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري ورقة عمل مقدمة، ضمن أعمال المؤتمر الدولي الرابع عشر بعنوان (مكافحة الجرائم إلإلكترونية)، طرابلس 2017 ، ص126.

شخصيته أو شركائه[1]. ويرى جانب من الفقه بأنها: مشاهدة وإثبات الحالة في مكان الجريمة، ومشاهدة وإثبات الآثار المادية التي خلفها ارتكاب الجريمة[2]. و عرفها آخرون بأنها الفحص الدقيق للآثار المادية للجريمة، والأدلة الموجودة في مكان وقوع الجريمة وتجميع الأشياء والادوات وتسجيل كافة المعلومات والقرائن بدون تأخير خوفاً من اندثار الاثار أو محوها بواسطة الجاني أو الطبيعة[3] .

ومن خلال ما تقدم نتوصل إلى أن المقصود بالمعاينة هو: انتقال أعضاء الضبط القضائي إلى مكان ما، للقيام بما يحفظ كل ما من شأنه يفيد في كشف الجريمة، وإثبات الحالة التي يوجد فيها الأشخاص أو الأشياء في ذلك المكان من أجل كشف الحقيقة في الجريمة محل إجراء المعاينة. فعملية المعاينة والتحقيق تتمثل بالنهج الذي من خلاله يتم دراسة الجرائم وفهمها، يسعى من خلالها المحققين لفهم الطريقة التي إرتكب من خلالها الجريمة والدوافع، وهوية الشخص الذي ارتكب الجريمة، والدلائل التي تركها المجرم في مسرح الجريمة، أو أي أدلة أخرى. وما قد يسهل بعض عمليات التحقيق أن المجرمين المحترفين يميلون لإتباع نهج محدد حينما يرتبكون الجرائم، بل ويتركون ذات الأثار غالباً[1].

الفرع الثاني

صعوبات إجراءات المعاينة الإلكترونية وتحصيل الدليل

عند التحقيق في الجرائم الإلكترونية، فإن إستخلاص الدليل الإلكتروني، يتطلب توافر مجموعة من الشروط والضوابط، من أجل رصانة هذا الدليل لأنه سيكون دليل براءة أو إدانة للمتهم، وعلى ضوء ذلك فإن الحصول على الأدلة الإلكترونية الجنائية يجب إظهاره من قبل أشخاص لهم الخبرة والدراية الفنية والتقنية في هذا المجال والتخصص في معاينة وتفتيش أجهزة الحاسب الآلي، وكيفية الولوج إلى البيانات المخزنة بصورة معقدة وخطرة، من أجل عدم اندثار أو تلف أو محو هذه الأدلة الإلكترونية[2].

---

(1) - إبراهيمي جمال، التحقيق الجنائي في الجرائم إلكترونية، اطروحة الدكتوراه، جامعة مولود معمري، تيزي وزو، كلية الحقوق والعلوم السياسية، 2018 ، ص 56.

(2) - د. محمود صالح العادلي، البحث والتحقيق الجنائي في الإرهاب الإلكتروني، بحث منشور، مجلة دراسات تربوية، العدد 6، 2021، ص 1223

(3) - فيروز عوض الكريم صالح، إجراءات التحري والضبط في الجريمة الالكترونية، أطروحة دكتوراه، جامعة شاندي، كلية القانون، 2017 ، ص 99.

(1) - سامي حارب المنذري، موسوعة العلوم الجنائية، تقنية الحصول على الاثار والادلة المادية، الجزء الاول، مركز بحوث الشارقة، 2007، ص 113.

(2) - مأمون محمد سلامة، الاجراءات الجنائية في التشريع المصري، دار النهضة العربية، القاهرة، 2001 ،ص645.

ولكي يكون إستخلاص الأدلة الإلكترونية وفق آلية وشروط معينة، فهذا الامر يتطلب للقيام به من قبل أشخاص يتمتعون بخبرات فنية وعلمية في هذا المجال، فالخبرة هي إجراء يتعلق بموضوع يتطلب الإلمام بمعلومات فنية من أجل إستخلاص الدليل الرقمي منه، أو هي الإستشارة الفنية التي يستعين بها المحقق أو القاضي في مجال الإثبات، لمساعدته في تقدير المسائل الفنية التي يحتاج تقديرها إلى مساعدة فنية أو إدارية لا تتوافر لدى أعضاء السلطة القضائية المختصة بحكم عمله وثقافته. والخبرة كدليل في الإثبات تنصرف إلى رأي الخبير الذي يثبته في تقريره وبما أن تقرير الخبير يُعد من الادلة الفنية فإن إجراء الخبير هو من إجراءات جمع الأدلة، وعلى ضوء ذلك فللمحقق الإستعانة بالخبراء ليستطلع رأيهم في بعض الامور الفنية والتقنية التي تعرض له أثناء تأدية مهمته في التحقيق الذي ينتهي بإصدار قرار بأن لا وجه لإقامة الدعوى أو بإحالتها إلى محكمة الموضوع. وأما الخبرة في مرحلة المحاكمة فإنها تساعد القاضي في تكوين عقيدته للفصل في الدعوى[1].

فشرط الخبرة والتخصص في إجراء المعاينة والتفتيش لها أهمية كبيرة، وهذه الأهمية تلعب دوراً كبيراً، من خلال الخبرة الفنية والتقنية في عملية الحصول وإستخلاص أدلة إثبات الجريمة الإلكترونية، إذ تعد عملية الحصول على الأدلة الرقمية صعب الوصول إليها لما تتطلبه من خبرة ومهارة كبيرة في مجال الحاسب الآلي[2]، ويرجع ذلك إلى تعدد صور وأشكال الجرائم الإلكترونية، ما بين مهاجمة المعلومات بغرض تدميرها أو السيطرة عليها أو قد يكون المقصود به وهو الأجهزة كنشر فيروس يعمل على إتلاف وحداته الرئيسية مثلا. أو قد يكون الأمر مجرد اختراق لكلمة مرور خاصة لأحد البنوك أو لمؤسسة كبرى بغرض الاحتيال أو الحصول على الاموال، وقد تكون مجرد إثبات الذات، وإظهار المقدرة العالية في مجال الحاسب الآلي، ولما كانت عملية تجميع الادلة الرقمية الجنائية، في الجرائم الإلكترونية تعد من أهم وأصعب الأمور التي تواجه عملية الإثبات الجنائي، لذا كان لزاما أن يتم اللجوء إلى خبير في المجال الفني والتقني مختص في الشؤون المعلوماتية التقنية للحصول على الدليل العلمي الفني الجنائي[3].

وتجدر بالإشارة أن التطور التقني لم يؤثر على عملية المعاينة فحسب، بل أثر بشكل عام على العدالة الجنائية وسهل عمل الشرطة في كل مجال، فبات بإمكان الشرطة الوصول لمحل الحادث بسرعة

(1) - د. ممدوح محمد ممدوح ، المصدر السابق ، ص 127.

(2) - د. علي هاشم ، المصدر السابق، ص 135.

(3) - عبدالناصر محمد فرغلي، المسماري محمد عبيد، الاثبات الجنائي بالادلة الرقمية من الناحية القانونية والفنية ضمن وقائع المؤتمر العربي الالو لعلوم الادلة الجنائية والطب الشرعي، المقام في جامعة نايف العربية للعلوم الامنية، 2007، ص 34.

أكبر، وبات بإمكانهم التواصل مع بعضهم أثناء العمل بشكل سريع، وإن لهذا التطور التقني دوراً مهماً وفعالاً في تسهيل عملية جمع المعلومات من قبل الشرطة[1].

وإن للتطور التقني دوراً مهماً في المعاينة بشكل عام، إذ تساعد المحققين في الوصول للأدلة، الإلكترونية منها وغير الإلكترونية مثل الحمض النووي، ومن المتوقع التكنولوجية المستقبلية سيكون لها أثر واسع على العدالة الجنائية، بل ولها تأثير واسع في الطب الشرعي، وذلك من خلال تسهيل مهمته في فحص الأدلة وتقييمها. ويمكن أن يقسم دور التقنيات في المعاينة إلى قسمين وهما:

1- دورها في مساعدة القضاة والمحققين، أو الشرطة في إيجاد الأدلة والبحث عن مرتكبي الجرائم، فقد يبين استخدام المجرم للبطاقات الائتمان موقعه.

2- إستخدام التقنيات لمحو الأدلة أو إخفاء آثار الجرائم التي يرتكبها الأشخاص وخاصة في الجرائم الإلكترونية، إذ قد يستخدمها الأشخاص في إخفاء الأدلة أو مسحها أو الحصول على نسخ ثانية، وسندرسها في نطاق أنواع معينة من الأجهزة.

وفي ظل الدور المهم الذي لعبة التطور التكنولوجي، إلاّ أن هناك صعوبات قد تواجه جهات التحقيق، تؤثر سلبا في ضياع أو اتلاف أو محو الدليل وملامح الجريمة، من خلال بيان تأثير هذه التقنيات على عملية المعاينة والتحقيق.

وإن إستخدام التقنيات الحديثة في المعاينة يعني تسهيل عملية خزن البيانات وإستعادتها وتحليلها، ويقصد بتلك البيانات تلك التي تحصلها الشرطة أثناء معاينتها لموقع الجريمة من بصمات أصابع أو أسلحة وغيرها، وكذلك للتقنيات دوراً مهماً في عملية تخزين وتحليل الأدلة الإلكترونية التي تحصلها الشرطة أثناء عملية المعاينة في الجرائم الإلكترونية[1].

وتكمن المشكلة هنا أن هذه التقنيات وان سهلت عملية المعاينة بشكل عام إلا أنها في واقع الحال تنطوي على مشاكل وعوائق عديدة ومن بينها ما يأتي:

1- إن هذه التقنيات تكلف مبالغ طائلة.

---

(1) - حفصي عباس، المصدر السابق، ص 44.

(1)- Hakan Hekim, INFORMATION TECHNOLOGY AND CRIMINAL INVESTIGATIONS: DOES IT MATTER?, The University of North Carolina, 2009, page 12.

2- تتطلب هذه التقنيات وجود أفراد شرطة يعلمون كيف إستخدامها أو تتطلب على الأقل تعليمهم كيف يستخدمون هذه التقنيات مما يعني بالنتيجة الحاجة المستمرة لتدريبهم[1].

ومن خلال ما تقدم نلاحظ إن تطور الجرائم الإلكترونية له آثار مهمة ومنها الحاجة الماسة لتبني تقنيات حديثة تساعد الشرطة في جمع البيانات وتحليلها وفهمها من أجل الحصول على صورة واضحة في الجرائم الإلكترونية، وذلك لأن هذه الجرائم بحكم تعريفها يُعتمد على وسائل الإلكترونية في إرتكابها مما يتطلب تقنيات متطورة تتعامل مع هذه الجرائم، هذا من جهة ومن جهة ثانية فأن تطور التقنيات يسهل على الشرطة جمع الأدلة حينما يعانون مكان إرتكاب جريمة الإلكترونية، وذلك للسهولة النسبية للوصول وإستخدام العديد من التقنيات مثل الهواتف الذكية والحواسيب، وما قد يسهل من عملية المعاينة هو التطور السريع للتقنيات مثل الطائرات المسيرة والتي شهدت إستخدام وتطور واسع في السنوات القليلة الأخيرة والتي تتمكن من الوصول لأي مكان بسرعة هائلة مما يسهل عملية إجراء المعاينة[1].

ومن المهام التي تساعد فيها الحواسيب فيما يتعلق بالجرائم، هي جمع البيانات المتعلقة بالجرائم وخزنها وتحليلها، والتواصل مع المشتبه بهم، وإجراء بحث عن تفاصيل متعلقة بالجريمة الالكترونية، والكشف عن نشاط الضحايا في الجرائم من خلال كشف تاريخ نشاطهم في استخدام الحواسيب والأجهزة التقنية الأخرى والتي قد تكشف على سبيل المثال إن الشخص لم يكن ضحية جريمة قتل وانما كان الشخص منتحراً، فإستخدام الحواسيب في بعض جوانبه لا يتطلب خبرة عالية من اعضاء الشرطة او المحققين، ولكن في جوانب أخرى فإنه يتطلب مهارة وخبرة كبيرة[2].

لكن توجد صعوبات عدة في هذه المسائل، إذ يمكن لمرتكبي الجرائم الإلكترونية أن يحذفوا البيانات المتعلقة بالجريمة بسهولة، وكذلك يمكن للمتهم الذي يتم ضبط أجهزته، أن يحذف البيانات عن بعد مما يصعب المعاينة على الشرطة، وأيضا يمكن أن يتم عمل نسخة ثانية من الأدلة الموجودة على الحاسوب مما قد يعيق عملية التحقيق. أما عن تأثير بطاقات الائتمان فأنها قد توضح أنشطة مرتكبي الجرائم الإلكترونية من خلال الأجهزة التي ابتاعوها وارتكبوا فيها الجرائم، أو قد توضح ارتكابهم لجرائم الإحتيال الإلكتروني، وإن استخدامها يبين تاريخ نشاط مرتكب الجرائم مما يسهل العثور عليه.

---

(1)- Dr. Jarrod Sadulski, Unintended consequences of technology in policing, American Military University, 2017, the link:
((https://www.police1.com/american-military-university/articles/unintended-consequences-of-technology-in-policing-EQhuM6wsvpCNKqYF/)).

(1)- U.S. Department of Justice Office of Justice Programs National Institute of Justice, Investigative Uses of Technology: Devices, Tools, and Techniques, 2017, October 07.

(2)- ibid, page 34.

وأما الجرائم التي قد تنشأ عن استخدام أجهزة متعلقة ببطاقات الإئتمان هي، إمكانية إستخدام أجهزة اختراق تساعد المجرمين على حصول على بيانات شخصية للمستخدمين والتي قد تستخدم ضدهم [1] ، بالإضافة إلى امتلاك أجهزة تساعدهم على ترميز المعلومات المسروقة أو الإحتيالية مما يضفي عليها طابعاً شرعياً. وأيضاً تكمن المشكلة والصعوبة في أجهزة الإحتيال الخاصة ببطاقات الإئتمان، بسبب صغر حجمها مما يجعل عملية إيجادها أثناء المعاينة صعبة، فقد تتخذ شكل بطاقة ائتمان أو جهاز يرتبط بحاسوب ما أو جهاز مربع صغير، وتزداد الامور تعقيداً اكثر، بسبب سهولة الحصول على الاجهزة الإلكترونية التقنية والآلات واستخدامها دون تسجيلها أو التصريح عنها[2].

من الأجهزة الأخرى التي لها تأثير على عملية المعاينة هي أجهزة حفظ البيانات مثل الأقراص الدائرية وغيرها، وتسهل هذه الأدوات نسخ أي بيانات موجود على أي جهاز الكتروني والتي تسهل على المستخدم ارتكاب الجرائم مثل الإبتزاز أو التهديد[1].

وهناك أجهزة تقنية أخرى، تساعد المحققين ولها أثار مفيدة هي أجهزة التعقب والتي تستخدم للكشف عن الأجهزة الأخرى، فلو إستخدم الشخص جهاز ما يبث موجات راديوية فبإمكان الشرطة الكشف عنه من خلال الإستعانة بهذه الأجهزة، ويمكن من خلالها الكشف عن الأجهزة التي يستخدمها المجرم في إرتكاب الجريمة وغيرها. وكذلك الحال بالنسبة لآلات التصوير الرقمية في المنزل، فمن خلالها يمكن للشرطة أن تعرف كيف تم إرتكاب الجريمة وكيف دخل المجرمون للمنزل أو لمكان آخر معين، وغيرها من المسائل. ولكن أغلب هذه الاجهزة يمكن أن تخترق وتقرصن من قبل المجرمين وذلك للوصول لبيانات مهمة مفيدة لهم، ولا يمكننا هنا أن نوضح دور التقنيات وحجمها وعددها، لكننا حاولنا بيان مسألة مهمة، وهي أن التقنيات كما تساعد رجال الشرطة والمحققين في العثور على الأدلة وحصرها وجمعها، كذلك يمكن أن توظف من قبل المجرمين لإرتكاب الجرائم وخاصة الإلكترونية والتي تسهل عليهم حذف البيانات ومحوها[2].

---

(1)- U.S. Department of Justice Office of Justice Programs National Institute of Justice, op.cit, page 35.

(2)- Ibid, page 36.

(1)- S. Department of Justice Office of Justice Programs National Institute of Justice, op.cit page 40.

(2)- S. Department of Justice Office of Justice Programs National Institute of Justice, op.cit, page 47.

أولا : طرق إجراء المعاينة :

تتم المعاينة في جرائم الأنترنت كأي جريمة أخرى، عن طريق الانتقال إلى محل الواقعة الجرمية، والإنتقال هنا لا يكون إلى العالم المادي، وإنما إلى عالم افتراضي، أو عالم الفضاء الإلكتروني[1]، فالمعاينة تتم بالإنتقال إلى محل الواقعة الجرمية كقاعدة اجرائية مقررة في هذا الشأن، إلى أنه في إطار جرائم الأنترنت فإن الانتقال يعد من الموضوعات الجديدة، وذلك لان مسألة الانتقال هذه لا تكون بالضرورة عبر العالم الرقمي، فهناك عدة طرق يستطيع بواسطتها عضو سلطة التحقيق أو أعضاء الضبط القضائي، أن ينتقل بها إلى عالم الفضاء الإلكتروني للمعاينة، وذلك من خلال إجراء المعاينة عن طريق مكتبة المحكمة من خلال الكمبيوتر الخاص به[1]. وكذلك يحق له أيضا اللجوء إلى مقر عمل مزود بخدمة الإنترنت الذي يعد أفضل مكان يمكن من خلاله إجراء المعاينة. ويستطيع المحقق أيضا الغنتقال إلى العالم الأفتراضي للمعاينة من خلال مكتب الخبير التقني المتخصص إذا توافر له في القانون ما يبيح ذلك[2].

ونجد أن (المشرع الكويتي) أشار في المادة (76) من قانون الإجراءات الجنائية الكويتي، والتي تنص على انتقال المحقق لأي مكان ليثبت حالة الأمكنة، والأشياء، والأشخاص ، ووجود الجريمة المادية، فهل يكون للجريمة الالكترونية وجود مادي يمكن للمحقق معاينتها؟ نجد في هذه المادة أن المشرع الكويتي شرع هذه النص لضبط جريمة لها وجود مادي محسوس في العالم الخارجي، وما يؤكد ذلك هو نص المادة (91) من ذات القانون والتي أوجبت على المحقق وضع الأشياء والأوراق التي تضبط في حرز مغلق وتربط كلما أمكن. فالمحقق الذي يقوم بمعاينة الجريمة الإلكترونية، يجب أن يكون ملما بمهارات هذه التقنية والتكنولوجيا ، لكي يحافظ على الادلة الالكترونية، من التلف، أو الحذف، أو المحو[3].

ويرى الباحث أن الخبرة والمعاينة الجنائية في الجرائم الإلكترونية اليوم تحتاج إلى إدارة خاصة يعمل بها متخصصون في أنظمة المعلومات ويتمتعون بصفات وخبرات فنية وتقنية من خلال الصفة التي يتمتعون بها، وهو ما يتطلب إنشاء إدارة خاصة للخبرة والمعاينة في الجرائم الإلكترونية، ولا يجب الاكتفاء بمجرد تدريب القائمين على إدارة الخبرة الجنائية، أما رجال القضاء والمحققين وأعضاء

(1) - نادر عبد الكريم الغزواني، المصدر السابق ، ص 119.
(1) - إبراهيمي جمال ، المصدر السابق، ص 59.
(2) - أمير فرج يوسف ، المصدر السابق، ص 299.
(3) - عبدالفتاح بيومي حجازي، مبادئ الاجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، 2007، ص 158 وما بعدها.

الضبط القضائي، فلا شك أنهم يحتاجون للتأهيل من خلال إدخالهم لدورات وتدريب على استخدام مهارات الحاسب الآلي.

ثانيا : ضوابط إجراء المعاينة :

يرى جانب من الفقه أنه يجب توافر ضوابط عدة لإجراء المعاينة، يتوجب الاخذ بها عند القيام بمعاينة مسرح الجريمة الإلكترونية[1]، وهي: تحديد أجهزة الحاسب الآلي الموجودة في مكان المعاينة وتحديد موقعها بأسرع وقت ممكن وفي حالة وجود شبكة إتصالات يجب البحث عن خادم الملفات بهدف تعطيل الإتصالات لمنع تخريب الأدلة الموجودة أو محوها، مع تصوير الأجهزة الموجودة. وأيضاً وضع حراسة كافية على مكان المعاينة ومراقبة التحركات داخل مسرح الجريمة ورصد الاتصالات الهاتفية من وإلى مسرح الجريمة مع أبطال مفعول أجهزة الهاتف النقال، لكي لا يتم اختراق الانظمة والبيانات بطريقة معينة مما يؤدي إلى تدمير أدلة الجريمة المعلوماتية، متى ما تم توصيلها بأجهزة محل المعاينة[1]. وكذلك ملاحظة الطريقة المعد بها النظام المعلوماتي والآثار التي يخلفها ومعرفة السجلات الإلكترونية التي تزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز المتصل عن طريق الدخول إلى النظام أو الموقع، أو الدخول معه في حوار، وبرتوكولات الاتصال عبر الإنترنت وان تعلقت الجريمة بهذه الشبكة والتي تعرف باختصار (ip) ، ويتعين أيضا ملاحظة وإثبات حالة التوصيلات الخيوط المتصلة بكل مكونات النظام الإلكتروني لكي يمكن تحليل البيانات و مقارنتها والوصول إلى الدليل عند عرض الأمر إلى القضاء[2]. وعدم نقل المواد المعلوماتية خارج مسرح الجريمة الا بعد التأكد من خلو المحيط الخارجي للحاسب الآلي من مجالات القوة المغناطيسية التي قد تتسبب في محو البيانات ولن يتأثر ذلك إلا عن طريق خبراء الحاسب الآلي، ولذلك يجب أن يتضمن الفريق الذي يتولى ضبط وتحريز الأدلة على أثنين أو أكثر من خبراء الحاسب الآلي. 5- التحفظ على محتويات سلة المهملات وما فيها من أوراق ممزقة وشرائط وأقراص ممغنطة وغير سليمة أو محطمة، ورفع البصمات التي قد توجد عليها والتحفظ على مستندات الإدخال والمخرجات الورقية لجهاز الحاسب الآلي[3].

(1) - د. رامي متولي القاضي ، د. عمر سالم، المصدر السابق، ص 280 .
(1) - أحمد محمود خليل، التحقيق الجنائي، دار الكتب والدراسات العربية، 2017 ، ص 209.
(2) - د. محمود رجب فتح الله ، مسرح الجريمة إلكترونية، المصدر السابق، ص 252.
(3)- حفصي عباس جرائم التزوير الإلكتروني، اطروحة دكتوراه، جامعة وهران - 1 ، كلية العلوم الإنسانية، الجزائر، 2014 ،ص 48.

المطلب الثاني

أثر التطور التكنولوجي في التفتيش في الإلكتروني

التفتيش يهدف إلى تحديد مدى جدوى تقديم المتهم إلى المحاكم الجنائية لإقرار هذا الحق في مواجهته وأيضا يُعد التفتيش والمعاينة والتحقيق الإبتدائي، هي من الضمانات المقررة دستوريا للمتهم، إذ يجري التحقيق الابتدائي عادة من قبل الضباط المسؤولين عن التحقيق في مراكز الشرطة ومن قبل المحققين أحياناً، وعملهم في ذلك يتم تحت اشراف قاضي التحقيق، وعضو الادعاء العام في هذه المرحلة ويكون دور قضاة التحقيق، دوراً إيجابياً في جمع أدلة الاثبات أو النفي للوصول إلى الحقيقة، وتبدو أهمية مرحلة التحقيق الإبتدائي في تحضير الدعوى وتحديد مدى قابليتها للنظر أمام قضاء المحكمة.

الفرع الأول

مفهوم التفتيش وأسبابه

الأصل في القانون أنه لكل شخص ومكان حرمة، لا يمكن انتهاكها واجراء التفتيش بحقها، ولكن قد استثنى المشرع الجنائي هذه المبدأ وقد سمح بإجراء التفتيش لبعض الأشخاص والأماكن عند الضرورة، وقبل الدخول في شرح هذا الموضوع ، يتوجب علينا في البدء توضيح مفهوم التعريف اللغوي والاصطلاحي والتشريعي للتفتيش.

فالتفتيش هو إجراء من إجراءات التحقيق يقوم به موظف مختص طبقاً لإجراءات قانونية في محل يتمتع بحرمة بهدف الوصول إلى أدلة مادية لجناية أو جنحة تحقق وقوعها لأثبات ارتكابها أو نسبها إلى المتهم[1]. وأيضاً عرفه بعضهم وقالوا: هو إجراء قانوني، يتضمن في جوهره ثم اعتداء على حق الإنسان في الاحتفاظ بسره وحرمة مسكنه، فالتفتيش ينظمه القانون لتحقيق مصلحة المجتمع في الوصول إلى أدلة الجريمة[2].

أما تعريف التفتيش الإلكتروني: هو عملية تفتيش تنصب على المكونات المادية بأوعيتها المختلفة، داخل أنظمة الحاسب الالي، للبحث في أي شيء يتصل بالجريمة المعلوماتية، للكشف عنها، ويدخل في نطاق التفتيش التقليدي وفقا لإجراءات قانونية معمول بها[3]. وهناك من يعرفه بأنه : البحث في مستودع سر المتهم على أشياء مادية أو معنوية تفيد في كشف الحقيقة ونسبتها إليه. أو الاطلاع على

(1) - د. حسين بن سعيد الغافري ، المصدر السابق، ص 472.
(2) - د. قدري عبد الفتاح الشهاوي، ضوابط التفتيش في التشريع المصري والمقارن، منشأة المعارف، الإسكندرية، 2004 ، ص 15.
(3) - د. امحمدي بوزينة أمنة، المصدر السابق، ص 62.

محل منحه القانون حماية خاصة، كونها مستودع سر صاحبه، يفترض في ذلك أن يكون هذا المحل جهاز الحاسوب و أنظمة رقمية أو الإنترنت[1]. وعلى ضوء هذا التعريف فإن التفتيش في الجرائم الإلكترونية، وعن الدليل الإلكتروني الرقمي، فهو يشمل ثلاثة مكونات، المكونات المادية للحاسب الآلي والمكونات المنطقية للحاسب الآلي. بالإضافة إلى التفتيش في شبكات الحاسب الآلي[2]. فالتفتيش يعد من أهم إجراءات التحقيق في الكشف عن الحقيقة، لأنه غالباً ما يسفر عن أدلة مادية تؤدي إلى كشف ملابسات الجريمة ونسبتها للمتهم.

ثانيا : أسباب التفتيش الإلكتروني :

لا يمكن أن تكون إجراءات التفتيش صحيحة ومشروعة، إلاّ عندما تكون هناك أسباب قانونية، تستدعي القيام بالتفتيش وانتهاك حرمة الشخص والمسكن والأشياء، والتي ضمن لها الدستور الحماية اللازمة لعدم انتهاكها، ويمكن القول أن أهم ضمانة لإجراء التفتيش هو وجود سبب عن إصدار أمر التفتيش، سواء على الاشخاص أم الأماكن أو الاشياء ، فوجود السبب، هو من يبرر إجراء التفتيش، فسبب وقوع الجريمة، يتم على أساسها إصدار قرار التفتيش والاشخاص المراد تفتيشهم، بناء على دلائل وقرائن كافية، لإرتكاب جريمة ما، عملاً بقاعدة المشروعية، وهي "لا جريمة ولا عقوبة إلا بنص" بمعنى أنه لا يجوز التفتيش من اجل فعل غير مجرم ولا يشكل جريمة، فوجود سبب لإصدار أمر التفتيش يعد ضمانة بالنسبة للمتهم وحرمة الاشخاص والاماكن[1]. وعلى ضوء ذلك سنحاول ذكر أهم الاسباب التي تستدعي اجراء التفتيش للبحث عن الادلة الإلكترونية، والتي تفيد في كشف الحقيقة. وهي كالآتي:

1- وقوع جريمة (جناية أو جنحة) فوقوع الجريمة هو الدافع أو المبرر للإجراء التفتيش ويتحقق بوقوع الجريمة الإلكترونية، وإتهام اشخاص معينين بإرتكاب جريمة أو الاشتراك فيها، ووجود أدلة يخشى اتلافها أو حذفها، موجودة في محل الجريمة، أو الشخص المراد تفتيشه، أي أن تكون الجريمة وقعت بالفعل فلا يجوز إجراء التفتيش بحثا عن أدلة جريمة مستقبلية[2].

2- التحقق الفعلي من وقوع الجريمة الإلكترونية، فهذا السبب لا يقوم إلاّ بعد وقوع الجريمة، بناء على إخبار من المجنى عليه أو من ذويه أو من الجهات المخولة قانوناً، وعلى ضوء ذلك يحق لقاضي التحقيق إصدار أمر التفتيش في حال وقوع فعل يشكل جناية أو جنحة، ولا بد أن تشكل هذه الجريمة

---

(1) - د. لورنس سعيد الحوامدة، المصدر السابق، ص916.

(2) - د. محمد ممدوح بدير، المصدر السابق صفحة 113.

(1) - فايز محمد راجح غلاب، الجرائم المعلوماتية في القانون الجزائري واليمني، أطروحة دكتوراه، جامعة الجزائر، كلية الحقوق ، 2010، ص 317.

(2) - فيروز عوض الكريم صالح ، المصدر السابق، ص 115.

قدراً من الخطورة، ويرى القاضي انه من الضرورة القيام بالتفتيش عنها لما تشكله الجرمية إعتداء على الحقوق الفردية أو الحريات [1].

3- السعي نحو الحصول على الدليل الرقمي أثناء التحقيق، بمعنى أن من أهم الاسباب التي تدفع الاشخاص المعنين لإجراء التفتيش هو السعي نحو إستخلاص الدليل الإلكتروني لإثبات الجريمة وكل ما يتعلق بها من ظروف وإحداث، فإجراء التفتيش هو وسيلة لتحقيق غاية، تتمثل هذه الاخيرة بالكشف عن وقائع الجريمة، وعلى أساس ذلك فأن سبب إجراء التفتيش هو وقوع جناية أو جنحة، وثمة قرائن قوية تفيد في كشف الحقيقة والمتهم[2].

4- الحفاظ على الادلة وكل ما يتعلق بالوسيلة الإلكترونية في مكان الحادث، خوفاً عليها من التلف، أو المحو، أو رفع البصمات أو التلاعب والتغيير وغيرها من الافعال التي قد تؤدي إلى ضياع معالم الجريمة[1].

وقد ذهبت محكمة النقض المصرية في حكم لها (الأصل في القانون أن الإذن بالتفتيش هو إجراء من إجراءات التحقيق، لا يصح إصداره إلا لضبط جريمة، جناية أو جنحة، وقعت بالفعل، وترجحت نسبتها إلى متهم معين، وأن هناك من الدلائل ما يكفي للتصدي لحرمة مسكنة أو لحرمته الخاصة)، وبناءً عليه وتطبيقاً على الجرائم الإلكترونية، فإنه لابد أن يكون التفتيش مشروعاً، وأن نكون بصدد جريمة إلكترونية، واقعه بالفعل، سواء كانت جناية أم جنحة. ولابد من إتهام شخص أو أشخاص معينين بارتكاب هذه الجريمة الإلكتروني أو المشاركة فيها. وكذلك لابد من توافر أدلة قوية أو قرائن على وجود أجهزة تقنية، أو أدلة إلكترونية رقمية، تفيد في كشف الجريمة[2].

أما المشرع العراقي فقد تناول موضوع أسباب إجراء التفتيش من خلال نص المواد (74 و 75 و 76 و 77 و 78 و 79)[3]، من قانون أصول المحاكمات الجزائية رقم (23) لسنة 1971 المعدل، وهذه الاسباب تتعدد وتتنوع وفق ظروف الجريمة والحادثة، فقد وسع المشرع الجنائي من تعدد أسباب القيام بإجراء التفتيش عند التحقيق في أي جريمة أو شخص يشتبه به، أو وجود ما يشكل خطراً، أو في حال وجود سبب يفيد في الكشف عن الجريمة تحت اي ظرف كان، وهذا ما يحسب للمشرع العراقي لكونه قد أحاط بجميع ظروف وأسباب تفيد للقيام بالتفتيش عن أي أدلة، وهذا قد يساعد المحققين والقضاة للتفتيش عن الأدلة الإلكترونية كأحد طرق إثبات الجريمة الإلكترونية.

---

(1) - لهوى رابح، الشرعية الإجراءات للإدلة المعلوماتية المستمدة من التفتيش، أطروحة دكتوراه ، جامعة باتنة 1 ، كلية الحقوق والعلوم السياسية، الجزائر، 2021، ص 144.

(2) - د. قدري عبد الفتاح الشهاوي ، المصدر السابق، ص 18 .

(1) - حفصة عباس صفحة، المصدر السابق، ص 48.

(2) - د. حسين بن سعيد الغافري ، المصدر السابق، ص 487.

(3) - ينظر: المواد (74 - 79) من قانون إصول المحاكمات الجزائية رقم 23 لسنة 1971 المعدل.

الفرع الثاني

مدى قابلية الأنظمة التكنولوجية والتقنية للتفتيش

أولا : محل التفتيش في الجرائم الإلكترونية:

يشترط لصحة التفتيش، أن ينصب على محل، ويقصد بمحل التفتيش عند بعضهم، بالمكان الذي يحتفظ فيه الشخص بأسراره المادية، أما الاسرار المعنوية فلا يمكن التفتيش عنها، لكونها تقع في كمائن النفس، ومن ثم فلا يمكن التفتيش عنها، الاّ بواسطة الإستجواب أو الإعتراف[1]. ومحل التفتيش في الجرائم، يقصد به مستودع سر الإنسان، فهو إما مسكن أو شخص أو رسائل في الجرائم التقليدية، أما محل التفتيش في الجرائم الإلكترونية، فهو الحاسوب أو أي جهاز تقني[1]، والبحث في المكونات المادية والمعلوماتية (البيانات الرقمية)، أما الجهة المختصة لإصدار أمر التفتيش، فتختلف بأختلاف التشريعات، فبعض التشريعات منحت هذا الاختصاص لقاضي التحقيق كالتشريع العراقي، ومنها من منح هذا الاختصاص للنيابة العامة، كما هو الحال في مصر والسودان[2]. وأيضاً يتمثل محل التفتيش، بالبحث عن البيانات المخزنة في الاجهزة التقنية الحديثة، من خلال القيام بعملية الولوج للأنظمة المعلوماتية التي يتم تحديدها، لضبط ما يعد صالحا كدليل أو قرينة لأثبات إرتكاب الجريمة[3]. وهذا يقتضي من الشخص القائم بتفتيش معرفة كيفية التعامل مع برامج وملفات البيانات المخزنة في الحاسب الآلي، وكذلك الحذر من إستعمال كلمة المرور للدخول إلى النظام، و تثير مسألة محل التفتيش مشكلة خاصة، بكيفية تنفيذ إذن التفتيش والذي يشترط فيه أن يكون محدداً في نطاق وحدود تنفيذ الإذن بالتفتيش، وقد ذهب بعض الفقه الجنائي أن محل التفتيش في الجرائم الإلكترونية، ينبغي أن يشمل البرامج أو الكيانات المنطقية، والبيانات المسجلة في ذاكرة الحاسبة، أو في مخرجاتها، والتسجيلات المثبتة لاستخدام نظام المعالجة الآلية للبيانات، وهذا ما أخذت به الشرطة الكندية، إذ إعتمدت الشرطة التابعة لمركز المعلوماتية الكندي نموذجا ، للإذن بالتفتيش يتضمن التصريح بالبحث عن ضبط البرنامج أو كيان الحاسب المنطقي، والتي يدخل فيها برنامج التطبيق، ونظم التشغيل وما يتفرغ عنها من نظم البيانات المستخدمة بواسطة برنامج الحاسوب، وأيضا السجلات التي تثبت إستخدام الأنظمة الآلية المعالجة للبيانات والسجلات المستخدم في عملية الولوج داخل النظام الآلي لمعالجة البيانات[4].

---

(1) - فايز محمد راجح غلاب، المصدر السابق، ص 320.
(1) - د. حسين بن سعيد الغافري ، المصدر السابق، ص 490.
(2) - فيروز عوض الكريم صالح، المصدر السابق، ص 241.
(3) - مصطفى عبد الباقي، المصدر السابق ، ص 289.
(4) - د. رامي متولي القاضي، د. عمر سالم، المصدر السابق، ص 272.

فعملية التفتيش يمكن أن تشمل بعض المكونات الإلكترونية في بعض الحالات، وهذه الحالات هي كالآتي: الحالة الأولى: في حالة ما إذا كانت هذه المكونات موجودة في مكان خاص في مسكن المتهم أو أحد ملحقاتها، فإنها تأخذ الأحكام ذاتها، المقررة لتفتيش المسكن، وبنفس الضمانات المقررة في مختلف التشريعات المقارنة. الحالة الثانية: إذا كانت مكونات الحاسب الآلي المادية منعزلة عن غيرها من أجزاء الكمبيوتر أم أنها متصلة بجهاز أو نهاية طرفية في مكان اخر، كمسكن غير مسكن المتهم، بحيث إذا كانت هناك بيانات مخزنة في أوعية نظام آخر[1]، فإن عملية الكشف تصبح صعبة جدا، وربما مستحيلة وذلك حتى تتم عملية التفتيش في هذه الاجهزة المرتبطة بأجهزة في أماكن أخرى، يتعين مراعاة القيود والضمانات التي يوجبها المشرع لتفتيش هذه الأماكن. وفي ألمانيا، يمكن أن يمتد التفتيش إلى سجلات البيانات التي تكون في موقع آخر تطبيقاً لمقتضيات القسم (103) من قانون الإجراءات الجنائية الالماني، وذلك عندما يكون مكان تخزين البيانات الفعلي خارج المكان الذي يتم فيه التفتيش. الحالة الثالثة: إذا وجدت مكونات الحاسوب المادية في حالة الحاسبات الآلية المحمولة، في أماكن عامة بطبيعتها كالمطاعم، والسيارات العامة، وسيارات الأجرة، إلى أخره. فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص، وبنفس الضمانات والقيود ذاتها المنصوص عليها في هذه الحالات، وقد أخذت بعض التشريعات بذلك كالتشريع الجنائي الكندي في المادة (487) والتي أجازت إصدار امر قضائي بالتفتيش وضبط أي شيء يؤدي إلى إعتقاد بأن الجريمة قد وقعت أو يشتبه في وقوعها، ونصت المادة نفسها صراحة على إمكانية تفتيش مكونات الحاسوب المادية للكشف عن الجريمة المعلوماتية، باتخاذ أي إجراء أو القيام بأي فعل لازم لجمع الأدلة والحفاظ عليها[1].

وعن مدى إمكانية تفتيش مكونات الحاسب الآلي ، فأن أي جهاز حاسب تقني يتكون من مكونات مادة (hard ware) ومكونات منطقية (soft ware)، كما أن له شبكات إتصالات بصرية سلكية ولا سلكية، سواء كان ذلك على المستوى المحلي أو الدولي، إن المحل الذي ينصب عليه النشاط الإجرامي للجرائم الإلكترونية، يكمن في المعلومات التي تحتويه وهي مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح لان تكون محلاً للتبادل والاتصال أو للتفسير والتأويل أو للمعالجة، سواء بواسطة أفراد أو الانظمة الإلكترونية وهي تتميز بالمرونة فيمكن تغييرها وتجزئتها وجمعها أو نقلها بوسائل واشكال مختلفة والمعلومات تختلف عن البيانات، إذ أن الأخيرة تعبر عن مجموعة من الأرقام والكلمات والرموز أو الحقائق أو الاحصائيات الخام، التي لا علاقة بين بعضها

(1) - علي محمود علي، المصدر السابق ، ص 48.
(1) - د. امحمدي بوزينة أمنة ، المصدر السابق، ص 62.

بعضا ولم تخضع بعد للتفسير أو التجهيز للاستخدام وتخلو من المعنى الظاهر في أغلب الاحيان، أما المعلومات فهي المعنى الذي يستخلص من هذه البيانات.

وتجدر بالإشارة إلى ان ما يحتويه الحاسب الالي من معلومات وبيانات لا يمكن النظر اليها بمعزل عن الوسيط المادي الذي يمكن أن تدمج فيه، فعلى الرغم من الأهمية الأقتصادية للمعلومات فإنها تبقى مجرد أفكار غير قابلة للسرقة، أو أن تكون هذه المعلومات محلاً لعدد من الجرائم كالنصب أو خيانة الامانة، ومن ناحية اخرى فإنه قد لا يتوافر في هذه المعلومات مقومات الملكية الفكرية حتى تحميها النصوص الخاصة بحماية هذا النوع من الملكية[1].

وفيما يتعلق بإمكانية التفتيش وضبط الأدلة في نظام الحاسب الالي، يرى جانب من الفقه الجنائي أنه متى كان الغاية من التفتيش هي ضبط الأدلة المادية التي تفيد في كشف الجريمة، فان هذا المفهوم يمتد حتى يشمل البيانات الإلكترونية بمختلف إشكالها وأنواعها، وعلى العكس من ذلك فهنالك من يرى اذا كانت الغاية من إجراء التفتيش هي ضبط الادلة المادية التي تفيد في كشف الحقيقة فإن هذا المفهوم المادي لا ينطبق على البيانات والمعلومات الالكترونية غير المحسوسة أو المحسوسة، لذلك يقترح هذا الجانب الفقهي ، إزاء النقض التشريعي ضرورة أن يضاف إلى هذه الغاية التقليدية للتفتيش، إمكانية البحث وضبط المواد المعالجة عن طريق الحاسب الالي أو بيانات الحاسب الالي ، وبذلك تصبح الغاية الجديدة من التفتيش بعد هذا التطور التكنولوجي هي البحث وضبط الادلة المادية أو أي أدلة أخرى داخل الحاسب الالي[1].

ويرى جانب من الفقه[2] أن التفتيش الإلكتروني العابر للحدود لابد أن يتم في إطار إتفاقية خاصة ثنائية أو دولية تجيز هذا الامتداد وتعقد بين الدول المعنية، ومن ثم فإنه لا يجوز القيام بذلك التفتيش عبر الحدود في غياب تلك إتفاقية أو على الاقل الحصول على إذن الدولة الأخرى وهذه يؤكد على أهمية التعاون الدولي في مجال مكافحة الجرائم المرتكبة عبر الإنترنت وتطبيقا لهذا الإجراء الأخير ما حدث في ألمانيا أثناء جمع إجراءات التحقيق عن جريمة الغش وقعت في بيانات الحاسب الآلي، إذ تبين وجود اتصال بين الحاسب الآلي المتواجد في ألمانيا وبين شركة الاتصالات في سويسرا، إذ يتم تخزين البيانات الإلكترونية فيها وعندما أرادت سلطات التحقيق الألمانية ضبط هذه البيانات فلم تتمكن من ذلك إلا عن طريق التماس المساعدة الذي تم بالتبادل بين الدولتين . ومع ذلك إجازة المادة (32)

(1) - د. جاسم خريبط خلف، التفتيش في الجرائم المعلوماتية، بحث منشور ، مجلة الخليج العربي، المجلد 41، العدد 3 – 4 ، 2013 ، ص 242.

(1) - د. محمود رجب فتح الله ، مسرح الجريمة إلكترونية ، ص 258.

(2) - د. نبيلة هبه هروال، الجوانب الاجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الاسكندرية، 2007 ، ص 226.

من الإتفاقية الأوروبية بشأن جرائم الإنترنت إمكانية الدخول بغرض التفتيش والضبط في أجهزة أو شبكات تابع لدولة أخرى بدون إذنها في حالتين: الأولى إذا تعلق التفتيش بمعلومات وبيانات مباحة للجمهور، والثانية إذا رضي صاحب أو حائز هذه البيانات بهذا التفتيش[1].

ثانيا : شروط التفتيش الإلكتروني :

إن التفتيش في الجرائم الإلكترونية له طبيعة خاصة ومتميزة عن التفتيش في الجرائم التقليدية للمساكن والأشخاص، لأنه يخضع في إجراءاته إلى نصوص قانون الإجراءات الجزائية التي تلزم وقوع جريمة وإتهام شخص أو أشخاص معينين بارتكابها، بالإضافة لوجود قرائن ودلائل على ما يفيد في كشف الحقيقة، في الجهاز الإلكتروني لدى المتهم أو غيره، ومع توفر تلك الشروط فإنه يحق لسلطة التحقيق تفتيش الجهاز وملحقاتها ومكوناتها المادية والمعنوية للوصول للأدلة محل الجريمة، وما يحتمل أن يكون قد استعمل لارتكابها أو نتج عنها، وكل ما من شأنه يفيد في الحقيقة [1].فالدليل الإلكتروني لا ينتج فقط من جهاز الحاسب الآلي، وانما مصطلح الجهاز الإلكتروني يشمل جميع الأجهزة التي تحتوي على معالج بيانات ذات طبيعة رقمية من خلال تحويل بيانات الأرقام مثل كاميرات الفيديو أو التصوير الفوتوغرافي وأجهزة الهاتف النقال والأجهزة اللوحية وغيرها من الأجهزة الحديثة والبيانات[2]. ولهذا فإن إجراء التحقيق والتفتيش على محتويات الأجهزة الإلكترونية وكل ما يتعلق بالجريمة الإلكترونية، يتطلب الالتزام ببعض الشروط الشكلية والموضوعية، لكي تكون إجراءات إستحصال الدليل الرقمي الجنائي محصنة، ويكون لهذا الدليل القيمة القانونية عند الحكم في الدعوى من قبل محكمة الموضوع ، وعلى أساس ذلك فلا بد من توافر بعض الشروط عند إستخلاص الدليل الإلكتروني وهي كالآتي:

1- الشروط الشكلية للتفتيش الإلكتروني .

يشترط عند إصدار أمر بالتفتيش أن يكون محل التفتيش معيناً، وأن يكون مما يجوز تفتيشه، ويشترط بالضرورة أن يكون أمر التفتيش مسبباً، فاذا توافرت شروط التفتيش، أمكن اجراؤه، في أي محل يفيد إمكانية التوصل إلى كشف الحقيقة، إلاّ أن هناك بعض الاماكن التي منحها القانون الحصانة، ولا

(1)- د. محمد ممدوح مدير ، المصدر السابق، ص 117 .
(1) - علي محمود علي ، المصدر السابق، ص 35.
(2) - نبيلة هبة هورال، الجوانب الاجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات ، دار الفكر الجامعي، الاسكندرية، 2013، ص 237.

يمكن تفتيشها حتى وإن توافرت شروط التفتيش العامة، وذلك لتعلقها بالمصلحة العامة، يرى المشرع أنها أولى بالحماية والحصانة[1]، ويمكن إجمال هذه الأسباب على النحو الأتي:

أ- - أن يكون الإذن بالتفتيش مسبباً، له ضرورة ملحة، وتتمثل هذه الاخيرة بوقوع جريمة، بمعنى لا يمكن إصدار أمر التفتيش دون وقوع جريمة (جناية أو جنحة).

ب- - أن يكون الإذن بالتفتيش بحضور المتهم أو من ينيب عنه ان امكن، يعد حضور أشخاص معينين أثناء إجراء التفتيش من قبل الشخص المكلف بذلك قانونا، ويعد ذلك من الضمانات التي تكفل الإجراءات بشكل صحيح، ما يبعد الشك حول إمكانية دس الدليل من قبل القائمين به، وضمانة للقائم بالتفتيش من اتهامه من قبل المتهم أو أصحاب المكان بأن هناك أشياء أختفت بعد التفتيش كالمصوغات الذهبية والأموال.

ت- - تحرير محضر بإجراء التفتيش. يجب على القائم بأمر التفتيش أن يحرر محضر التفتيش بتدوين ما نتج عن التفتيش سواء تم الحصول على الدليل أم لا. وقد أقرت معظم التشريعات هذا الأمر، فنجد أن قانون الإجراءات الجنائية السوداني نص على أن تضبط الأوراق والاسلحة والات وكل ما يحتمل أن يكون قد إستخدم في إرتكاب الجريمة أو نتج عن ارتكابها أو ما قد وقعت عليه الجريمة، وتعرض تلك المضبوطات على المشتبه به أو المتهم، ويطلب منه أبداء ملاحظاته ويحرر ذلك في محضر ويوقع عليه أو يذكر فيه امتناعه عن التوقيع[1].

ث- تحديد وقت إجراء التفتيش يُعد وقت التفتيش من الأمور المهمة والتي تساعد في الحصول على الدليل الإلكتروني من عدمه. وذلك لسهولة إتلاف الدليل المعلوماتي ومحوه من قبل المتهم، فكلما كان التفتيش في وقت قريب بعد الجريمة، كلما كان فرصة الحصول على الدليل أكبر. ونجد أن بعض التشريعات قيدت ذلك بوقت معين كالقانون الأمريكي والقانون السوداني، وبعضها لم تقيده بوقت، كالتشريع العراقي، الذي لم يقيد التفتيش في زمن معين وكذلك المشرع المصري[2] .

ج- يجب تحديد نوع النظام المراد تفتيشه، ومن ثم يجب أن يكون القائم بالتفتيش على علم بقدر كبير بعلوم الأجهزة التقنية، حتى يتسنى له معرفة نظام الحاسوب المراد تفتيشه، أو الإستعانة بخبراء النظام للإستعانة بهم في عملية إجراء التفتيش ومعرفة إمكانية الحصول على كلمة السر والدخول للنظام المراد تفتيشه، ولهذه الإجراءات خصوصية تتميز بها، وذلك لدقة التعامل مع الأجهزة والبرامج الموجودة عليها، لكي تتم على أكمل وجه[3].

---

(1) - د. قدري عبد الفتاح الشهاوي ، المصدر السابق، ص 111.
(1) - د. محمود صالح العدلي المصدر السابق ، ص 1225.
(2) - فيروز عوض الكريم صالح، المصدر السابق، ص 118.
(3) - د. امحمدي بوزينة أمنة، المصدر السابق، ص 65.

2- الشروط الموضوعية للتفتيش الإلكتروني .

أما الشروط الموضوعية لإصدار أمر التفتيش فيمكن إجمالها بخمس نقاط على النحو الآتي:

أ- أن يكون التفتيش متعلقاً بجريمة إما تكون جناية أو جنحة قد وقعت فعلاً.
ب- أن يكون هناك إتهامات موجهة للشخص المراد تفتيشه أو تفتيش مسكنه[1].
ت- أن يكون التفتيش قد حدد لمكان محدد أو قابل للتحديد على الاقل[2].
ث- أن يكون التفتيش بقصد ضبط الأشياء المتعلقة بالجريمة أو تفيد في كشف الحقيقة[3].
ج- الحفاظ على السرية لضمان الحصول على دليل[4].

ونجد أن (التشريع الاردني) تناول موضوع التفتيش بنص المادة (13) على أنه : " أ- مع مراعاة الشروط والاحكام المقررة في التشريعات ذات العلاقة، يجوز لموظفي الضابطة العدلية الدخول إلى أي مكان يشتبه بإستخدامه لإرتكاب أي من الجرائم المنصوص عليها في هذا القانون، كما يجوز لهم تفتيش الأجهزة والإدوات والبرامج والأنظمة والوسائل المشتبه في استخدامها لارتكاب اي من تلك الجرائم بإستثناء بيوت السكن إلا بإذن من المدعي العام المختص قبل الدخول إليها، وفي جميع الأحوال على الموظف الذي قام بالتفتيش أن ينظم محضرا بذلك ويقدمه إلى المدعي العام المختص".

أما المشرع العراقي فقد تناول موضوع التفتيش في الفصل الرابع، من قانون أصول المحاكمات الجزائية العراقي رقم (23) لسنة 1971 وتعديلاته، بعنوان (التفتيش) من المادة (72) ولغاية المادة (86) وهذا يدل على أهتمام وتوسع المشرع العراقي في موضوع التفتيش، إذ جاء بنص المادة (72/أ/ب) منه على انه: "لا يجوز تفتيش أي شخص أو دخول أو تفتيش منزله أو أي محل تحت حيازته إلا في الاحوال المبينة في القانون" أما الفقرة (ب) من ذات المادة فقد تضمنت : "يقوم بالتفتيش قاضي التحقيق أو المحقق أو عضو الضبط القضائي بأمر من القاضي أو من يخوله القانون إجراؤه". ونلاحظ من نص المادة أعلاه أن المشرع العراقي قد وسع من مفهوم التفتيش وسمح لعدة جهات بإجراء التفتيش في حال تم ارتكاب جريمة ما، وايضا فأن المشرع وسع من مفهوم أمر التفتيش من حيث الاشخاص والاماكن، من خلال مضمون نص المادة (73/ب) والتي تنص على أنه: "يجوز تفتيش أي مكان دون مراعاة الشروط السابقة في حالة طلب المساعدة ممن يكون في داخله أو حدث حريق أو غرق أو ما شابه ذلك من أحوال الضرورة". وهنا يقصد في حال طلب المساعدة ممن

(1) - د. رامي متولي القاضي، المصدر السابق ، ص 270.
(2) - نادر عبد الكريم غزواني، المصدر السابق ، ص 120.
(3) - د. قدري عبد الفتاح شاوي ، المصدر السابق، ص 94.
(4) - عمار عباس الحسيني، مدى مشروعية التسجيل الصوتي بالهواتف النقالة كدليل في الاثبات الجنائي، بحث منشور، مجلة اهل البيت عليهم السلام ، العدد 8 ، 2009 ، ص 170.

يكون في داخله أو حدوث حريق أو غرق أو ما شابه ذلك من احوال الضرورة، وعلى ضوء هذا المفهوم فانه في حال طلب المجنى عليه إجراء التفتيش الالكتروني من قبل الاشخاص المعينين قانوناً، فهنا لا بد من الاستجابة لهذا الطلب ، وذلك لكون نص المادة يفيد العموم وليس على سبيل الحصر. أما نص المادة (75) فقد نلاحظ أن المشرع العراقي قد توسع اكثر في شمول الاشخاص والاشياء أو اي مكان اخر ، وذلك من خلال مضمون النص : " لقاضي التحقيق ان يقرر تفتيش اي شخص أو منزله أو اي مكان اخر في حيازته ....." إذ إن تعبير المشرع العراقي في مضمون نص المادة أعلاه عندما ذكر عبارة (أي مكان أخر) فان مفهوم هذا النص يسمح لأعضاء الضبط القضائي تفتيش أي مكان دون حصر الاشياء، ولكن يجب أن يكون أمر التفتيش قد صدر بناء على أمر قضائي. وهذا ما أكدته نص المادة (79) من القانون ذاته والتي تنص على أنه: " للمحقق أو لعضو الضبط القضائي أن يفتش المقبوض عليه في الاحوال التي يجوز له فيها القبض عليه قانوناً، ويجوز له في حالة وقوع جناية أو جنحة مشهودة أن يفتش منزل المتهم أو أي مكان تحت حيازته....." . ويدخل ضمن مفهوم أي مكان تحت حيازته، الاجهزة الإلكترونية بكل أنواعها، وأيضا فإن الجريمة المشهودة التي جاء ذكرها في نص المادة (79) يمكن أن تقع وتتحقق من خلال التصوير ومقاطع الفيديو، سواء كان هذا التصوير مباشراً أم مخزناً في ذاكرة الحاسب الآلي. ويجدر بالإشارة إلى أن الدستور العراقي النافذ لعام 2005 قد منح حق اتخاذ الإجراءات القانونية في مراقبة المراسلات البريدية والهاتفية الإلكترونية متى كانت هناك ضرورة للكشف عن جريمة ما تمس العدالة والأمن [1].

(1) - ينظر المادة (38) من الدستور العراقي النافذ لعام 2005.

الفصل الثاني

أثر التطور التكنولوجي على إجراءات التحقيق والمحاكمة

لعب التطور التكنلوجي دوراً كبيراً في مجال التحقيق والمحاكمة، وظهر ذلك التطور الملحوظ من خلال الجرائم الالكترونية والتي أصبحت تمارس مثل هذه الجرائم في شتى تفاصيل الحياة اليومية في كل أنحاء العالم، وهذا ما أدى إلى تطور وتغير حتى في مجال وأسلوب التحقيق والمحاكمة، فسابقا عندما يتم إرتكاب الجريمة، فإن الاسلوب التقليدي لإرتكاب أي جريمة كان لا يتعدى استخدام المواد المادية التقليدية، سواء في جرائم السرقة، أو التهديد، أو القتل، وكان أسلوب التحقيق في مثل هذه الجرائم، أسلوبا تقليديا ولا يتضمن تعقيداً أكثر ما يكون من رفع البصمات عن طريق فريق الأدلة الجنائية أو جمع الأدلة المادية من خلال معاينة مسرح الجريمة، أما اليوم فقد أصبح إرتكاب الجريمة أكثر تعقيداً وأكثر تطوراً، وذلك بسبب دخول التطور التكنولوجي والتقني في كل تفاصيل التعامل، سواء على الصعيد الإجتماعي والأقتصادي والسياسي والدولي، واصبح ارتكاب الجريمة اسهل وأسرع ولا تحتاج إلى وسائل مادية تقليدية لإرتكابها سواء اقتناء المجرم الإلكتروني على جهاز تقني حديث، لتحقيق مأربه، وبالمقابل فان وسائل التحقيق والمحاكمة ايضاً واكبت هذا التطور التكنولوجي وما نتج عنه من جرائم الإلكترونية، واقد واكبت أغلب التشريعات القانونية في الدول المتطورة تشريعاتها القانونية على نطاق قانون العقوبات وقانون الإجراءات لمكافحة هذه الجرائم الإلكترونية، ونجد أن أسلوب التحقيق قد ارتقى من خلال إستخدامه لأساليب وطرق حديثة ومتطورة من خلال متابعة المجرم والجريمة، وأيضا من خلال كشف ملابسات الجرائم الإلكترونية، وعلى ضوء ذلك سنقسم دراستنا في هذا الفصل إلى مبحثين، نخصص المبحث الأول لدراسة مظاهر تأثير التطور التكنولوجي على مرحلة التحقيق الابتدائي، أما المبحث الثاني فسيكون لدراسة مظاهر تأثير التطور التكنولوجي على مرحلة المحاكمة.

المبحث الاول

مظاهر تأثير التطور التكنولوجي على مرحلة التحقيق الابتدائي

يعتمد التنظيم القانوني في الدول الديمقراطية على الموازنة بين مصلحة الفرد من جهة ومصلحة المجتمع من جهة أخرى، إذ يقع على عاتق المشرع أن يحقق هذا التوازن، عند تشريع القوانين، فالمشرع الجنائي يحاول أن يواكب التطور التكنولوجي والتقني الذي يعيشه العالم بصورة عامة، والمجتمع المحلي بصورة خاصة، لكي يقدم الحلول الناجعة لمكافحة إنتشار الجرائم، فقد أدى التطور التكنولوجي إلى تطور الجرائم من جرائم ترتكب بصورة وأساليب تقليدية، إلى جرائم إلكترونية،

ترتكب بسهولة وسرعة ومن دون الحاجة لبذل جهد بدني، فالجرائم الإلكترونية لا تحتاج سوى أمتلاك جهاز حاسوب أو جهاز تقني صغير مرتبط بالإنترنت، بالإضافة إلى أن ما يميز الجرائم الإلكترونية أنها تُعد من الجرائم العابرة للحدود ، وهذه الميزة هي أحد أكبر الإشكاليات التي تواجه المشرعين الجنائيين سواء على صعيد إجراء التحقيق والتتبع أم على صعيد تطبيق القانون وإجراء المحاكمة. وعلى ضوء ذلك سنقسم هذا الموضوع إلى مطلبين، نخصص المطلب الاول لدراسة مراقبة المتهم والتحقيق في الجريمة الإلكترونية، أما المطلب الثاني سيكون لبحث موضوع الوسائل التقنية الناتجة عن التطور التكنولوجي في مجال السمعيات والمرئيات.

المطلب الأول

مراقبة المتهم والتحقيق في الجريمة الإلكترونية

تظهر أهمية موضوع المراقبة للمتهم، وذلك لتحقيق الهدف المرجو وهو كشف غموض الجريمة ومعرفة هوية المتهم، فبسبب الغموض الذي يحيط بكل جريمة بصورة عامة والجرائم الإلكترونية بصفة خاصة، بسبب تعدد الإسباب والدوافع لإرتكاب الجريمة، فعملية المراقبة تهدف لكشف الحقيقة وتوقيع العقاب على من يستحق بعد إدانته بالأدلة التي يتم إستخلاصها بإحدى طرق المراقبة، وعلى ضوء ذلك سنحاول بيان مفهوم المراقبة في الفرع الاول، ونخصص الفرع الثاني لبحث آليات تطبيق المراقبة الإلكترونية اثناء التحقيق.

الفرع الأول

مفهوم المراقبة والتحقيق في الجرائم الإلكترونية

أولا : التعريف بالمراقبة :

مصطلح المراقبة جاء في الأغلب ضمن الكتب والبحوث التي تتحدث عن العلوم القانونية والادارية والمالية، وهذا ما أدى إلى الإختلاف في بيان تعريفها، والسبب هو تباين نظرة كل كاتب، إذ تختلف نظرة بعضهم لمفهوم المراقبة من زاوية تختلف عن الاخر، فبعضهم يرى أن مفهوم المراقبة على أساس ما تسعى إليه من تحقيق الاهداف[1]، وجانب آخر عرف المراقبة: هي مجموعة من الإجراءات والعمليات لتقويم عمل ما كالهيئات التشريعية[2]، أما تعريف المراقبة في مصطلح أهل القانون، تعرف المراقبة على أنها: هي مجموعة من الاجراءات لجمع المعلومات من قبل رجال البحث

(1) - د. مصطفى محمد موسى، المراقبة الإلكترونية عبر شبكة الإنترنت، الطبعة الاولى، بدون دار نشر، 2003، ص 192.

(2) - د. عبدالمهيمن بكر، إجراءات الادلة الجنائية اثناء التفتيش، الطبعة الاولى، 1996، ص 306 .

الجنائي، أو هي إحدى أساليب وطرق البحث للحصول على المعلومات من مصدرها المعني بالتحقيق، قد يكون شخصاً أو مكاناً معنياً بالمراقبة بطريقة سرية[1]. ومنهم من عرفها بانها: عمل أمني له نظام معلوماتي إلكتروني يقوم على التقنية الإلكترونية إذ يتولى المراقب عن طريق الأجهزة الإلكترونية، عبر شبكة الإنترنت باستخدام البرمجيات الإلكترونية وذلك لتحقيق غرض محدد ونتيجة محددة[2].

ثانيا : التعريف بالتحقيق الإلكتروني

يقسم الفقه التحقيق إلى مرحلتين، تحقيق سابق، وتحقيق لاحق، فالتحقيق السابق أو الإحترازي فهي عملية إجراء تحقيق من السلطات المختصة على فرد أو مجموعة أفراد قد يكونون ذوي صلة بنمط إجرامي موجود في تلك الفترة، مثل التحقيقات التي تجريها الشرطة على مقرات العصابات أو غيرهم ممن تشك بكونهم ذوي سلوك إجرامي قد يتسبب بخطر على المجتمع، فأن هذا التحقيق هو بمثابة تدبير احترازي وضبط، تقوم به السلطات للعثور على أسلحة أو ما إلى ذلك، أما التحقيق اللاحق فهو إستجابة الشرطة لجريمة إرتكبت وذلك من خلال التحقيق بمشهد الحادث بعد إرتكاب الجريمة، وذلك بعد التبليغ عن الجرائم المتمثلة بالسرقة، أو الإغتصاب أو الإغتيال من قبل الضحية أو الأفراد أو غيرهم من قد يتواجد في محل الحادث لسلطات التحقيق أو الشرطة[1].

هذا ومن الجدير بالذكر أن الفقه الأمريكي وضع [2] تعريفات متعددة ومتنوعة للتحقيقات الجنائية منها "مفهوم وإجراءات في نظام العدالة الجنائية" وبعضهم عرفه "إعادة بناء أحداث قد وقعت بالفعل وذلك لمعرفة مرتكب الجريمة" وبعضهم عرفها "هي عملية جمع المعلومات والمعارف الضرورية لمعرفة سلوك الجاني وقت أرتكب الجريمة، وسلوك المجرم بعد ارتكاب الجريمة، ومعرفة الأسباب التي دفعته لإرتكاب الجريمة" وبعضهم عرفها بانها "إجراءات يحدد من خلالها من إرتكاب الجريمة وما الأدلة المتوفرة ضده". ومن خلال هذه التعاريف السابقة يمكن تحديد العناصر التي تمثل التحقيق وهي: جمع المعلومات، وتحديد الشخص المسؤول عن إرتكاب الجريمة، معالجة وتحليل المعلومات المتحصلة عن الجريمة، وبالإضافة إلى الكشف عن الجريمة. وجميع هذه المسائل السابقة تسمح

(1) - د. حيدر كاظم الطائي، المراقبة كإحدى طرق البحث الجنائي، بحث منشور، مجلة القانون للدراسات والبحوث القانونية، العدد التاسع عشر، 2019، ص 82 و 83.

(2) - د. اكرم سلام عبدالرؤوف سلام، المصدر السابق، ص 90 . وكذلك: خالد مشتهى، الجرائم الالكترونية المؤثرة على امن الدولة، رسالة ماجستير، جامعة جندوبة، كلية العلوم القانونية والاقتصادية، تونس، 2021، ص76.

(1)- Daniel A. Reilly, Finding the Truth with Criminal Investigation: Suspect, Subject, Defendant, Rowman & Littlefield Publishers August 15, 2019.

(2)- The editors of Britannica, Criminal Investigation, Britannica, the link: ((https://www.britannica.com/topic/criminal-investigation)), Accessed at ((23-05-2022)).

بإعادة بناء الحدث وتكوين صورة واضحة محل الحدث، وكنتيجة منطقية لذلك تساعد الشرطة بالوصول لمرتكبي الجريمة وكيفية إرتكابها وكيف ترك مرتكبي الجريمة موقع الحدث، وكيف أخفوا بعضاً من الأدلة [1]. ويعرف التحقيق أيضاً بانه عملية البحث المنهجي عن الحقائق، وأن أصل المفردة الانكليزية (investigation) يعود لمفرد في اللغة اللاتينية وهي (vestigere) والتي تعني مفردة التحقيق بها تعقب، وهي عملية بحث عن الحقائق تسعى من خلالها السلطات إلى أن تجمع المعلومات المتعلقة بالجريمة، ومن خصائص التحقيق هي ما يأتي:

1- إن التحقيق يشبه البحث العلمي، فهو قائم على جمع أقصى قدر ممكن من الحقائق.

2- إن الأهتمام به يتعدى نطاق القانون فتوجد مجالات عدة تهتم في التحقيق ومنها أقسام تكنولوجيا المواصلات والعلوم.

3- يتطلب التحقيق من المحقق أن يهتم لأدق التفاصيل، وذلك كل تفصيل قد يسهم في الكشف عن الحقائق.

4- يجب أن يكون الشخص المختص بالتحقيق ملائماً لعملية التحقيق، فالشرطي الذي يختص بمطاردة المجرمين لا يكون ملائماً لملاحظة الدلائل ومناقشة واستجواب بل يجب ان يقوم بذلك محقق[1].

أما بالنسبة للمشرع الأمريكي فلم يتناول معوقات التحقيق الجنائي رقم (18 /1510) ولم يعرف التحقيق الجنائي في الولايات المتحدة الأمريكية، ولكنه عرف المحقق الجنائي بما يأتي:

يستخدم مصطلح المحقق الجنائي للإشارة لأي فرد في أي قسم أو في أي قوات مسلحة أو في أي وكالة حكومية للقيام بالتحقيقات، للتحقيق في الإنتهاكات الحاصلة لقانون الجنائي للولايات المتحدة الأمريكية.

وتجدر بالإشارة إلى أن من العيوب التي قد تصيب التحقيق هي تلك الحالات التي قد تنشغل بها الشرطة في التحري وتحليل البيانات التي لديها، مع السعي لإيجاد الضحايا في بعض الحالات، بهذا قد تنشغل الشرطة في السعي لإيجاد الضحايا والبحث عن موقعهم عوضاً عن السعي لإيجاد مرتكبي

(1)- K. S. Dharmasiri, K.G.N.U Rannaweera, Anuruddhika Buddhadasa, K.B.N and De Silva, Criminal Investigation: A Brief Review of Importance of Biological Evidence, European Scholar Journal (ESJ), Vol. 2 No. 8, 2021.

(1)- Whitney D. Gunter and Christopher A. Hertig, an Introduction to Theory, Practice and Career Development for Public and Private Investigators, International Foundation for Protection Officers, 2005.

الجريمة، ومن المسائل التي تؤثر على أكمال التحقيق، البطء بالإجراءات الروتينية، وان تلك الحالات التي لا تسجل فيها الشرطة أو الجهات المسؤولة عن التحقيق الأدلة فتقل فرص إيجاد الجناة بشكل كبير جداً، فكلما قل تسجيل الادلة التي تم العثور عليها في مقر الحادث تقل فرص إيجاد الجناة بشكل كبير جداً[1].

ومن العوامل التي تساعد المحققين في حل الجرائم وكشف الحقيقة، هي البيانات التي يقدمها الضحايا، فلو قدم المجنى عليه المعلومات اللازمة، فإنه سيمكن الشرطة من إيجاد الجاني بشكل أكبر، ومن العوامل التي تساعد عملية التحقيق هي تطوير المحققين لقدراتهم التحليلية والتدريب على زيادة قدراتهم الإدراكية، وأختيار الأشخاص الذين لديهم القدرة على التحليل، وقدرة على الإنتباه بشكل أفضل لأدلة الجرائم، وبالإضافة لعدم دخول العامة لموقع الحادث لأن دخول العامة لموقع الحادث قد يسهم في ضياع العديد من الادلة، والمسألة ذاتها تنطبق على الجرائم الإلكترونية فدخول العامة لمواقع الجريمة قد يسبب في ضياع الأدلة أو اندثارها مثل تلك الحالات التي تسرق فيها الأجهزة أو تضيع فيها بصمات أصابع الجاني، أو المجنى عليه في موقع الحادث، من العيوب الأخرى التي قد تلحق التحقيق هي القناعات المسبقة للقضاة، أو عدم تفتح ذهن المحقق على احتمالات أخرى غير تلك المطروحة أمامه أو ضعف أدلة التحقيق، ضعف التدريب الذي يخضع له المحققين كلها عوامل تسهم في ضعف نتائج التحقيق[1].

وتُعد أعمال الاستدلال من صميم عمل وسلطة أعضاء الضبط القضائي إستناداً إلى القانون، إذ يتولى أعضاء الضبط القضائي البحث والإستقصاء عن الجرائم ومرتكبيها وجمع الإستدلالات اللازمة للتحقيق في الدعوى بغية الوصول إلى معالم الجريمة والمتهم، وكذلك من واجبات أعضاء الضبط القضائي قبول التبليغات والتي تتمثل في الأخبار عن الجرائم، والتبليغ هو إيصال خبر الجريمة إلى السلطات وقد يكون من مصدراً، مجهولاً، أو معلومة، أو شفاهية، أو كتابة، ومن مهام أعضاء الضبط القضائي واجب تلقي الأخبار والشكاوى عن الجرائم الإلكترونية وغيرها وكذلك على أعضاء الضبط القضائي تدوين جميع الأعمال التي يقومون بها عند الانتقال إلى مسرح الجريمة في محضر موقع عليها منهم يبين فيها ساعة وتاريخ ومكان حدوث الجريمة، وبالإضافة إلى ذلك فإن على أعضاء

(1)- Peter W. greenwood & Joan Petersilia, the Criminal Investgeation Process Voulume Summary and Policy Implications, Rand Institution, 1975, page 30-35.

(1)- Dr Amber McKinley, Criminal Investigative Failures, Volume 6, Number 1, 2018, page 83.

الضبط القضائي إجراء التحقيق الابتدائي والإستماع والإستجواب لأي شخص متهم أو أي شخص يظن أن لديه معلومات عن وقائع أو ظروف الجريمة التي حدثت[1].

أما الإجراءات الواجب اتخاذها للكشف عن الجريمة الإلكترونية هي، الدقة في اختيار العاملين في مجال البحث الجنائي والتركيز على من تتوفر فيهم الصفات المهنية والأخلاقية، وكذلك الاهتمام بمسرح الجريمة، و ضرورة سرعة الإنتقال له بما يحقق المحافظة على المكان بالوضع الذي تركه الجاني لإمكانية الاستفادة من الآثار المادية والمعنوية في الحيز الافتراضي للجريمة الإلكترونية. وأيضاً مراعاة التنسيق الهادف بين جهة التحقيق والبحث الجنائي و خبراء الأدلة الجنائية وتنظيم عملية دخول الخبراء إلى مسرح الحادث حسب رؤية المحقق وبالشكل الذي يكفل عدم ضياع معالم الحادث، وتوفير الأجهزة الحديثة الفنية والتقنية وإيجاد خبراء متخصصين لفحص جميع الآثار التي تركها المجرم بمسرح الجريمة[1].

الفرع الثاني

طرق وآلية تطبيق المراقبة الإلكترونية أثناء التحقيق

تتسم الجريمة الإلكترونية بحداثة أساليب إرتكابها، وسرعة تنفيذها، وسهولة إخفائها ودقة محو آثارها. وعلى هذا الأساس فإن الأمر يتطلب أن تكون جهات التحري والتحقيق بل والمحاكمة على درجة كبيرة من المعرفة بأنظمة الحاسب الآلي، وقد وجدت أجهزة الشرطة والتحقيق صعوبات جمة منذ ظهور هذه النوع المستحدث من الجرائم، سواء في كشف غموضها أو إجراء التفتيش والضبط[2]، أو التحقيق فيها على نحو يتوجب إعداد برامج تدريب وتأهيل لهذه الكوادر من الناحية الفنية على نحو يمكنها من تحقيق المهمة المطلوبة منها وعليه فإنه أساليب التحري أو التحقيق التقليدية قد لا تصلح لكشف هذا النوع من الجرائم الإلكترونية وهذا الأمر يتطلب تدخل المشرع الجنائي لتعديل قواعد قانون الإجراءات الجنائية وإستحداث قواعد إجرائية خاصة تتناسب والطبيعة المميزة للجرائم الإلكترونية[3].

وإن أسلوب إرتكاب الجريمة الإلكترونية يختلف اختلافاً كبيراً عن أسلوب إرتكاب الجرائم التقليدية، كذلك فإن الضرر الناتج عن الجرائم الإلكترونية لا يمكن الإستهانة به، فالتحقيق في الجرائم

(1) - د. محمود رجب فتح الله ، مسرح الجريمة الإلكترونية المصدر السابق ، ص 427.

(1) - محمد حمدان عاشور، أساليب التحقيق والبحث الجنائي، أكاديمية فلسطين للعلوم الامنية، 2010، ص50.

(2) - د. مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، مطابع الشرطة، القاهرة، 2009، ص208.

(3) - د. خالد حسن أحمد لطفي، آليات التحقيق الجنائي في جرائم تقنية المعلومات، دار الفكر الجامعي، الاسكندرية، 2020 ، ص 39 وما بعدها.

الإلكترونية هو عبارة عن فحص أجهزة الحاسب الآلي للجاني أو أي شخص له علاقة بالجريمة، فعملية التحقيق في الجريمة الإلكترونية ليست مقتصرة على الأجهزة الإلكترونية، بل من الممكن أن تكون أيضا عملية تتبع لبعض الأدلة والأمور التي أجراها الجاني أثناء عملية الاختراق أو بعد عملية الاختراق، فالتحقيق في مثل هذه الجرائم يتطلب تحليل الملفات والبيانات الإلكترونية والحركات التي قام بها المجرم، وعلى ضوء ذلك فعملية التحري والتحقيق في الجرائم الإلكترونية تتطلب فريق من أعضاء الضبط القضائي يمتلكون من المهارة والخبرة الكافية لغرض كشف خيوط الجريمة والوصول إلى مرتكبيها من خلال الإستعانة بذوي الخبرة وكذلك بأجهزة تقنية وبرامج متطورة لكشف الحقيقة[1].

ففي ظل التطور التكنولوجي والتقني الحاصل، فقد أصبح من الضروري أن يكون هناك نصيب من هذا التطور التقني، لتطبيق أسلوب المراقبة أثناء البحث والتحقيق من قبل أعضاء الضبط القضائي، أو من قبل أي شخص مكلف قانونا للقيام بالمراقبة، من خلال استخدام وتسخير التكنولوجيا الحديثة في مجال المراقبة الالكترونية[2]، وإذ إن الطابع العام للجرائم الالكترونية هي أنها ترتكب من قبل منظمات إجرامية تستهدف الحكومات، أو بعض فئات المجتمع أو الأعمال التجارية، للحصول على أموال أو بضائع. فالهدف الأساسي هو الربح المالي، لكن قد يكون كذلك هدفه الإضرار بالغير، وإن الأموال التي قد يتحصل عليها المجرمون من هذه الجرائم قد تستخدم في مشاريع أخرى إجرامية أو غير إجرامية. إن ممارسي هذا النشاط الإلكتروني هم أشخاص متمرسين والذين ينتظمون بمجاميع إجرامية رقمية، يلتقون بشبكات رقمية الكترونية سواء كان موقعاً أم قناة على الإنترنيت، ونادرا ما يحصل لقاء فيما بينهم مما يجعل مراقبتهم على أرض الواقع صعبة. يستخدمون مواقع إلكترونية محمية للتخلص من تتبع الحكومة لهم ولا يمنحون مواقعهم الإلكترونية إلاّ لمن يثقون بهم من الأشخاص، هذا العامل الأخير يجعل من تتبعهم صعب في المواقع الإلكترونية[3].

ولمعرفة كيفية التتبع والمراقبة على حواسيب المجرمين فيجب علينا أن نعرف أي الحواسيب التي تستحق التعقب والمتابعة في الجرائم، تسمى هذه الحواسيب في القانون الأمريكي المعني بالحواسيب المحمية، وليس لهذا المصطلح أي علاقة بحماية الحاسوب، ان مصطلح الحاسوب المحمي يشير للحاسوب الذي يستخدم للتأثير بشكل سلبي على التجارة بين الولايات أو التجارة الأجنبية أو للتأثير

(1) - د. منى كامل تركي، التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، الاسكندرية، 2009، ص182 .

(2) - رشاد خالد عمر، المشاكل القانونية للتحقيق في الجرائم المعلوماتية، المصدر السابق ، ص 181.

(3)- Secretary of State for the Home Department, Cyber Crime Strategy, 2010, the United Kingdom, page 25.

على الحواسيب الحكومية، وقد صنف القانون الأمريكي هذه الحواسيب على نوعين، منها الحاسوب الذي يستخدم بشكل حصري من المؤسسات المالية أو الحكومة الأمريكية أو لا تستخدم بشكل حصري من المؤسسات المالية أو الحكومة الأمريكية واستخدام بطريقة تشكل جريمة تؤثر على المؤسسات المالية أو الحكومية. وكذلك الحواسيب التي تؤثر على التجارة بين الولايات.....[1]

فالضبط في الجرائم الإلكترونية هو ضبط الأشياء التي تتعلق بالجريمة والتي تفيد في التحقيق الجاري بشأنها سواء كانت هذه الأشياء ادوات استعملت في ارتكاب الجريمة أم أشياء تنتج عنها أو غير ذلك مما يفيد في كشف الحقيقة. وإذ أننا بصدد التحري والتحقيق بالجرائم الإلكترونية فإننا أمام نوعين من المكونات التي يمكن ضبطها من قبل المحققين النوع الاول: المكونات المادية لا يشكل الأمر فيها أي خلاف فقهي فجميع الأجزاء التي تتصل بالحاسب الآلي تستحق أن يكون موضوعاً للضبط. أما النوع الثاني مكونات غير مادية وهي البيانات التي تتواجد داخل جهاز الحاسب الالي أو التي توجد في الشبكة العنكبوتية العالمية[1].

أما في فرنسا فقد كرس المشرع الجنائي الفرنسي مجموعة من القوانين تضمنت آلية المراقبة الالكترونية، وأهمها قانون الثقة في الاقتصاد الرقمي رقم (575) لسنة 2004، اذ تضمن الفصل الاول منه النص على حرية الإتصالات الإلكترونية ولا يجوز تقييدها إلاّ في إطار أحترام كرامة الانسان وحرية الاخرين، وكذلك جاء في الفصل السادس من ذات القانون الفقرة الأولى سابعا، والتي تتيح إجراء المراقبة الإلكترونية أثناء التحقيق في الجرائم الإلكترونية، بعد طلب من السلطة القضائية لحساب المصلحة العامة، وكل فعل يمثل إنتهاكاً للخصوصية أو الجرائم الجنسية أو إنتهاك لكرامة الإنسان[2].

أما المشرع الجنائي الأمريكي فإنه وضع شرطا لإجراء التحقيق والمراقبة الإلكترونية، ويتمثل هذا الشرط بوجود أي دليل بأن الحاسوب قد إستخدم للوصول إلى الإنترنيت أو إستخدم الإنترنيت للوصول للحاسوب، فمجرد تأثير الحاسوب بشكل سلبي على التجارة بين الولايات يعد كافياً لتحقق هذا الشرط، أي أن تحقق شرط تأثير التجارة على الولايات هو شرط جوهري من أجل تتبع حاسوب الشخص مرتكب الجريمة من قبل الشرطة الأمريكية[3].

---

(1)- Computer Fraud and Abuse Act 18 U.S.C. § 1030.

(1) - د. خالد حسن أحمد لطفي، آليات التحقيق الجنائي في جرائم تقنية المعلومات، المصدر السابق ، ص 74.

(2) - خالد مشتهى، الجرائم الالكترونية المؤثرة على امن الدولة، المصدر السابق، ص 80.

(3)- H. Marshall Jarrett & Michael W. Bailie, Op.Cit, Page 4.

وقد بينت أغلب المحاكم من أن توفر عنصر إستخدام الإنترنيت يُعدّ كافياً لإعتبار الحاسوب محمياً وتوافر (أي العناصر التي ذكرت في الفقرة الفرعية (t) من قانون الإحتيال الإلكتروني وإساءة إستخدام الحاسوب المرقم **18 U.S.code&1030**) وذكر ذلك في قضية، United States v. Drew[1] في العام 2009 ان الجريمة الرقمية تتحقق حينما يتم الحصول على معلومات من حاسوب محمي، وحينما يستخدم الفرد حاسوباً للإتصال أو للتواصل مع الإنترنيت وذلك ما ذكر في قضية أمام محكمة الدائرة الثامنة في العام 2007. وأما في قضية United States v. Trotter[1]، قد ذكر (لا حاجة لإقامة الدليل على وجود قناة تواصل بين الولايات حينما تتعلق الجريمة بالتجارة بين الولايات). وفي قضية أخرى فقد ذكر **Paradigm Alliance, Inc. v. Celeritas Technologies** (أن توفر حاسوب متصل بالأنترنيت لن يكفي لتحقق شرط التجارة بين الولايات)[2].

اما اسلوب التحري والتحقيق من قبل أعضاء الضبط القضائي، فقد نجد أن بعض التشريعات أعطت سلطة تقديرية لأعضاء الضبط القضائي في أختيار أسلوب إجراء التحري بالطريقة التي يراها مناسبة لإتمام عمله بصورة إيجابية وفي إطار الشرعية ودون المساس في حرمة الحياة الخاصة فتتعدد صور إجراء التحريات، فقد تتم عن طريق إجراء مقابلات استطلاعية مع ممثلي جهة المجنى عليه بهدف استقصاء الحقائق حول الجريمة الإلكترونية للحصول على أكبر قدر ممكن من المعلومات عن السلوك الإجرامي المكون لها، كما قد يتخذ البحث والتحري عن الجريمة الإلكترونية صورة المراقبة الإلكترونية عبر الإنترنت والتي تُعد أحد الركائز الأساسية التي يستند عليها رجال البحث والتحري لجمع المعلومات والإستدلالات حول الجرائم الإلكترونية[3].

أما (المشرع المصري) فقد نظم بمقتضى المادة (5) من قانون مكافحة جرائم تقنية المعلومات، بشأن مسرح الجريمة الإلكترونية ومدى السلطة الممنوحة لأعضاء الضبط القضائي، فقد أجاز القانون بقرار من وزير العدل بالإتفاق مع الوزير المختص منح صفة الضبطية القضائية للعاملين بالجهاز أو غيرهم ممن تحددهم جهات الأمن القومي، فيما يخص الجرائم التي ترتكب بالمخالفة لأحكام هذا القانون، وأيضاً فقد نظمت المادة (6) من القانون ذاته سلطات الضبط القضائي، ومنحهم سلطة

---

(1)- United States v. Drew, 259 F.R.D. 449, 457.

(1)- United States v. Trotter, 478 F.3d 918, 921 (8th Cir. 2007).

(2)- Paradigm Alliance, Inc. v. Celeritas Technologies, LLC, 248 F.R.D. 598, 602, 2008.

(3) - د. محمد كمال شاهين، الجوانب الاجرائية للجريمة الالكترونية في مرحلة التحقيق الابتدائي، المصدر السابق، ص 250.

الدخول والنفاذ إلى برامج الحاسب الآلي وقواعد البيانات وغيرها، وكذلك إصدار أمر لمقدمي الخدمة (الإنترنت والإتصالات) بتسليم ما لديهم من بيانات ومعلومات تفيد التحقيق[1].

أما (المشرع الجنائي العراقي) فقد تطرق لموضوع المراقبة من خلال قانون أصول المحاكمات الجزائية رقم (23) لسنة 1971 المعدل، فجاء بنص المادة (41) منه على أنه: (أعضاء الضبط القضائي مكلفون في جهات اختصاصهم بالتحري عن الجرائم .....وعليهم تقديم المساعدة لقاضي التحقيق والمحققين وضباط الشرطة ومفوضيها وتزويدهم بما يصل اليهم من معلومات عن الجرائم....). ومن خلال هذا النص نلاحظ أن المشرع العراقي أورد إطلاق الحرية أمام أعضاء الضبط القضائي في إجراء المراقبة والتحري عن أي جريمة وملاحقة مرتكبيها، وأيضا نلاحظ أن المشرع العراقي لم يقيد ويحدد طرق المراقبة، وإنما أطلقها ، إذ جاء بنص المادة (42) من ذات القانون عبارة (على أعضاء الضبط القضائي أن يتخذوا جميع الوسائل....). وهذا ما يحسب إيجابا للمشرع العراقي لأنه وسع من مفهوم المراقبة ووسائل تنفيذها، وهذا ما ينطبق في حال تم إستخدام وسائل التطور التكنولوجي الحديثة في مجال المراقبة .

أولا : مرحلة التحري وجمع الأدلة في الجرائم الإلكترونية :

إن إجراءات جمع الإستدلالات من الإجراءات التي تسبق التحقيق ورفع الدعوى الجزائية والتي يختص بها أعضاء الضبط القضائي والتي يكون المدعي العام مشرفاً عن أعمالهم، إذ يحق للنائب العام (المدعي العام) الأشراف على أعمال أعضاء الضبط القضائي ويلاحظ أن إجراءات جمع الإستدلالات تشمل عملية البحث والتحري حول الجريمة والتمهيد للتحقيق فيها للبدء في عملية التحقيق التي تختص بها المحكمة المختصة[1]. ويعرف الإستدلال بأنه: تلك المرحلة التي يتم فيها جمع المعلومات عن الجريمة والبحث عن مرتكبيها عن طريق الأساليب القانونية، إذ يجوز لأعضاء الضبط القضائي جمع المعلومات عن الجريمة الإلكترونية باي طريقة قانونية[2]. ومن مهام أعضاء الضبط القضائي في التحقيق في الجريمة الإلكترونية، تلقي البلاغات والشكاوى والتحري عنها وعادة ما تبقى الجريمة غامضة حتى يصل خبرها إلى السلطات المختصة، وهذا الوضع ينطبق على الجرائم كافة دون إستثناء، لكن يتجلى بوضوح بالنسبة للجرائم التقنية والإلكترونية نظراً إلى طبيعتها إذ يصعب على الأشخاص العاديين الإبلاغ عنها لما تطلبه من مهارات فنية غير متوافرة سوى لفئات

(1) - د. محمود رجب فتح الله، مسرح الجريمة الالكترونية، المصدر السابق، ص 427.

(1) - د. عمر محمد ابو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، دار النهضة العربية، 2004 ، ص882.

(2) - د. محمد كمال شاهين، الجوانب الاجرائية للجريمة الالكترونية في مرحلة التحقيق الابتدائي، المصدر السابق، ص 237.

مهنية أو تخصصية في مجال الحاسب الآلي، وفي الأحوال جميعها فإن أي إخبار عن جريمة سواء كان فاعلها مجهولا أم معلوما، ينبغي أن يتضمن على الأقل معلومات أوليه عن الجريمة مثل تحديد محل الجريمة ومكان وقوعها ونوعها اذ تُعد هذه العناصر مهمة وضرورية لرجال الضبط القضائي في أي أخبار متعلق بالجرائم الإلكترونية، ويتم الكشف عن الجرائم إلكترونية بوضع برمجيات حاسوبيا معينة خصوصا فيما يتعلق بجرائم القرصنة أو نشر المواد الإباحية أو جرائم التهديد أو الإبتزاز وغيرها، وكذلك من مهام أعضاء الضبط القضائي أو الجهاز المكلف بالتحري والتحقيق في الجرائم الإلكترونية هو معاينة مسرح الجريمة و سبق وأن تكلمنا عن هذا الموضوع في الفصل الأول من هذا الباب[1].

ثانيا : مرحلة التحقيق الإبتدائي في الجرائم الإلكترونية :

تعد مرحلة التحقيق الإبتدائي هي المرحلة الأولى من مراحل سير الدعوى الجزائية بل وأخطرها والأكثر مساساً بحرمة الحياة الخاصة، فالتحقيق الإبتدائي ينصرف إلى مجموعة الإجراءات التي تجريها سلطات التحقيق قبل إجراء المحاكمة، وأيضا يعرف التحقيق الإبتدائي بأنه: مجموعة من الإجراءات التي تباشرها السلطات المختصة بالتحقيق في الدعوى عن جريمة إرتكبت لكشف الحقيقة، وذلك بالبحث والتنقيب عن أدله وتجميعها وتقديرها لإثبات حدوث الجريمة ونسبتها إلى المتهم لتحديد مدى كفايتها لإحالة المتهم للمحكمة أو لنفي الاتهام كأساس للأمر من بالأوجه لإقامة الدعوى[2]. فمرحلة التحقيق الابتدائي من شأنها البحث وتدقيق الأدلة وجمعها وإستظهار قيمتها وإستبعاد الأدلة الضعيفة وإستخلاص رأي مبدئي بشأنها، ومن ثم تستطيع المحكمة أن تنظر الدعوى وقد أتضحت عناصرها وتكشفت ملامحها وهذا ما يساعد في كشف الحقيقة وتحقيق العدالة[3]. ومن ثم فمرحلة التحقيق الإبتدائي لها أهمية بالغة في تحقيق المصلحة العامة وأيضاً بإعتبارها ضمانة للحرية الشخصية، ومن الضمانات التي يتميز بها التحقيق الإبتدائي كإجراء لضمان حرمة الحياة الخاصة بصفة عامة، وضمان الحق في الخصوصية المعلوماتية للأفراد في الجريمة الإلكترونية بصفة خاصة، وذلك بغض النظر عن القائم بها والتي تتمثل أهم تلك الضمانات هي: تدوين التحقيق والذي

(1) - د. خالد حسن أحمد لطفي ، آليات التحقيق الجنائي في جرائم تقنية المعلومات ،المصدر السابق، ص 40.
(2) - د. محمد كمال شاهين، الجوانب الاجرائية للجريمة الالكترونية في مرحلة التحقيق الابتدائي ، المصدر السابق، ص 168.
(3) - خالد عياد الحربي إجراءات التحري والتحقيق في جرائم الحاسوب الإنترنت، المصدر السابق، ص191.

يهدف إلى ضرورة أن تكون إجراءات التحقيق بالكتابة في محضر يعد لهذا الأمر بالإضافة إلى سرية التحقيق الإبتدائي وهذا ما قررته أغلب التشريعات المقارنة[1].

فالتحقيق الإبتدائي هو أول مرحلة من مراحل الدعوى الجزائية وهو عبارة عن إجراءات تتخذها السلطات من أجل تمحيص الأدلة التي أسفرت عنها مرحلة جمع الإستدلالات مع محاولة جمع الأدلة جديدة تساعد في التحقيق للكشف عن الجريمة التي وقعت، ولخصوصية الجريمة الإلكترونية فإن الأمر يتطلب أن يتم تطوير أساليب التحقيق الجنائي وإجراءاتها بصورة تتلاءم مع هذه الخصوصية ومن إجراءات التحقيق الإبتدائي في الجريمة الإلكترونية هو التفتيش في الجريمة الالكترونية وأجهزة الحاسب الالي، وسبق أن تكلمنا عن هذا الموضوع في الفصل الأول من هذا الباب[1]. ومن مهام أعضاء الضبط القضائي، أو الجهاز المكلف بالتحقيق في الجرائم إلكترونية سماع أقوال الشهود والمشتبه بهم ومن النادر جداً ما نجد شاهداً على وقائع جريمة الكترونية وذلك لعدة أسباب منها: أن الجرائم المعلوماتية تتطلب دراية كافية بالجوانب الفنية والتقنية للحاسب الآلي، وكذلك الجرائم الإلكترونية ترتكب في هدوء أي أن الجاني يرتكبها وحده دون وجود أحد معه، بالإضافة إلى أن الجرائم الإلكترونية لا تترك آثاراً خارجية يشهد بها أحد كما هو الحال في الجرائم التقليدية، ويعد كذلك من الاجراءات التي يقوم بها أعضاء الضبط القضائي هو سماع أقوال المشتبه بهم، ويقتصر هذا الإجراء بإعلام المشتبه بهم بالتهم المنسوبة إليهم ومجمل الأدلة الموجه ضدهم دون مناقشة تفاصيلها في الواقعة[2]. وكذلك على أعضاء الضبط القضائي واللجنة المكلفة بالتحري والتحقيق في الجرائم الإلكترونية الإستعانة بالخبراء فعلى سلطات التحقيق أو المحقق أو المحكمة، الاستعانة بأصحاب الخبرة الفنية المتميزة في مجال الحاسب الآلي، وذلك بغرض الكشف عن غموض الجريمة وجمع الأدلة والتحفظ عليها أو مساعدة المحقق في كشف الغموض في العمليات الإلكترونية الدقيقة[3]. وبناء على ذلك فإذا كانت الإستعانة بخبير فني في المسائل الفنية البحتة أمراً واجباً على جهة التحقيق أو القاضي فهي أوجب في مجال الجرائم الإلكترونية، ونجد أن المشرع المصري قد جاء بنص المادة (10) من قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 إذ نظم عملية الإستعانة بالخبراء إذ تضمنت إنشاء سجلات في الجهاز القومي لتنظيم الإتصالات لقيد الخبراء يقيد بأولهما الفنيون والتقنيون العاملون به، و يقيد في الأخر الخبراء من الفنيين والتقنيين من غير العاملين

(1) - محمود نجيب حسني، شرح قانون الاجراءات الجنائية، دار النهضة ، 1998، ص 614.
(1) - د. خالد حسن أحمد لطفي، آليات التحقيق الجنائي في جرائم تقنية المعلومات ، المصدر السابق، ص 58.
(2) - د. محمود رجب فتح الله، مسرح الجريمة الالكترونية، المصدر السابق، ص 476.
(3) - د. عبدالفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، الاسكندرية، 2006، ص 138.

بالجهاز، وعلى أعضاء الضبط القضائي و اللجنة المكلفة في التحقيق في الجرائم الإلكترونية من واجباتهم التحفظ على أدوات الجريمة بمعنى يجب على أعضاء الضبط القضائي عند الانتقال لمسرح الجريمة أن يقوموا بضبط كل ما يتعلق بموضوع الجريمة ويفيد في كشف الحقيقة سواء كانت الأشياء المضبوطة تعود للمتهم أم لغيره، ولا يهم نوعها أو طبيعتها، فهنالك كيانات مادية إلكترونية وأيضا هنالك كيانات معنوية إلكترونية، ويلاحظ أن هذا النوع من الضبط يشكل صعوبة لدى أعضاء الضبط القضائي وذلك لصعوبة ضبط البيانات المعنوية للأجهزة الالكترونية وعدم وجود الخبرة الكافية لأعضاء الضبط القضائي في مثل هذه الامور فيجب عليهم الإستعانة بأصحاب الخبرة عند ضبط المواد الإلكترونية التي تستخدم دليلا في الواقعة[1].

وتبدأ إجراءات البحث والتحري في الجريمة الإلكترونية من قبل أعضاء الضبط القضائي متى أتصل علمه بوقوع جريمة ما، سواء تم هذا الإتصال عن طريق البلاغ أو الشكوى أو عن أي طريق آخر، أو من خلال القيام بجمع الإستدلالات والمعلومات حول الجريمة، بمعنى أن عملية إخبار السلطات المختصة بوقوع جريمة، هو أساس بدأ إجراء التحقيق في الجرائم، ففي الجرائم الإلكترونية تُعد عملية الابلاغ لها أهمية كبيرة لكونها تسهم في متابعة مرتكبي مثل هذه الجرائم وتعطي للمجنى عليه الثقة والأمان بأن حقه سيتم إرجاعه له من خلال السلطة القضائية، فعدم المبادرة بتقديم الابلاغ عن وقوع الجرائم الإلكترونية يؤدي إلى وقوع جرائم كبيرة وأشد خطراً كالتي تحدث في البورصات العالمية وتؤدي إلى إنخفاض أسهمها وخسارتها[2]. ويجب أيضاً عند تقديم المعلومات والبلاغ، أخذ بعض المعلومات من خلال المبلغ والتي ينبغي أن يدونها المحقق عنده تلقي البلاغ، وهذه المعلومات تكون عن طريق طرح بعض الأسئلة للشخص المبلغ، وتتمثل هذه الأسئلة كالآتي: معرفة تاريخ وقت تلقي البلاغ ، وايضاً أخذ بعض المعلومات الخاصة بالمبلغ ، فضلاً عن توجيه سؤال عن طبيعة ونوع الجريمة الإلكترونية محل البلاغ، ومن البديهي السؤال عن متعلقات الجريمة المرتكبة والتي تتمثل ببعض الأسئلة التي تبدأ بماذا ؟ وأين؟ وكيف؟ ومن؟ ولماذا؟ .إذ تسهم هذه المعلومات في مساعدة المحقق على تحديد ما إذا كان السلوك محل البلاغ يعد سلوكاً إجرامياً يندرج ضمن جرائم الحاسوب والإنترنت[3]. وأيضاً وضع تصور مبدئي عن خطة العمل المناسبة للتحقيق في الحادث. بالإضافة إلى تحديد نوع الخبرة الفنية التي يحتاجها في المعاينة ورفع وتحريز الأدلة من موقع الحادث فجميع هذه

(1) - د. خالد حسن أحمد لطفي، آليات التحقيق الجنائي في جرائم تقنية المعلومات، المصدر السابق، ص 52.

(2) - على عدنان الفيل، إجراءات التحري وجمع الادلة والتحقيق الابتدائي في الجريمة المعلوماتية، المصدر السابق، ص 11.

(3) - د. خالد حسن أحمد لطفي، الدليل الرقمي ودورة في إثبات الجريمة المعلوماتية، دار الفكر الجامعي، الاسكندرية، 2020، ص98.

المعلومات يحتاجها المحقق أثناء التحقيق للبحث والتحقيق في الجرائم الإلكترونية للوصول إلى مرتكبيها[1].

فالتحري هو الوسيلة أو الطريقة التي يتم بمقتضاها الوقوف على حقيقة أمر من الأمور، فهي عبارة عن الإجراءات اللازمة للكشف عن الجريمة، ومعرفة مرتكبيها، وكذلك هي عملية تجميع للقرائن والأدلة التي تثبت وقوع الجريمة ونسبتها إلى فاعلها. وهناك من يعرفها على أنها: هي المعلومات التي جمعت عن الوقائع المطلوب معرفتها، أو أي وقائع تصل إلى علم أعضاء الضبط القضائي[1]. ويقتضي ذلك إجراء التحريات اللازمة وتدوين المعلومات حول الجريمة، ومن ثم إجراء التحريات اللازمة حول الشبهات والبلاغات التي وصلت للسلطة العامة، وذلك لتحديد الواقعة وهوية مرتكبيها وهو ما يعرف بإستنطاق الشبهات[2].

فالتحقيق في الجرائم الإلكترونية يتطلب إتخاذ خطوات عملية وعلمية لأجراء التحقيق في مثل هذه الجرائم، فقد يتطلب إجراء التحقيق في هذه الجرائم، الدقة في التخطيط والتفتيش ومتابعة تحركات المتهم، وهذا يعني أن تكون عملية التخطيط دقيقة بما فيه الكفاية لتحديد مستوى أختصاصي لدعم الشرعية الرقمية التي تكون مطلوبة في مسرح الجريمة الإلكترونية إذ تقوم وحدة متخصصة بالشرعية الرقمية بما يلزم من الخطوات التالية، وهي الإحاطة بمسرح الجريمة الإلكترونية، ومعرفة نوع الجريمة والطريقة المناسبة لإجراء التفتيش والإستيلاء على المعدات التي قد تحتوي على الدليل الإلكتروني لإستخلاصه[3]. وأيضاً تأمين موقع الحادث: بمعنى يجب أن يكون الشخص المسؤول عن البحث في مسرح الجريمة الإلكترونية ممارساً لعمله مع ضمان سلامة جميع الأشخاص في مكان الحادث وسلامة جميع الأدلة من مسرح الجريمة الإلكترونية سواء التقليدية، أو الإلكترونية، ويجب أن يلاحظ ان الأدلة المحتملة على أجهزة الحاسب والأجهزة الإلكترونية الأخرى يمكن تغييرها بسهولة أو حذفها أو تدميرها، كما يجب اتباع السياسات والإجراءات القانونية لتأمين مسرح الجريمة الإلكترونية[4]، بالإضافة إلى جميع الإجراءات المتخذة من أجل الحفاظ وتأمين الادلة، وللقيام بتأمين الأدلة الرقمية يكون باتباع بعض الامور الفنية والتقنية للحفاظ على كلمات السر وغيرها من

(1) - خالد عياد الحربي، إجراءات التحري والتحقيق في جرائم الحاسوب الإنترنت، المصدر السابق ، ص191.

(1) - بلقيس غازي عيدان الفلاحي . د. رحمة الله حبوب، الجهات المختصة بإجراء التحريات الجنائية في القانون العراقي، بحث منشور، مجلة كلية المعارف الجامعة، العدد ، المجلد ، 2018 ، ص 459.

(2) - د. محمد كمال شاهين، المصدر السابق ، ص 249.

(3) - أحمد محمود خليل، التحقيق الجنائي (تحقيق النيابة العامة)، دار الكتاب والدراسات العربية، الاسكندرية، 2017، ص 82.

(4) - د. خالد حسن احمد لطفي، آليات التحقيق الجنائي في جرائم تقنية المعلومات، المصدر السابق ، ص 44 و 47.

الملاحظات المكتوبة الخطية في مسرح الجريمة، بالإضافة إلى الإحتفاظ بأي وثائق ورقية في مسرح الجريمة الإلكترونية وإبعاد جميع الأشخاص عن مسرح الجريمة بما فيها من مصادر الأدلة التي تم جمعها، وأيضا تأمين جميع الاجهزة الإلكترونية المتواجدة في مسرح الجريمة بما في ذلك الأجهزة الشخصية والمحمولة[1].

ونلاحظ أيضاً من ضمن مظاهر التطور التكنولوجي والتقني ومدى تأثيره في مجريات التحقيق ومراقبة المتهم، هو الوضع تحت المراقبة الإلكترونية هو أحد الأساليب الحديثة و المبتكرة كبديل للعقوبة السالبة للحرية، وتكون مؤقتة المدة، ويقال له السجن في محل الاقامة، ويقوم هذا الأسلوب على السماح للمحكوم عليه البقاء في منزله ولكن بشرط أن تكون تحركاته محدودة، فالمراقبة تتم بواسطة جهاز شبيه بالساعة أو السوار يثبت في معصم اليد أو في الساق، لذلك أطلق على هذا النظام (السوار الإلكتروني)، كما يسميه بعض العاملين في المجال العقابي، وقد أخذ هذا النظام كبديل للعقوبة السالبة للحرية قصيرة المدة في التشريعات العقابية في الولايات المتحدة الأمريكية، ويعمل السوار الإلكتروني المستخدم في المراقبة عن طريق ثلاث وسائل: الأولى وهي طريقة البث المتواصل وهو ما أخذ به غالبية الدول التي أخذت بهذا النظام، ويرسل السوار إشارات محددة كل خمس عشرة ثانية إلى مستقبل موصل بالخط الهاتفي في مكان إقامة الشخص وينقل هذا المستقبل إشارات أوتوماتيكية إلى نظام معلوماتي مركزي مجهز بتقنيات يمكنها من تسجيل هذه الإشارات والمعلومات، ويوجد هذا النظام لدى الجهة التي تتولى رقابة المحكوم عليه. أما الطريقة الثانية فهي تسمى طريقة التحقق الدقيق بموجبة يُرسل نداء تلفوني بشكل أوتوماتيكي إلى محل إقامة الشخص الخاضع للمراقبة الإلكترونية، ويستقبل هذا النداء ويرد عليه عبر رمز صوتي مبرمج مسبقا. الطريقة الثالثة وهي المراقبة عبر الأقمار الصناعية المعمول بها في الولايات المتحدة الأمريكية[1]، أما في ظل قانون الإمارات الإتحادي رقم 17 لسنة 2018 بشأن تعديل بعض أحكام قانون الإجراءات الجزائية في المادة (355) إجراء الوضع تحت المراقبة إلكترونية بأنه: هو حرمان المتهم المحكوم عليه من أن يتغيب في غير الاوقات الزمنية المحددة له عن محل إقامته أو أي مكان آخر يعينه الأمر الصادر من النيابة العامة أو المحكمة المتخصصة بحسب الأحوال، ويتم تنفيذها عن طريق وسائل

(1) - راشد محمد المري، المهارات الفنية رجال الأمن في التحقيق والبحث الجنائي، بحث منشور، مجلة روح القانون، العدد الثاني والتسعون، 20 20 ، ص 92.

(1) - عبدالهادي درار، نظام المراقبة الالكترونية في ظل تطورات النظم الاجرائية الجزائية، بحث منشور، جامعة جيلالي اليابس، كلية الحقوق، مجلة الدراسات والبحوث القانونية، العد الثالث، 2017، ص 147.

إلكترونية تسمح بالمراقبة عن بعد وتلزم الخاضع لها بحمل جهاز إرسال الإلكتروني مدمج طوال فترة الوضع تحت المراقبة[1].

وتأسيساً على ما تقدم نجد أن إستراتيجية مكافحة الجريمة الإلكترونية من الناحية الإجرائية بشقيها الوقائي والقضائي تتميز بأنها ذات طبيعة فنية وتقنية خاصة تقتضي من القائمين عليها أن يتوافر لديهم مهارات فنية فائقة[2]، ومن ثم ضرورة تأسيس وحدات متخصصة لمكافحة هذه الجرائم سواء من الناحية القضائية باتخاذ الإجراءات المانعة من إرتكاب الجريمة الإلكترونية، وذلك بمعرفة مأموري الضبط الإداري (police administrative) أو من بعض القائمين على خدمات الإتصال بالإنترنت كمزودي الخدمات أو من الناحية القضائية، من خلال إتخاذ إجراءات جمع الأدلة والتحقيق فيها بمعرفة سلطة التحقيق الابتدائي الاصلية، أو إجراءات المحاكمة، تلك الإجراءات يسبقها إجراء آخر تحضيري ينشأ بعد إرتكاب الجريمة وقبل التحقيق فيها يهدف إلى البحث والتحري وجمع الإستدلالات والمعلومات عنها ووضعها تحت تصرف سلطة التحقيق ويمثل مثل هذا الإجراء التحضيري أهمية كبيرة في مساعدة سلطة التحقيق الإبتدائي في أداء عملها. كما يتعين أن تأتي الإجراءات التي تتخذها سلطات التحقيق بشقيها الوقائي والقضائية متفقة وصيانة الحق في الخصوصية المعلوماتية للأفراد ولن يأتي ذلك إلاّ من خلال سلطات مدربة متخصصة في مجال البحث والتحري والتحقيق في الجريمة الإلكترونية[1].

ونجد أن المشرع العراقي أولى هذه المهمة إلى قانون أصول المحاكمات الجزائية العراقي رقم (23) لسنة 1971 المعدل بالإضافة فقد أوكل هذه المهمة للتحقيق في الجرائم إلى جهاز الإدعاء العام وفقا للقانون الصادر بالرقم (49) لسنة 2017 وقد حددت هذه القوانين سلطات التحري وجمع الأدلة ومساعدة سلطات التحقيق الإبتدائي فألقت على عاتقهم إجراءات التحري وجمع الإستدلالات التي تسبق التحقيق في الدعوى العامة كما أوجبت عليهم قبل ذلك البحث عن الجرائم ومرتكبيها عند تلقي البلاغات عنها، فمن أهم الواجبات الملقاة على عاتق أعضاء الضبط القضائي هو الدور الرقابي كوسيلة لحماية القانون وهيبته ولهم أيضاً اتخاذ كل ما من شأنه التوصل إلى كشـــف معالم الجريمة

(1) - د. خالد ممدوح إبراهيم، إجراءات التقاضي الإلكتروني في المواد المدنية و الجنائية، دار الفكر الجامعي، 2021 ، الاسكندرية، ص 246.

(2) - على عدنان الفيل، إجراءات التحري وجمع الادلة والتحقيق الابتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث، 2011، ص 25 وما بعدها.

(1) - د. محمد كمال شاهين، الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي، المصدر السابق، ص 135.

وهو تكليف عام أورده المشرع في صلب القانون[1].

وتأسيساً على ما تقدم يجب أن يتم تشكيل فريق التحقيق من أشخاص فنيين وأخصائيين من ذوي الخبرة الطويلة في مجال الحاسوب[2]، والإنترنت، يمتازون في مهارات تقنية في الحاسوب والتحقيق الجنائي بشكل عام والتحقيق الجنائي الإلكتروني بشكل خاص، أو أن يستعين هؤلاء المحققون بخبراء في مجال الحاسوب والإنترنت، ليتمكنوا من فك الشيفرات السرية والتعامل مع التعقيدات التي تفرضها ظروف وملابسات كل جريمة. فالتحقيق في الجرائم الإلكترونية يتطلب الإستعانة ببعض الخبراء في الجرائم التقليدية مثل خبير البصمات وخبير التصوير، الذين يُعدون من الخبراء الأساسيين في معظم أنواع الجرائم، بالإضافة إلى غيرهم من الخبراء الذين قد يفرضهم إرتباط جريمة الحاسوب والإنترنت محل التحقيق بجريمة أخرى من الجرائم التقليدية كجرائم القتل وغيرها. ونظراً لأن التحقيق في الجرائم الإلكترونية يتطلب مهارات فنية قد لا تتوافر لدى الكثير من المحققين، فإن تشكيل فريق خاص بالتحقيق في هذا النوع من الجرائم الإلكترونية قد يكون أمراً ضرورياً وإن كان اسلوب عمل الفريق يستخدم في التحقيق في كثير من أنواع الجرائم، إلاّ أنه يأخذ أهمية خاصة في جرائم الحاسوب والإنترنت لما تطلبه من مهارات وخبرات متنوعة ومتعددة[1].

ثالثا : الإجراءات المستحدثة في التحقيق بالجرائم الإلكترونية:

من أهم إجراءات البحث والتحقيق الفنية والعلمية الجديدة التي أرستها معظم الإتفاقيات والمعاهدات الدولية في هذا الصدد منها: الدخول والنفاذ إلى برامج الحاسب الآلي وقواعد البيانات وغيرها من

---

(1) - بلقيس غازي عيدان الفلاحي . د. رحمة الله حبوب، المصدر السابق، ص 462.

(2) - يعرف القانون الحاسوب بتعريف واسع وهو (أي جهاز الكتروني أو مغناطيسي أو الكترو-كيميائي أو أي وحدة معالجة بيانات سريعة تقوم بوظائف منطقية أو لوغاريتمية أو وحدات التخزين. وتتضمن "وحدة خزن البيانات أو وحدة التواصل المتعلقة فيه أو مرتبطة بجهاز مشابه له) ان هذا التعريف لعمومية تعريف الحاسوب من قبل المشرع**United** . وذكرت أحد المحاكم تعريف الحاسوب أيضا بانه أي وحدة معالجة بيانات، وذلك في قضية **States v. Mitra** في العام 2005. ينظر: The CFAA exists against the backdrop of numerous state computer crime laws that are beyond the scope of this Report. E.g., VT. STAT. ANN. tit. 13, §§ 4101–07. Computer misuse statutes have been enacted in “all fifty states . . . .” KERR, supra note 7, at 29; accord Computer Crime Statutes, NAT’L CONF. OF STATE LEGISLATURES (Feb. 24, 2020).

وعرف القانون نوع آخر من الحاسوب هو الحاسوب المحمي والذي كان الحاسوب المستخدم من مؤسسة مالية أو من قبل الحكومة الأمريكية والذي يستخدم للتأثير على التجارة بين الولايات أو التجارة أو الاتصالات الخارجية. وما يعد من قبيل الحاسوب هي الهواتف الذكية وتطبيقاتها والحواسيب التي تستخدم لإدارة المواقع الرقمية ومعالجة البيانات وقد عدت أحد المحاكم الحواسب الخادمة بمثابة حاسوب محمي بموجب أحكام هذا القانون وذلك في سياق قضية **hiQ Labs, Inc. v. LinkedIn Corp** في العام 2019 أمام محكمة الدائرة التاسعة الإتحادية. ينظر: hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 999 (9th Cir. 2019).

(1) - خالد عياد الحلبي، المصدر السابق ، ص 198.

الأجهزة والنظم المعلوماتية. والطريقة الثانية هي إعتراض المراسلات والمراقبة الإلكترونية، وكذلك الحفظ والإفشاء العاجلان للمعطيات الإلكترونية، ونجد أن إتفاقية منظمة الأمم المتحدة المتعلقة بمكافحة الجريمة المنظمة عبر الوطنية تضمنت في نص المادة (20) منها على أساليب التحري الخاصة بما فيها التسريب التي عبرت عنها بالأعمال المستترة[1]. أما المشرع الفرنسي فقد نظم عملية التسرب في المادة (7/694 و 9/694 و 706/ 81 و 87/706) من قانون (2004 / 207) المتضمن قانون الإجراءات الجنائية المعدل. (والتسرب) هو من الناحية الامنية هو (تلك العملية المحضر لها والمنظمة والمراد من القيام بها التوغل داخل وسط النظم المعلوماتية لمعرفة حقيقتها معرفة جيدة من خلال نشاطها البارز وكشف الخفي منه)[1]، ويمكن تصور عملية التسرب في نطاق الجرائم الإلكترونية من خلال دخول ضباط الشرطة أو أعوانهم إلى العالم الإفتراضي وإختراق المواقع وفتح ثغرات إلكترونية فيها أو اشتراكهم في محادثات الدردشة أو حلقات اتصال مباشرة مع المشتبه فيهم والظهور بمظهر كما لو كان فاعلاً مثلهم، مستخدما في ذلك الأسماء وصفات مستعارة سعي منه للإستفادة منهم حول كيفية اقتحام الهاكر للموقع. أما (المشرع المصري) فقد جاء في نص المادة (6) من قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018 لتضع هذا الإجراء في إطار قانوني إذ نصت على انه: لجهة التحقيق المختصة بحسب الأحوال ان تصدر امراً مسبباً لمأموري الضبط القضائي المختصين لمدة لا تزيد على (30) يوم قابلة للتجديد لمرة واحدة، متى كان لذلك فائدة في ظهور الحقيقة على إرتكاب جريمة معاقب عليها بمقتضى أحكام هذا القانون بواحد أو أكثر. ويتضح من هذا النص أن المشرع المصري قد وضع شروطاً لإتمام عملية التسرب (البحث والتفتيش والدخول والنفاذ إلى برامج الحاسوب وقواعد البيانات وغيرها من الأجهزة ونظم المعلومات)، ويتعين مراعاتها عندما تقتضي ضرورات التحقيق [2].

وقد أوصت الإتفاقية الأوروبية حول الجرائم الإلكترونية لعام 2001 من خلال نص المادة (21) جميع الدول الأعضاء بضرورة تبني اعتراض المراسلات ومراقبة الإتصالات في تشريعاتها الداخلية ضمن إجراءات البحث والتحقيق، الأمر الذي لقي استجابة واسعة من طرف غالبية الدول الاوروبية[3]. أما (المشرع الفرنسي) كان سباقاً إلى تبني عملية إعتراض ومراقبة الإتصالات الإلكترونية ضمن إجراءات التحري والتحقيق الجنائي من خلال قانون الإجراءات الجزائية لعام

(1) - د. محمد ابو العلا عقيدة، مراقبة المحادثة التلفونية، دار النهضة العربية، 2008، ص 192.
(1) - د. خالد حسن أحمد لطفي ، آليات التحقيق الجنائي، المصدر السابق، ص 79.
(2) - د. رامي متولي القاضي ، مكافحة جرائم تقنية المعلومات، المصدر السابق، ص 281.
(3) - إبراهيمي جمال ، التحقيق الجنائي في الجرائم الالكترونية، المصدر السابق، ص 87.

1991 ، ثم تبعه المشرع الأمريكي في عام 2000 بعد تعديل القانون الإتحادي الإجرائي، نظراً لثبوت نجاعة هذا الأجراء في تعقب الدليل وإثبات الجرائم الإلكترونية[1].

ومن ضمن الإجراءات التي يقوم بها أعضاء الضبط القضائي أو الفريق المكلف بالبحث والتحقيق في الجريمة الإلكترونية هو أسلوب الحفظ والإفشاء العاجلان للمعطيات الإلكترونية، ويُعد هذا الإجراء بالنسبة للغالبية الدول أسلوباً جديداً في عملية البحث والتحري في مجال مكافحة الجريمة الإلكترونية، وتمت الإشارة إليه لأول مرة في لائحة الجمعية العامة لمنظمة الأمم المتحدة رقم (65 / 63) لعام 2001 المتعلقة بمكافحة إساءة إستعمال تكنولوجيا المعلومات لأغراض إجرامية، اذ نصت في المادة الأولى (ف / و) على ضرورة سماح الدول الأعضاء لجهاتها المختصة بالإستدلال، وأمر مزودي خدمة الإتصالات القيام به بالحفظ السريع للمعطيات الإلكترونية المتعلقة في التحقيقات الجنائية[1]، وبعدها تضمنت (إتفاقية بودابست) لمكافحة جرائم المعلوماتية لعام 2001 إجراءات الحفظ والإفشاء على البيانات المخزنة في نظم المعلوماتية. وألزمت الدول الموقعة على الإتفاقية من خلال المادتين (16 و 17) إتخاذ الإجراءات التي ترى أنها ضرورية من أجل السماح للسلطات المختصة في التحقيق عن الجرائم إلكترونية بأن تأمر بالحفظ والإفشاء العاجلين على المعطيات المعلوماتية المخزنة. أما المشرع المصري فقد جاء في قانون الإجراءات الجنائية المصري في المواد (95) مكرر بأنه: 1- لقاضي التحقيق أن يأمر بضبط جميع الخطابات والرسائل والجرائد والمطبوعات والطرود لدى مكاتب البريد أو جميع البرقيات لدى مكاتب البرق، وأن يأمر بمراقبة المحادثات السلكية واللاسلكية أو إجراء تسجيلات لإحاديث جرت في مكان خاص متى كان لذلك فائدة في ظهور الحقيقة في جناية أو جنحة معاقب عليها. 2- لرئيس المحكمة المختصة في حالة قيام دلائل قوية على أن مرتكب إحدى الجرائم المنصوص عليها في المادتين (166 مكرر) و (308) مكررا من قانون العقوبات قد إستعان في إرتكابها بجهاز تلفوني معين ان يأمر بناء على تقرير مدير عام مصلحة التلغرافات والتلفونات وشكوى المجنى عليه في الجريمة المذكورة بوضع جهاز التلفون مسكون تحت الرقابة للمدة التي يحددها[2].

أما (المشرع الاردني) فقد نظم موضوع التحفظ والإفشاء العاجل ضمن قانون جرائم أنظمة المعلومات الأردني رقم (30 9 لسنة 2010 فنجد أن المشرع الأردني قد منح أعضاء الضبط القضائي (الضابطة العدلية) بعد الحصول على إذن من وكيل النيابة (المدعي العام) المختص أو

(1) - د. خالد حسن أحمد لطفي ، آليات التحقيق الجنائي ، المصدر السابق، ص 82.

(1) - كامل سعيد، جرائم الكمبيوتر والجرائم الاخرى في مجال تكنولوجيا المعلومات، دار الثقافة للنشر، عمان، 2002، ص 46.

(2) - د. خالد حسن أحمد لطفي ، آليات التحقيق الجنائي، المصدر السابق، ص 85.

المحكمة المختصة، الدخول إلى أي مكان تشير الدلائل إلى استخدامه لإرتكاب أي من الجرائم المنصوص عليها في القانون، وقد نص القانون النموذجي للإجراءات الجزائية على التحفظ العاجل للبيانات الحاسوبية وبيانات مرور الإتصالات السلكية واللاسلكية، إذ أجاز القانون لعضو النيابة العامة إصدار أمر لضمان التحفظ العاجل على بيانات الحاسوب و بيانات الاتصال السلكية واللاسلكية المخزنة بواسطة حاسوب، أو نظام إتصالات في الحالات التالية: إذا كان هناك إحتمال بأنه تم ارتكاب جريمة، وكذلك إذا كان لدى عضو النيابة العامة مبرر للاعتقاد بأن البيانات متعلقة بالتحقيق في الجريمة. وفي حال إذا كان لدى عضو النيابة العامة مبرر للإعتقاد بأن الجهات المعنية عرضة للفقدان أو التعديل[1]

وهناك مجموعة من الإجراءات التقنية والفنية التي تساعد المحقق وأعضاء الضبط القضائي للوصول إلى كشف الحقيقة وهوية المجرم في الجريمة الإلكترونية، وهذه الإجراءات هي:

1- الوسائل الإجرائية: هي تلك الإجراءات التي تتخذ أثناء إجراء طرق التحقيق الثابتة والمحددة، والأساليب المتغيرة، وغير المحددة، التي تثبت وقوع الجريمة، وتحدد شخصية مرتكبيها. وتتمثل هذه الوسائل على النحو الاتي [1]: اقتفاء الأثر. من العقبات التي قد تواجه الشرطة في عمليات التحقيق هي عمليات محو الرسائل إذ قد يعمد المجرم إلى استخدام تطبيقات تمحي الرسائل التي إستخدمها للإبتزاز أو لاختراق مواقع مما يجعل عملية الرقابة على رسائله معقدة، وتكمن المشكلة في الجرائم التي لا يوجد فيها أي دليل عدى الرسائل التي ابتز بها والتي تتمثل بالصور أو المعلومات الشخصية، ومن ثم أن مراقبة الشرطة لرسائله قد تكون عقيمة مما يعني تبرئته من أي تهمة تسند إليه لغرض التخلص من هذا الخطر توجد تطبيقات تكتشف عمليات محو الرسائل والتي تساعد على إعادة هذه الرسائل التي تم محوها، والتي تتوفر لسلطات التحقيق بالطبع، يوجد حاليا تطبيقان متوفران للمساعدة على الكشف عن هذه البيانات وأداة واحدة ايضاً. تكمن المشكلة بالتورية، بانتفاع مستخدمي هذه البرامج من مسألة أن أغلب الحاسبات تحتوي على مساحة فارغة، فتقوم بإخفاء البيانات بها من الصور، أو الرسائل الممحية، ومن ثم فإن البيانات لن تظهر للشرطة حينما تقوم بالتحقيق ولن يعلم أي شخص محتوى الرسائل سوى المرسل والمستقبل، ويقوم الشخص الذي قام بالتورية بإستبدال الصورة ببيانات أخرى عوضاً عنها فعلى سبيل المظاهر قد تظهر الصورة التي قام بإبتزاز شخص

(1) - مصطفى عبد الباقي التحقيق في الجريمة الإلكترونية و إثباتها في فلسطين المصدر السابق ، ص 286.
(1) - خالد عياد الحلبي، المصدر السابق ، ص 212 . وكذلك : د. اكرم سلام عبدالرؤوف سلام، المصدر السابق، ص 88.

آخر بشكل صورة اعتيادية[1]. ومن الجدير بالذكر أنه توجد برامج تورية مجانية وبعض منها تجارية، ويوجد العديد من الأشخاص حول العالم من يستخدمون برامج التورية بشكل مشروع، مما يجعل عملية إستبدال الصور، أو مسحها سهلة بالنسبة لهم، مما يعني إمكانية الحصول على هذه البيانات بسهولة من المواقع الإلكترونية أو حتى شرائها وإستخدامها لأغراض إجرامية من قبلهم[2].

2- **الوسائل المساعدة** للكشف عن الجرائم الإلكترونية: يحتاج رجال التحقيق في جرائم الحاسوب إلى مشاهدة وفحص الأدلة الجنائية، وهي غالبا ما تتميز بسهولة الإستخدام والبعد عن التعقيد، لان الكثير من مستخدمي الحاسوب يستخدمونها كبرامج عرض الصور وبرامج فك الملفات وغيرها[3]. ولذلك ينبغي على ضباط التحقيق أن يكونوا على معرفة في اتباع عدة إساليب في حالات أخرى، ولذلك فإنه يحتاج للوسائل المادية والمعنوية ليستخدمها في التحقيق ، ورغم أن التعامل مع الأدلة بشكل مباشر يعد من مهام خبير الحاسوب الجنائي في فريق التحقيق إلا أن معرفة ضباط التحقيق ببعض أساليب الفحص والمتابعة التي يستخدمونها أمر مطلوب وله مردود إيجابي على التقيد بالإجراءات الصحيحة الضامنة لنجاح التحقيق. ومن هذه الوسائل والبرامج الإلكترونية المساعدة، والتي من خلالها يتم إرتكاب الجريمة الإلكترونية، ومن خلال هذه البرامج نفسها يمكن لفريق التحقيق ان يستغلها لمتابعة الجريمة والمجرم، وكشف الحقيقة هي[1]. **أ- عناوين الإنترنت (mac&ip) والبريد الإلكتروني وبرامج المحادثة:** هو المسؤول عن أرسال حزم البيانات عبر الإنترنت وتوجيهها إلى أهدافها ويشبه إلى حد بعيد العنوان على مغلف رسائل البريد التقليدية بعد وضعها في صندوق البريد، وهو يتيح للموجات والشبكات المعنية بنقل الرسائل، يوجد عنوان(ip) بكل جهاز مرتبط بالإنترنت ويتكون من أربعة أجزاء[2]. **ب- البروكسي** (proxy) يعمل تطبيق برنامج البروكسي كوسيط بين الشبكة ومستخدمها إذ تضمن الشركات الكبرى المقدمة لخدمة الإتصال بالشبكات قدرتها لإدارة الشبكة وضمان الأمن وتوفير خدمات الذاكرة الجاهزة، إذ يتلقى مزود البروكسي عبر الإنترنت طلبا من المستخدم حيث يبحث عن الصفحة المطلوبة ضمن ذاكرة كاشي (cache)، وأهم مزايا مزود البروكسي أن ذاكرة كاشي المتوافرة لديه يمكن أن تحتفظ بتلك العمليات التي تمت عليها مما يجعل دورها قويا في الإثبات عن طريق فحص تلك العمليات المحفوظة بها والتي تخص المتهم والموجودة

(1) - د. عزالدين عثماني، إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلومات، بحث منشور، مجلة دائرة البحوث والدراسات القانونية والسياسية، العدد الرابع، 2018، ص55.

(2)- Gary R. Gordon, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, January 2003, page 40-45.

(3) - علي عدنان الفيل، المصدر السابق، ص 74.

(1) - خالد عياد الحلبي، المصدر السابق ، ص 205 و 206 .

(2) - على عدنان الفيل، إجراءات التحري وجمع الادلة والتحقيق الابتدائي في الجريمة المعلوماتية، المصدر السابق، ص 69.

لدى مزود الخدمة[1]. **ج- برامج التتبع** يمكن لبرامج التتبع أن تقوم بالتعرف على محاولات الإختراق ومن قام بها وإشعار الجهة المتضررة بعملية الإختراق، وحينما يحصل إختراق أو هجمة على الموقع يقوم الجهاز بإخطار السلطات المختصة على الحدث ويقوم بحظر أي نشاط مماثل لذلك. تستخدم معظم المنظمات هذا التطبيق في داخل نطاق الشبكة الرقمية للمنظمة يستخدم هذا التطبيق العديد من الأجهزة والأنظمة والتي تساعد جميعها في تعقب النشاط ومعرفة نمطها وآلية إرتكاب عملية الإختراق[2]، ثم يبدأ بعملية مطاردة تستهدف أقتفاء أثر مكتب عملية الإختراق حتى يصل إلى الجهاز الذي حدثت العملية من خلاله، وهذا البرنامج يتكون من شاشة رئيسية تقدم للمستخدم بياناً شاملاً بعمليات الإختراق التي تحدث ضد جهازه وتحمل اسم الحدث وتاريخ حدوثه وعنوان (ip) الذي تمت من خلاله[1].

ونجد أن المشرع العراقي قد تطرق إلى موضوع المراقبة الإلكترونية أثناء التحقيق، في مشروع قانون الجرائم المعلوماتية والتقنية، والذي لم يتم إقراره لحد الان، وجاء بنص المادة (26/ ثالثا/ج) منه على أنه: (للقاضي المختص أن يأمر بالدخول إلى أجهزة الحاسوب والشبكات أو اي جزء منها والى البيانات المخزنة فيها والى اي واسطة أو وسيلة يمكن أن تخزن فيها بيانات الحاسوب الموجودة داخل العراق وله إعتراض البيانات ورصدها ومراقبتها بقرار مسبب ولمدة وغرض محددين). ونلاحظ من نص المادة أعلاه أن المشرع العراقي قد تناول موضوع المراقبة الإلكترونية بشكل عام، دون أن يخوض في تفاصيل وشروط ومدى هذه المراقبة، مما يتطلب معالجة هذا الموضوع قبل التصويت على هذا القانون، حتى لا نكون أمام انتهاك المعايير الاساسية للحقوق والحريات الخاصة .

ويرى الباحث أنه عند تشكيل فريق التحقيق، أو جهاز عمليات خاص، مختص في التحقيق في الجرائم الالكترونية، يجب أن يكون الاخير على درجة كبيرة من الأهمية والخبرة في مكافحة الجرائم الإلكترونية، ويتوجب على أعضاء هذا الجهاز أن يملك الالمام الفنية والتقني ، فيما يتعلق بتكنولوجيا المعلومات والبيانات الرقمية، للتوصل إلى حل الغموض الفني في أنظمة الإنترنت بحيث يمكن تطوير عملهم بالاستعانة بمجموعة من الخبراء الدوليين، ذلك لإمتداد هذه الجرائم عبر النطاق الدولي والإقليمي ولكونها من الجرائم المتطورة مع تطور التكنولوجيا .

---

(1) - د. عزالدين عثماني، إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلومات، المصدر السابق، ص 54 . وكذلك: د. اكرم سلام عبدالرؤوف سلام، المصدر السابق، ص 88.

(2) Ibid, page45.

(1) - د. خالد ممدوح إبراهيم، الجرائم المعلوماتية، المصدر السابق ، ص 203.

المطلب الثاني

الوسائل التقنية الناتجة عن التطور التكنولوجي في مجال السمعيات والمرئيات

أدى التطور التكنولوجي والتقني في الوقت الحاضر إلى إكتشاف أجهزة أسهمت بشكل كبير في تقدم الشعوب وتحضرها، وفي المقابل أدى هذا التطور إلى مخاطر كبيرة تهدد حقوق الأفراد وحياتهم الخاصة، وقد تضاعف أهتمام التقنية الحديثة للتصوير الفوتوغرافي والتسجيل الصوتي، وأدى ذلك بالنتيجة إلى ظهور مشكلات قانونية عديدة تتعلق بمدى مشروعية إستخدام مثل هذه الأجهزة ومدى الحماية المقررة لحرمة الشخص وخصوصياته من المخاطر الناجمة عن إساءة استخدام هذه الاجهزة، إذ تسعى سلطات التحقيق إلى الكشف عن الجريمة وضبط الجناة، بالإستعانة بما قدم لها التطور التكنولوجي والتقني في مجال الرقابة السمعية والبصرية من إستخلاص الأدلة والبراهين التي تثبت إدانة الشخص عند قيامة بإرتكاب جريمة ما. **وهنا يثار التساؤل عن مدى مشروعية هذه الإجراءات؟** وهل يختلف الأمر لو كان القيام بالإجراءات هو أحد أعضاء الضبط القضائي خلال مرحلة التحقيق وجمع الإستدلالات، أو من قام بهذا الأمر ليس من فريق سلطة التحقيق؟ وقد أدى التطور في الجريمة الإلكترونية خلال أواخر القرن الماضي وبداية هذا القرن بإستخدام المجرمين لأحدث الأساليب العلمية في إرتكاب الجرائم الإلكترونية، ما يستوجب إلى ضرورة البحث عن الحلول الناجحة للحد من تفاقم معدلات الجريمة الالكترونية، ولذا استمر التطور التقني في إنتاج أجهزة التصوير وزيادة كفاءة عدساتها التصويرية بتقنية عالية، وإختراع الدوائر التلفونية المغلقة التي تسمح بمراقبة المكان ومعرفة كل ما يدور بداخلة، كما أن إستخدام أجهزة المراقبة المرئية لتحديد مكان الشخص وتصرفاته دون علمه أو ضد رغبته، يؤدي إلى تهديد واضح وخطير لخصوصيات الأفراد. وللإجابة على التساؤل الذي يخص مدى شرعية استخدام الوسائل والاجهزة التقنية لإجراء التنصت والتسجيل الصوتي، سنحاول الأجابة من خلال تقسيم هذا الموضوع إلى فرعين، نخصص الفرع الاول لدراسة التنصت ومراقبة المكالمات وأجهزة الكمبيوتر، ويكون موضوع دراستنا في الفرع الثاني هو الوسائل المرئية الإلكترونية.

الفرع الأول

التنصت ومراقبة المكالمات وأجهزة الكمبيوتر

التسجيل الصوتي هو بالأصل مفردة فنية، أكثر مما هي مصطلح قانوني، إلاّ أن فقهاء القانون الجنائي حاولوا الوصول إلى تعريف هذه المفردة بمناسبة الحديث عن تسجيل المكالمات الهاتفية والأحاديث

الخاصة، كأحد الجرائم الواقعة على حرمة الحياة الخاصة[1]. فيعرف التسجيل: (هو حفظ الحديث على مادة معدة لذلك لإعادة الاستماع إليه فيما بعد)[2]. وأيضا يعرف التسجيل الصوتي بأنه: (عبارة عن ترجمة التغيرات المؤقتة لموجات الصوت الخاصة بالكلام أو الموسيقى إلى نوع آخر من الموجات أو التغيرات الدائمة، ويكون التسجيل عادة بواسطة آلة تترجم موجات الصوت إلى اهتزازات خاصة)[3]. ولقد أدى ظهور أجهزة التسجيل الصوتي الحديث إلى زيادة الخطورة على حرمة الحياة الخاصة، والسبب في ذلك أن الحواجز المادية لا تقف عقبة أمام هذه الوسائل التي تستطيع كشف أسرار الناس وخصوصياتهم بسهولة، ودون أن يشعروا بذلك. أما فيما يخص مدى حجية استخدام التسجيل الصوتي في الإثبات كدليل رقمي جنائي، ومدى تأثير هذه الوسائل الحديثة في السياسة الجنائية، فقد لعبت هذه الوسائل دوراً كبيراً إذ تطورت أساليب التسجيل الصوتي وأثرها على الحياة الخاصة تطورا ملحوظا[1].

أولا : موقف الفقه من شرعية التسجيل الصوتي:

إنقسم الفقه القانوني إلى عدة آراء بشأن شرعية وقبول التسجيل الصوتي، كإجراء من إجراءات التحقيق، فهناك الرأي الفقهي المعارض للتسجيل الصوتي، ويمثل الفريق المعارض للتسجيل الصوتي جماعة المدافعين عن الحقوق الشخصية للأفراد، ويقولون إنه لو سمح بإستخدام تلك الأدوات في التحقيق فإنه سلطات الأمن ستسعى إلى استخدام مثل هذه المناهج للتحقيق في أبسط القضايا، الأمر الذي يعد انتهاكا لحقوق الإنسانية والحياة الخاصة، ويعتمد هؤلاء المبدأ الدستوري الخاص بحماية حقوق الإنسان في الحفاظ على السكينة، ويعدون إستخدام السلطات العامة والتحقيق لهذه الأدوات اعمالاً غير نبيلة ومخالفة للآداب العامة. ويشبهون هذه الاعمال بأسلوب عمل الجاسوس[2]. أما الرأي الفقهي المؤيد للتسجيل الصوتي وحسب هذا الرأي من الفقه، يمكن الأخذ وإعتماد بالتسجيل الصوتي كدليل غير ممنوع قانونياً، الأخذ به في الإثبات الجنائي بحجة أن تسجيل المحادثات مشروع قانوني،

(1) - علي نعمة جواد الزرفي، الجريمة المعلوماتية الماسة في الحياة الخاصة، المكتب الجامعي الحديث، 2020 ، ص 117 .

(2) - سامية عبد الرزاق خلف، التعدي على حرمة الحياة الخاصة باستخدام التكنولوجيا الحديثة، بحث منشور، مجلة الدراسات القانونية، العدد 25، 2010، ص 124.

(3) - صالح عبد الزهرة حسون، احكام التفتيش وآثاره في القانون العراقي، ط1، مطبعة جامعة بغداد، 1979، ص 124 وما بعدها.

(1) - مبروك اساسي، مشروعية الصوت والصورة في الاثبات الجنائي، اطروحة دكتوراه، جامعة الحاج لخضر – باتنة 1، كلية الحقوق والعلوم السياسية، 2017، ص 132 . وكذلك: حيدر فالح حسن، التنصت الالكتروني على سرية الاتصالات والمراسلات بين التجريم والمشروعية، مقال منشور، على التطبيق الالكتروني (قانونجي)، بتاريخ 2022/9/5.

(2) - علي نعمة جواد الزرفي، الجريمة المعلوماتية الماسة في الحياة الخاصة، المصدر السابق، ص 122.

أي لا يوجد نص قانوني يمنع إستخدام الحديث المسجل على شريط أو اي جهاز تقني، في الإثبات الجنائي أو بأي وسيلة أخرى، ولذا يكون الإستناد إلى التسجيل الصوتي من الأمور المباحة قانونا، كذلك يوجد فريق آخر من الفقه يسوغ عملية التسجيل الصوتي على اعتبار أن هذا التسجيل لا يشكل إنتهاكا لحرمة الحياة الخاصة، أكثر مما هو نتاج عن عملية تفتيش الأشخاص والمنازل التي أباحها القانون[1]، وأيضاً ذهب جانب آخر من الفقهاء إلى تفضيل التسجيل الصوتي على الدليل الكتابي وذلك لأن التزوير في تقليد الصوت يكون أصعب من التزوير في الدليل كتابي[2].

ثانيا : موقف التشريعات المقارنة من التسجيل الصوتي:

نجد أن (المشرع الامريكي) في التعديل الرابع للدستور الأمريكي كفل حماية المواطن الأمريكي من التدخل التعسفي الواقع من قبل السلطة العامة في التفتيش وحرمته المساكن والأشخاص، ولكن الصياغة الحرفية له لم تتطرق إلى حماية المحادثات الشخصية صراحة، ومنع تسجيلها بشكل غير قانوني، والجديد بالذكر أن القانون الفدرالي الصادر عام (1968) في الباب الثالث منه والمتعلق بالتنصت التلفوني والمراقبة الإلكترونية حظر اللجوء إلى إلتقاط الأحاديث الشخصية التي تتم عادة بإستعمال أجهزة إلكترونية أو غيرها إلاّ بناء على أمر من السلطات القضائية وصدر بعد ذلك قانون الإتصالات الاتحادي رقم (18) لسنة 1970 بموجبه حظرت المادة (2518) إجراء أي تسجيل أو تنصت على المحادثات الخاصة سواء كان شفوياً أم هاتفيا[1].

أما موقف (المشرع الفرنسي)، فلم يتضمن التقنين الدستوري الفرنسي نصاً خاصاً يحدد مدى مشروعية التنصت للمحادثات و تسجيلها، وهذا ينطبق على قانون الإجراءات الجنائية الفرنسي الصادر عام 1957 الذي لم يتضمن كذلك نصا صريحا حول التسجيل والتنصت، ولقد بقي قانون الإجراءات الجنائية الفرنسي حتى عام (1970) خالياً من أي نص يحدد الوضع القانوني لتسجيل المحادثات الشخصية والتنصت عليها، ولكن في العام نفسه صدر قانون رقم (7) يوليو 1970 وبات بموجبه تسجيل المحادثات الخاصة أمراً غير مشروع، ولا يجوز الاستناد إلى ما يستمد منه من أقوال، وجرم بمقتضى المادتين (368) و (369) من قانون العقوبات أي إعتداء على المحادثات التي تجري في مكان خاص، كما أن تسجيل المحادثات الخاصة يُعد جائزاً بناء على أمر قضائي للتحقيق على وفق الشروط والضمانات المنصوص عليها في المادتين (80 و 81) من قانون

(1) - محمد رشاد ابراهيم مفتاح، الحماية الجنائية للحق في حرمة الاتصالات الشخصية، أطروحة دكتوراه، جامعة الاسكندرية، كلية الحقوق، 2009 ، ص 83.

(2) - د. قدري عبد الفتاح الشهاوي، الموسوعة الشرطية القانونية، عالم الكتب للنشر، القاهرة، 1997، ص420.

(1) - علي نعمة جواد الزرفي ، المصدر السابق، ص 126.

الإجراءات الجنائية، اذ تسمح لقاضي التحقيق إتخاذ كافة الإجراءات التي يراها مناسبة في إظهار الحقيقة[1].

أما موقف المشرع العراقي فنجد أن دستور جمهورية العراق لسنة 2005 جاء بنص المادة (40) منه على أن: حرية الإتصالات والمراسلات البريدية والهاتفية والإلكترونية وغيرها مكفولة ولا يجوز مراقبتها أو التنصت عليها أو الكشف عنها الاّ لضرورة قانونية وأمنية وبقرار قاضٍ. ويتبين من خلال هذا النص أن المشرع الدستوري وسع من نطاق حماية الاتصالات ليشير إلى الهاتفية منها والالكترونية وغيرها، مما فتح المجال أمام أي وسيلة أخرى تستحدث نتيجة التطور العلمي، ومنها ما يحصل عن طريق الحاسوب والأجهزة الذكية في ظل التطور التكنولوجي الذي يعيشه العالم[2]، ومع ذلك فإن قانون أصول المحاكمات الجزائية العراقي رقم (23) لسنة 1971 المعدل، جاء خالياً من أي نص يسمح في إمكانية اللجوء إلى إستخدام التنصت على المحادثات وتسجيلها في مجال الاثبات الجنائي، وإشار الدستور المذكور إلى أن إمكانية اللجوء إلى هذه إجراءات لضرورة العمل والعدالة، أما فيما يخص قانون العقوبات العراقي رقم (111) لسنة 1969 المعدل، فلم يتضمن تجريم التنصت على المحادثات أو تسجيلها إلاّ أن المادة (328) تعاقب على إفشاء المكالمات الهاتفية وتسهيل ذلك للغير، دون أن تشير إلى فعل التسجيل والتنصت ذاته، وأنها تجرمه إذا صدر من الموظف المكلف بخدمة عامة أو المستخدم في دوائر البرق والبريد والتلفون[1].

ويرى الباحث ضرورة إسراع المشرع العراقي إلى سد النقص التشريعي، بإضافة تعديل يجيز اللجوء إلى هذا الإجراء عند إجراء التحقيق في جرائم الجناية أو الجنح في الإثبات الجنائي بشروط وضمانات تكفل حق المجتمع والفرد في الحياة الخاصة، مع ضرورة تجريم تسجيل الصوت إذا تم خارج الإطار القانوني، والشروط والضمانات تجنبا لسوء إستعمال هذه الإجراءات.

الفرع الثاني

الوسائل المرئية الإلكترونية

عرف الفقه الجنائي الصورة بأنها: إمتداد ضوئي لجسم الإنسان، وهي تمثل فكرة أو دلالة للإشارة إلى شخصية صاحبها، ولا تشكل فرقاً عندما تكون الصورة على حقيقتها، أم دخلت عليها بعض التغيرات . كما عرفت الصورة بأنها: محاكاة للجسم البشري أو جزء منه[2]، وأيضاً أورد المشرع

(1) - سهيل محمد العزام، الوجيز في جرائم الانترنت، المكتبة الوطنية ، الاردن، ط 1، 2009 ، ص 63.
(2) - علي نعمة جواد الزرفي، المصدر السابق، ص 131.
(1) – ينظر: المادة (328) من قانون العقوبات العراقي رقم 111 لسنة 1969 المعدل.
(2) - د. محمود نجيب حسني، سرح قانون العقوبات، القسم الخاص، دار النهضة العربية، 1978، ص 776.

العراقي مفردة التصوير في قانون أصول المحاكمات الجزائية العراقي رقم (23) لسنة 1971 المادة (70) منه (لقاضي التحقيق أو المحقق .....وأخذ تصويره الشمسي .....) وهنا يقصد بالتصوير الشمسي كل ما يمثل صورة الشخص، مهما كانت الوسيلة .

وأيضاً يعرف التصوير المرئي: هو تسجيل الإحداث تسجيلا متحركا على مادة إلكترونية قابلة لحفظ التصوير إذ يمكن إعادة مشاهدته أكثر من مرة بما يسهم في إثبات الجريمة أو نفيها عن المتهم أو المتهمين [1].

أما الموقف التشريعي من مشروعية التصوير كأحد وسائل الإثبات والتحقيق في الجريمة الإلكترونية فقد كان الموقف التشريعي المقارن له رأي مختلف في مدى مشروعية الدليل المتحصل من التصوير المرئي، فقد أنقسم التشريع بين مؤيدٍ للأدلة المتحصلة منها، وبين معارض لها[1]. ونجد أن التشريع الأمريكي أهتم بحماية الحياة الخاصة للأفراد في أغلب القوانين والتشريعات الأمريكية وهو بذلك قد واكب حركة التطور العلمي والتكنولوجي التي باتت فيها تلك الوسائل والتقنيات المتطورة تشكل فعلاً مضراً ويشكل خطراً للحق في الحياة الخاصة، فجاءت تلك التعديلات القانونية التي مست القوانين العقابية في تلك الدول، التي أقرت بهذا الحق كحق مستقل وجب حمايته جنائيا من أي إعتداء أو انتهاك قد يقع عليه، لذلك اتجهت التشريع الجنائي في امريكا لإضفاء حمايتها على حرمة الحياة الخاصة، على الرغم من وجود بعض التباينات في وجهة نظر المشرع لكل نظام قانوني، إذ شملت تلك الأفعال المجرمة والتي تُعد إعتداءً على الحق في الخصوصية بعدما شهدت المجتمعات تطور وسائل الاتصال وظهور تقنيات متطورة في نقل وتسجيل الصوت والصورة، فأصبح من الضروري قانوناً تجريم تلك الإعتداءات على حرمة الحياة الخاصة، بإستعمال أجهزة التنصت والتجسس المتطورة[2].

أما (المشرع الفرنسي) فقد اتجه نحو حماية الحياة الخاصة من وسائل التجسس عليها، مما دعا المشرع لوضع نصوصٍ خاصة، إذ جرم المشرع الفرنسي في المادة (368) من قانون العقوبات القديم فعل الحصول على الحديث والتقاط الصور والفيديو دون موافقة صاحب الشأن، وقد نصت المادة المذكورة سلفاً على أنه: يعاقب بالحبس من شهرين إلى سنة وبغرامة من 2000 إلى 50,000 فرنك، أو بإحدى هاتين العقوبتين كل من إعتدى عمداً على الحياة الخاصة للآخرين : 1- بالتنصت أو

(1) - علي نعمة جواد الزرفي، المصدر السابق، ص 136.
(1) - د. رامي متولي القاضي، الدليل الجنائي الرقمي في التشريع المصري، المصدر السابق، ص 212.
(2) - موسى مسعود ارحومة، قبول الدليل العلمي امام القضاء الجنائي، الطبعة الاولى، من غير دار نشر، 1999 ص 5150.

بالتسجيل أو بالنقل بواسطة أي جهاز كان، صادر في مكان خاص من شخص دون موافقته. 2- بالتقاط أو نقل بواسطة أي جهاز، صورة شخص في مكان خاص دون موافقته. ونجد أنه المشرع الفرنسي قد عدل هذا نص بالمادة (226) من قانون العقوبات الفرنسي الجديد ساري المفعول، وقد نصت المادة الجديدة على أنه: يعاقب بالحبس سنة وغرامة 300000 الف فرنك، كل من إعتدى بوسيلة أياً كانت على الحق في الحياة الخاصة للآخرين: 1- بالتقاط أو بالتسجيل أو بنقل بدون موافقة صاحب الشأن وكان الإعتداء في مكان خاص. وواضح أن هذا النص جعل التصوير جريمة معاقب عليها متى تم التصوير في مكان خاص بغير رضا صاحب الشأن بما يجعل من الدليل المتحصل عليه عن طريق هكذا تصوير دليلا غير مشروع[1].

ويرى الباحث أن وسائل التصوير مهما كان نوعها فهي قد تساعد في كشف الغموض والحقائق لما لها من دور كبير وأثر في إجراءات التحقيق والإثبات الجنائي، ولكن من خلال إقرار مجموعة من الضمانات التي توفر الحماية للحياة الخاصة من التعدي عليها بحجة كشف الحقيقة، وهذا ما نلاحظه في أغلب التشريعات الجنائية الدولية والإقليمية من تقنينها للدور المؤثر لوسائل التصوير ومدى حجية الأدلة التي تقدمها مثل هذه الأجهزة التقنية الحديثة. وعلى المشرع العراقي أن يواكب التطور التكنولوجي الذي يعيشه البلد في ظل العولمة والانفتاح الذي يعيشه المجتمع، وأن يحرص على إدراج ما يستجد ويستحدث من الجرائم الإلكترونية، لكون العراق من الدول التي تعتمد القوانين التقليدية لمكافحة جرائم الإنترنت والتكنولوجيا، ولم يتم تشريع أي قانون جديد كما فعلت دول (أوربا) وبعض الدول العربية، وهذا يمثل قصوراً تشريعياً ويسبب خللا في الامن الإجتماعي والأقتصادي والسياسي. فالجريمة الإلكترونية لا يمكن وصفها على أنها جريمة عادية لكن بثوب جديد، وانما هي جريمة جديدة مستحدثة ترتكب بكل سهولة وعن بعد ولا تتطلب أي مجهود بدني، فهي تستهدف مصلحة معنوية لا مادية، لكونها تستهدف معلومات وأشياء غير محسوسة، وهذا يعني أن محاولة تطويع النصوص الجنائية التقليدية على الجرائم الإلكترونية، أمر لا يمكن الإعتماد عليه فقد ظهر هناك قصور تشريعي واضح في أغلب التشريعات المقارنة، إزاء الإحاطة بهذه الجرائم التقنية الحديثة.

(1) - علي نعمة جواد الزرفي، الجريمة المعلوماتية الماسة بالحياة الخاصة، المصدر السابق ، ص 136.

المبحث الثاني

مظاهر تأثير التطور التكنولوجي على مرحلة المحاكمة

التنظيم القضائي، لم يكن بمعزل عن التطور التكنولوجي والتقني الذي يعيشه العالم في الوقت الحاضر، إذ أدى هذا التطور الأخير إلى تطور التعاملات، سواء على الصعيد الحكومي الاداري، أم القضائي، مما أدى إلى تسخير هذا التطور التكنولوجي للإستفادة منه في مجال تطوير القضاء وتسهيل المهمة على المتقاضين والمحامين وحتى القضاة، عن طريق إنشاء منظومة التقاضي الإلكترونية، ما دفع بالمشرعين في بعض الدول، إلى تشريع قوانين تواكب التطور التكنولوجي، تنظم عمل المحاكم والتقاضي الإلكتروني بطريقة سهلة وميسرة،

وتأسياً على ما تقدم سنقسم دراستنا في هذا المبحث إلى مطلبين. نخصص المطلب الاول لبحث التنظيم القانوني لمرحلة المحاكمة الإلكترونية، أما المطلب الثاني فيكون لدراسة تقنيات التقاضي عن بعد في ظل التطور التكنولوجي.

المطلب الأول

التنظيم القانوني لمرحلة المحاكمة الإلكترونية

إن شبكة الإنترنت ليس لها مقر في دولة معينة ولا شخص محدد، بل أنها توجد موزعة ومنتشرة على جميع أنحاء العالم، فهي تجمع عدد كبير من الشبكات مختلفة النوع والمصدر والوظيفة وترتبط بها الخطوط التلفونية، والبرامج الالكترونية من كل دول العالم، ولذلك فإن شبكة الإنترنت العالمية لا تخضع لقضاء محدد أو سيطرة دولة معينة، بسبب عدم وجود قانون جنائي معين أو رقابة أو سيطرة دولة معينة، بما يترتب على ذلك تعدد القوانين الجنائية التي تنطبق عليها بتعدد الدول المرتبطة بها باعتبار القرار الجنائي يتعلق بسيادة الدولة، وهنا تكمن المشكلة الأساسية التي تتعلق بشبكة الإنترنت العالمية تكمن في تدويل الجرائم المرتكبة من خلال هذه الشبكة، كما لو تم نشر رسالة من خلال هذه الشبكة فإنها تمر عبر عدد من الدول مع غياب رقابة جهة معينة على هذه الشبكة وعدم وجود قانون محدد يحكمها، وأن القاعدة الأساسية المطبقة في الوقت الحاضر هي أن التشريع الجنائي الدولي يطبق بالنسبة لكافة الجرائم التي ترتكب على اقليمها بغض النظر عن جنسية مرتكبيها أي سواء كانوا وطنيين أم اجانب، فالدولة هي المختصة بالمحافظة على الامن في كافة أنحاء الاقليم التابع لها وهو ما يطلق عليه مبدأ إقليمية القانون الجنائي. وعلى ضوء ذلك سنحاول بحث مسألة متطلبات المحاكمة الالكترونية في الفرع الاول، ونخصص الفرع الثاني للبحث في موضوع القانون الواجب التطبيق

على الجرائم الإلكترونية، أما الفرع الثالث فسيكون للبحث في موضوع ضمانات المحاكمة الإلكترونية.

الفرع الأول

متطلبات المحاكمة الإلكترونية

إن فكرة المحكمة الإلكترونية تستلزم ابتداءً نظاماً حاسوبياً يدير عمل كل محكمة على حدة، وربط المحاكم معا لتؤدي عملها عبر الوسائل الإلكترونية ولتقوم قواعد البيانات مقام الوثائق والملفات الورقية على نحو يتيح سرعة الوصول إلى المعلومات وسرعة إسترجاعها والربط فيما بينها[1]. الأمر الثاني: أن المتقاضي أو المحامي عند رغبته في إقامة الدعوى بطريقة إلكترونية يقوم بإرسال عريضة الدعوى عبر البريد الإلكتروني الخاص بكل محكمة من خلال موقع إلكتروني مخصص لهذا الغرض متاح (24) ساعة يومياً طيلة أيام الأسبوع، إذ يتم استلام هذه المستندات بمعرفة الشركة القائمة على إدارة هذا الموقع، ثم تقوم بإرساله إلى المحكمة المختصة فيتسلمه الموظف المختص بقلم المحكمة ويقوم بفحص المستندات والتأكد من هوية المستخدم ثم يقرر قبول هذه المستندات أو عدم قبولها ويرسل للمتقاضي رسالة إلكترونية يعلمه فيها بإستلام المستندات وطبيعة الإجراءات والقرار الصادر بشأنها[1].

ولغرض تطبيق إجراءات التقاضي عن بعد لابد من وجود محكمة تعمل بوسائل إلكترونية يباشر من خلالها مجموعة من القضاة نظر الدعوى والفصل بها بموجب تشريعات تخولهم مباشرة الإجراءات القضائية بتلك الوسائل التقنية، بإعتماد تقنيات فائقة في الحداثة لملفات الدعاوى والتي سيتم تدوين الإجراءات القضائية من خلالها، أي بمعنى برمجة الدعوى الكترونياً وحوسبة الدعوى لتكتمل منظومة هذا النظام[2].

فتطبيق مشروع التقاضي عن بعد هي إحدى اتجاهات السياسة الجنائية وتمثل جانب من مظاهر التطور التكنولوجي والتقني، وعلى ضوء ذلك فلا بد من وجود تشريعات وبيئة تهيأ لإنجاح هذا المظهر الذي يمثل دار العدالة، وتخفيف المعاناة عن الافراد والمجتمع، ومثال على ذلك نجد أن وزارة العدل السعودية قد اسست جملة من الإجراءات إلكترونية إذا أتاحت لجميع القضاة خاصية الدخول على أنظمة المحاكم والاطلاع على القضايا والتعامل معها عن بعد، ووفرت لجميع المتعاملين القضائيين إمكانية رفع الدعوى إلكترونياً ومتابعة إجراءاتها عن بعد بإستخدام الهواتف الذكية

(1) - د. جابر فهمي عمران، لوجستيات التقاضي، المكتب الجامعي الحديث، 2022 ، ص 103.
(1) - د. اشرف جودة محمد ، المصدر السابق ، ص 33.
(2) - د. هادي حسين عبد علي، نصيف جاسم محمد، مفهوم التقاضي عن بعد ومتطلباته، المصدر السابق، ص299 .

والحواسيب وقامت بأرشفة قطاع العدالة إلكترونيا[1]، ووفرت تطبيق الإتصال المرئي والمسموع عن بعد من خلال (40) محكمة وإدخلت هذا النظام إلى السجون ضمانا لعدم تنقلهم لمسافات طويلة إلى الجهات القضائية[2]، وبتاريخ (7 / يونيو / 2020) بدأ لأول مرة إستخدام تقنية التقاضي الإلكتروني (المحكمة الإلكترونية) عن طريق نوعين من التقاضي: (الترافع الإلكتروني، والذي يتمثل تبادل المذكرات والترافع وإيداع أوراق الدعوى، بالإضافة إلى النوع الثاني من التقاضي، وهو جلسة المرافعة عبر الإتصال المرئي)[3]. وتُعد محكمة جدة أول جهة قضائية تعمل بنظام التقاضي الإلكتروني عن بعد تستخدم النظام الشامل إبتداءً من أستلام عريضة الدعوى ودخول المدعي إلى موقع المحكمة لتسجيلها إلكترونياً وسير إجراءات التقاضي وصولاً إلى إصدار الحكم، هذا في القضاء العادي، وفي مجال القضاء الإداري فقد تم إطلاق البوابة الالكترونية لديوان المظالم التي تقدم مجموعة من الخدمات الإلكترونية والتي منها نافذة المعرفة، والتي تعد قاعدة بيانات تحتوي على مختلف الانظمة والقوانين والقرارات، وكل ما يحتاج له القضاة والمحامين والخصوم في سير الدعوى أمام المحكمة الالكترونية[1]. أما في (فرنسا) فقد حصل إتفاق بين وزارة العدل والمجلس الوطني الفرنسي لنقابة المحامين فيما يتعلق بالإتصالات الإلكترونية بين المحاكم والمحامين بتاريخ 2007/7/28 ووضعت شبكة إتصال بين الطرفين إذ مكن هذا النظام المحامين من فحص الملف ونقل المستندات والاطلاع على جدول الجلسة وإرسال واستقبال الرسائل الإلكترونية المتعلقة بالوثائق والإجراءات مع كتابة الضبط، وهذا في المسائل المدنية والجزائية[2]، كما تجهز مرفق العدالة هناك بكاميرات لنقل جلسات المحاكمة بالصوت والصورة من خلال استخدام تقنيات المحادثة المرئية عن بعد في التحقيق والمحاكمة على نطاق واسع وفقا للمادة 71/706 من قانون الإجراءات الجنائية الفرنسي المعدل بقانون رقم (1436) لسنة 2009 الذي أقر عند إستدعاء ظروف القضية أو التحقيق ، لذلك أو لقيام حالة الضرورة لاستخدام تقنية المحادثة المرئية المسموعة، سماع الشخص وإستجوابه ومواجهته بأشخاص آخرين باستعمال تلك التقنية وتكون كل تلك الإجراءات في محضر سمعي ومرئي، وجاء التعديل الأخير المعدل بالقانون (1636) لسنة 2016 مخولاً إستعمالها لوكلاء الجمهورية وقضاة التحقيق سواء في التحقيق مع الشهود أو المحاكمة، أو المواجهة، أو سماع الخبراء، في فرنسا أو بينها وبين الدولة الأعضاء، للإتحاد الاوربي في التحقيقات الأوربية المشتركة

(1) - د. خالد ممدوح إبراهيم، إجراءات التقاضي عن بعد، المصدر السابق ، ص 57.
(2) - د. صفاء اوتاني، المصدر السابق، ص 195.
(3) - حسام فاضل حشيش، المصدر السابق ، ص 115.
(1) - د. عمارة عبد الحميد ، المصدر السابق، ص 587 ، وكذلك : د. اشرف جودة محمد، المصدر السابق ، ص43.
(2) - د. عصماني ليلى، نظام التقاضي الإلكتروني آلية لإنجاح الخطط التنموية، مجلة المفكر، العدد الثالث عشر، جامعة وهران 2، 2016، ص221.

في إطار المساعدة القضائية في المسائل الجزائية المتبادلة بينهم وهذا إلتزامٌ بالإتفاقية الأوروبية الجديدة للمساعدة القضائية في المسائل الجزائية المقررة من طرف مجلس الإتحاد الأوروبي بتاريخ (30 نوفمبر 2000)[1].

الفرع الثاني

القانون الواجب التطبيق على الجرائم الإلكترونية

المحكمة الجنائية المختصة في الجرائم الإلكترونية يقصد بها (تلك المحكمة التي تتمتع بولاية قضائية قد خولت إياها بموجب أحكام القانون، وذلك للنظر والفصل في الدعوى التي ترفع إليها)، وتعني هذه الفكرة في المقام الأول، أن للقضاء ولاية قضائية خاصة به دون سواه فيما يتعلق بكل الأمور ذات الطبيعة القضائية وله وحده دون سواه سلطة تحديد ما إذا كانت القضية المطروحة أمامه للبت فيها تقع ضمن أختصاصه وفقا لما ينص عليه القانون أم لا. وتعني هذه الفكرة في المقام الثاني، أنه لكل فرد الحق في أن يحاكم أمام محاكم عادية أو هيئات قضائية تستخدم إجراءات قانونية وضعت على نحو صحيح، وأنه لا ينبغي إنشاء هيئة قضائية لا تستخدم مثل هذه الإجراءات لتمارس الولاية القضائية الخاصة بالمحاكم أو الهيئات القضائية العادية، ويمكن القول إن المحاكم الجنائية لا تكون مختصة بنظر الدعوى المرفوعة اليها إلاّ إذا كانت مختصة بالنسبة لشخص المتهم من حيث نوع الجريمة المسندة إليه، ومن حيث المكان الذي إرتكبت فيه الجريمة أو المكان الذي وجدت فيه جثة المجنى عليه أو المال الذي ارتكبت الجريمة من أجله[1].

تبرز أهمية تحديد القانون الواجب التطبيق والمحكمة المختصة في مجال الجرائم الإلكترونية، فقد أخذ هذا الموضوع مجالاً واهتماماً كبيرين من قبل الباحثين والفقهاء لما تتميز به الجريمة الإلكترونية لكونها من الجرائم التي تتميز بأنها عابرة للحدود، ولكون أغلب الأفعال المكونة للجريمة ترتكب خارج الحدود، أو أنها تمر عبر شبكة الإنترنت العالمية، وهو ما يبرز أهمية اختبار مدى ملائمة قواعد الاختصاص في القانون الواجب التطبيق[2].

وعلى ضوء ذلك سنحاول دراسة هذا الموضوع من خلال بيان توضيح المبادئ التي تحكم تطبيق القانون من إذ المكان. وتوضيح مفهوم مبدأ إقليمية النص الجنائي، ومدى تطبيق مبدأ عينية النص

(1) - د. عمارة عبد الحميد ، المصدر السابق ، ص 586.
(1) - أمير فرج يوسف ، المصدر السابق، ص 421.
(2) - د. محمد حسين منصور، المسؤولية الالكترونية، دار الجامعة الجديد، الاسكندرية، 2007، ص 135.

الجنائي، وبيان فعالية تطبيق مبدأ شخصية النص الجنائي، ولهذا المبدأ (شخصية النص الجنائي) وجهان أحدهما إيجابي والآخر سلبي [1].

وتعد مسألة الأختصاص القضائي بالجريمة الإلكترونية من المشكلات الحديثة التي تواجه الإجراءات، وتواجه أيضاً سلطات إنفاذ القانون (التحري، التحقيق، القضاء)، وذلك نتيجة الثورة التكنولوجيا في وسائل الاتصالات الحديثة، وظهور شبكة المعلومات العالمية (الإنترنت) والتي يترتب عليها سهولة الاتصال وتبادل المعلومات والانتقال عبر شبكات الإنترنت بين الأفراد، وليس فقط على النطاق الإقليمي بل على المستوى الدولي والعالمي.

أولا: الاختصاص القضائي في الجريمة الإلكترونية بحسب المبدأ الإقليمي : ويقصد بهذا المبدأ أنه حق تطبيق القانون أو مبدأ حق العقاب لقانون محل الفعل غير المشروع، تطبق بمقتضاه الدولة قانونها الوطني على كافة الجرائم التي ترتكب على إقليمها. بغض النظر عن جنسية مرتكبيها سواء كان مرتكب الجريمة مقيماً على اقليم الدولة بصفة دائمة أو عارضة، بصرف النظر عن طبيعة المصلحة محل الاعتداء[1]، لذا يُعد مكان وقوع الجريمة هو نقطة البداية لمعرفة مدى تطبيق قانون العقوبات من حيث المكان، ووفقا لمبدأ الإقليمية، ينعقد اختصاص القضاء الوطني وسلطة التحقيق كما في حالة نشر الصور الإباحية أو العبارات التي تحث على الكراهية والعنصرية أو التي تنشر على شبكة الإنترنت بصرف النظر عن الدولة التي صدر منها هذا العمل الإجرامي طالما يمكن أن تتحقق النتيجة الاجرامية على الإقليم الوطني[2]، أما في حالة بث الفيروسات التي تتم بإدخال الجاني فيروساً إلى نظام الحاسوب متصل بشبكة الإنترنت العالمية، وهو في إقليم دولة أخرى، فينتقل أثره الاجرامي ليصيب العديد من الأجهزة في شتى أنحاء العالم، وتتحقق النتيجة الاجرامية في كثير من الدول، ليختص بها القضاء الوطني سلطة التحقيق في كل دولة تتحقق فيها أحد العناصر المكونة للسلوك الإجرامي، أو تحقق فيها النتيجة الاجرامية. ويرتكز مبدأ الإقليمية و تطبيق القانون على إعتبارات موضوعية وإجرائية تهدف إلى تحقيق أهداف العقاب وتطبيق قانون عقوبات الإقليم ذاته الذي وقعت فيه الجريمة، وذلك لسهولة الوصول إلى الأدلة وسهولة إجراءات التحقيق والمحاكمة في مكان إرتكاب الجريمة وتحقيق الردع العام وتحقيق التوازن داخل المجتمع الذي اختل بوقوع الجريمة[3].

---

(1) - د. محمد محمود بدير ، المصدر السابق، ص 197.

(1) - أمير فرج يوسف ، المصدر السابق، ص 382 .

(2) - أمير فرج يوسف الاثبات الجنائي الجريمة الإلكترونية و الاختصاص القضائي المصدر السابق، ص386 وما بعدها .

(3) - يراجع: د. محمد كمال شاهين، المصدر السابق، ص 183 وما بعدها.

وأخيراً نقول إنّ مبدأ الإقليمية يقوم على أساس مكان وقوع الجريمة أو أحد عناصرها المادية وهذا المبدأ يبدو لنا انه غير ملائم للجريمة الإلكترونية والسبب يعود لطبيعتها غير المادية من جهة ومن جهة أخرى لصعوبة اكتشافها و تحديد مكان وزمان وقوعها.

ثانيا : الأختصاص القضائي في الجريمة الإلكترونية بحسب مبدأ العينية: وفقا لهذا المبدأ فان تطبيق قانون العقوبات يعني تتبع التشريع العقابي الوطني لجرائم محددة بعينها تمس مصالح الدولة الجوهرية وأمنها ولو وقعت خارج اقليم الدولة، لذلك يجد مبدأ العينية اساسه في فكرة الخطر الاجتماعي الذي يحدثه المجرم بفعلة ضد مصالح الدولة، اذ قد لا تعني الدولة التي ارتكبت الجريمة على إقليمها بملاحقة من ارتكب الجريمة، مما يشجع على ارتكاب تلك الجرائم، فكان من اللازم أن يتقرر للدولة حق ملاحقة كل جريمة تمس المصالح العامة للدولة وان وقعت خارج اقليمها الوطني، بصرف النظر عن جنسية مرتكبيها، فالعبرة بطبيعة الجريمة لا بمكان وقوعها، وذلك للحفاظ على أمنها ومصالحها. وتأسيساً على ما تقدم فإن الاختصاص وفقا لمبدأ العينية ينعقد لسلطات التحقيق والقضاء الوطني بالجرائم الإلكترونية، أو التي ترتكب عن طريق شبكة الإنترنت العالمية مثل السعي أو التخابر لدى دولة اجنبية والمعاقب عليها في أغلب التشريعات المقارنة، كما ينعقد الاختصاص لسلطات التحقيق حتى لو كان الشخص الذي قام بالتخابر أو إفشاء الاسرار أو الموقع الذي إستخدمه موجود في الخارج وبصرف النظر عن جنسية الجاني[1].

فهذا الاختصاص في الواقع يواجه العديد من الصعوبات ترجع بالأساس إلى طبيعة وخصائص الجريمة الإلكترونية إذ لا تظهر مادياتها بوضوح، كما أن الفاعل يبقى مجهولا بالإضافة إلى تعدد وتنوع الأنظمة القانونية في العالم واختلافهم، ما يترتب عليه البطء والتعقيد طول مدة الاجراءات.

ثالثا : الأختصاص القضائي في الجريمة الإلكترونية بحسب مبدأ الشخصية: ووفقا لهذا المبدأ يتم التحقيق ومحاكمة كل من إرتكب فعلاً مجرماً حتى وإن حصل إرتكاب الفعل المجرم خارج القطر، فعلاً يُعد جناية أو جنحة في هذا القانون يعاقب بمقتضى أحكامه إذا عاد إلى دولته وكان الفعل معاقبا عليه بمقتضى البلد الذي إرتكب فيه. ويوجد لمبدأ الشخصية لتطبيق القانون وجهان الأول إيجابي والآخر سلبي، ويقصد بالوجه الإيجابي تطبيق النص الجنائي على كل من يحمل جنسية الدولة ولو ارتكبت الجريمة خارج اقليمها. أما الوجه السلبي لتطبيق مبدأ الشخصية وقانون العقوبات، فيعني تطبيق النص الجنائي على كل جريمة يكون المجني عليه فيها منتميا إلى جنسية الدولة حتى لو كان الجاني أجنبياً وإرتكب الجريمة خارج اقليم الدولة، ويعد ذلك حماية لحقوق ومصالح مواطني الدولة

(1) - د. محمد كمال شاهين، المصدر السابق، ص 194.

التي تأخذ بمبدأ الشخصية في وجهه الإيجابي والسلبي[1]. وتطبيق مبدأ الشخصية على الجريمة الإلكترونية فإنه يمكن تطبيقه بوجهه الإيجابي كما لو قام الجاني بالتخطيط والإعداد للجريمة التي يمكن أن يبدأ في تنفيذها بعد أن غادر القطر الموجود به، وذلك عن طريق البرامج محددة الوقت كإستخدام القنابل الموقوتة كما في اتلاف المعلومات. كما يمكن تطبيق مبدأ الشخصية في وجهة السلبي طبقا لنص المادة (113-7) من قانون العقوبات الفرنسي الجديد يتم حماية الفرنسي المتضرر من جريمة تقليد مصنفة الفني وهو خارج الدولة الفرنسية، وأما عن تطبيق مبدأ الشخصية وفقا للقانون الأمريكي نجد أنه يتماشى والطبيعة الخاصة للجريمة الإلكترونية اذ يعد الوجود المعنوي للجاني على الإقليم الامريكي سببا لانعقاد الإختصاص وفقا لمبدأ الشخصية[2]، وأما الإتفاقية الأوروبية للجريمة الإلكترونية لسنة 2001 وذلك في محاولة منها للحد من مشكلة تنازع الاختصاص، إذ نصت الفقرة الخامسة من المادة (22) من الإتفاقية، على أنه "في حالة مطالبة أكثر من دولة من الدول الاطراف بالاختصاص القضائي بشأن جريمة من الجرائم الإلكترونية والتي تقرها الإتفاقية، إذ تقوم الدول الاطراف المعنية متى كان ذلك ملائما، بالتشاور بغرض تحديد الاختصاص القضائي الأكثر ملائمة للمحاكمة[1].

والملاحظ أن هذا المبدأ يعتمد بصفة أساسية على الجاني من حيث الكشف على هويته، ومن ثم التعرف على جنسيته وهذه المعلومات تعد صعبة وعسيرة في الجرائم الإلكترونية من إذ صعوبة إستعمال التشفير والأسماء المستعارة بالإضافة إلى اللغة الصعبة والمعقدة وكذلك يكون الفعل غير معاقب عليه في بعض الدول، لذلك نرى بأنه يجب أن يكون هناك قانون جنائي دولي على غرار القانون الدولي الخاص.

رابعا: انتفاء المبادئ التقليدية أمام خصوصية الجريمة المرتكبة عبر الإنترنت: فيما يخص إقليمية القانون وعينية النص الجنائي وشخصية النص الجنائي . يترتب على عدم تبعية شبكة الإنترنت لأي جهة أو شخص محدد لعدم وجود مقر لها في دولة معينة تخضع لرقابتها أو سيطرتها ونظرا لعدم وجود قانون جنائي موحد يحكم هذه الشبكة (الإنترنت) فإن القوانين الجنائية التي تنطبق عليها تتعدد بتعدد الدول المرتبطة بها باعتبار أن القانون الجنائي يتعلق بسيادة الدولة[2]، والاصل في القوانين

(1) - د. خالد حسن أحمد لطفي، القانون الواجب التطبيق على الجريمة المعلوماتية، دار الفكر الجامعي، الاسكندرية، 2019 ، ص 108.
(2) - المصدر نفسه، ص 131.
(1) - د. محمد كمال شاهين ، المصدر السابق، ص 196.
(2) - محمد لموسخ ، تنازع الاختصاص في الجرائم الالكترونية، بحث منشور، مجلة دار المنظومة، جامعة قاصدي مرباح، كلية الحقوق والعلوم السياسية، العدد 2، 2009 ، ص 148.

وهو إقليمية القانون الجنائي فإذا ما إرتكب شخص ما جريمة عن طريق الإنترنت بداخل الدولة وتحققت نتيجتها في الدولة ذاتها، فالقانون الواجب التطبيق بلا منازع هو قانون هذه الدولة بغض النظر عن جنسية الجاني أو المجنى عليه فقط يكفي أن تكون هذه الجريمة على إقليم الدولة سواء كان إقليماً برياً أو بحرياً أو جوياً، ويترتب على تطبيق مبدأ إقليمية قانون العقوبات عدم أهتمام الدولة إلاّ بالجرائم التي تقع على إقليمها فلا يمتد إلى ما يرتكب خارجه من جرائم ولو كان مرتكبوها من رعايا هذه الدول غير أن هذه النتيجة قد لا تتفق مع حماية مصالح الدولة خاصة فيما يتعلق بالجرائم التي ترتكب عبر الإنترنت، وذلك راجع إلى البعد الدولي والعالمي لنشاط الشبكة العالمية (الإنترنت) إذ يضع دول مختلفة في حالة اتصال دائم والبيانات والمعلومات التي يتم إدخالها وتحميلها على الشبكة تنتشر في ثوان معدودة في كل الدول المرتبطة بها، إذ تكون متاحة لأي مستخدم في تلك الدول، وكذلك الأمر بالنسبة لمبدئي عينية وشخصية النص الجنائي اللذين لا يمكن تطبيقهما في هذا النص في هذا النطاق فإذا كان هذين المبدئين وضعا لكي يغطيا القصور الذي يتميز به مبدأ إقليمية النص في الجرائم تقليدية، فالأمر غير ذلك في الجرائم المرتكبة عبر الإنترنت خاصة في ظل عالمية الشبكة إذ إن السلوك في هذه الجريمة يمر عبر عدد من الدول، الشيء الذي يخلق أشكالا كبيرا في تحديد القانون الواجب التطبيق نظرا لاختلاف تشريعات الدول وعدم وجود اتفاقيات دولية أو اقليمية، فهناك دول تأخذ بمبدأ الإقليمية وأخرى بمبدأ العينية ودول أخرى تأخذ بمبدأ الشخصية للنص الجنائي، الامر الذي يثير نزاع فيما بينها على القانون الواجب التطبيق فكل دولة ترى لنفسها الحق بمتابعة الجاني[1].

خامسا: الاختصاص القضائي للجريمة الإلكترونية (المبدأ العالمي أو الشامل): أو كما يسميه بعضهم مبدأ عالمية القاعدة الجنائية، أو بنظام العقاب العالمي أو الاختصاص الشامل، إذ يُعد هذا المبدأ بمثابة علاج قانوني للحد من القصور التشريعي في مكافحة بعض الجرائم المعقدة، والإشكاليات التي تثيرها بعض الجرائم، بصفة عامة وعلى الجرائم الإلكترونية بصفة خاصة[2]. لذا فإن مبدأ (عالمية النص الجنائي) هو صلاحية تقررت للقضاء الوطني في ملاحقة ومحاكمة وعقاب مرتكبي أنواع معينة من الجرائم التي يحددها التشريع الوطني دون النظر لمكان إرتكابها، ومهما كانت جنسية مرتكبيها أو ضحاياها[3]، إذ إن فلسفة هذا المبدأ تتمثل في تمكين السلطات القضائية للدولة من ملاحقة الجرائم

(1) - د. محمد ممدوح مدير ، المصدر السابق، ص 198.

(2) - د. عبدالفتاح خضر ، النظام الجنائي ، الجزء الاول، المصدر السابق، ص 119.

(3) - د. احمد فتحي سرور، الوسيط في قانون الاجراءات الجنائية، الطبعة العاشرة، دار النهضة العربية، القاهرة، 2016، ص 110.

الخطرة والتي تمس الضمير العالمي بإلغاء الاشتراطات المتصلة بمبدأ الإقليمية لإيجاد طرق فعالة لمكافحة عدد من الجرائم ومنها الجرائم الإلكترونية[1].

وبالنظر إلى الطبيعة الخاصة للجريمة الإلكترونية بعدّها من الجرائم العالمية العابرة للحدود، يلاحظ انه بإمكان أحد الأشخاص ان يخطط لإرتكاب الجريمة الإلكترونية في دولة وينفذها في دولة أخرى، وتتحقق النتيجة الغجرامية في دولة ثالثة، أو عدد من الدول، ثم يغادر كل منها إلى دولة رابعة، والاخيرة هي التي تقبض عليه فيها، هذا فضلا عن أنه في الكثير من الأحيان يصعب تحديد مكان مرتكبي الجريمة عبر شبكة الانترنت كجرائم نشر الفايروسات وغيرها. إضافة إلى أنه يمكن إرتكاب الجريمة الإلكترونية من قبل المسؤولين الرسميين في دولة ما، أو بموافقة السلطات الرسمية مما يشكل إنتهاكا للمصالح العليا للدول، والتي تقف الضوابط التقليدية في مسألة الاختصاص عاجزة عن مجابهة مثل هذه الجرائم الإلكترونية الدولية، الأمر الذي تظهر معه أهمية تطبيق مبدأ العالمية للنص الجنائي، أو الأختصاص الشامل، وخاصة في مثل هذ الجرائم أو في حالة فرار الجاني إلى دولة أخرى أو عدم مقدرة سلطات الدولة على ملاحقة الجاني، لذلك فإن عولمة القانون الوطني يعد بمثابة العلاج القانوني في مثل هذه الحالات[1]، إلا أنه يوجد ثمة معوقات امام تطبيقه على الجريمة الإلكترونية يمكن أجمالها على النحو الأتي: يثير مبدأ العالمية، أو الأختصاص الشامل عند تطبيقه مسألة تنازع الاختصاص، وذلك على الرغم من أنه مبدأ العالمية هو أحد الحلول لها إلاّ أن تلك المشكلة تثور إذا تمسكت عدة دول بالاختصاص في إحدى الجرائم الإلكترونية إستنادا إلى مبدأ الإقليمية أو الشخصية (الإيجابي أو السلبي) أو المبدأ العيني مثل جرائم بث الفيروسات، إذ تختص الدولة التي صدر منها عملية البث وتخص الدولة التي تحققت فيها النتيجة[2]. وكذلك أن تطبيق مبدأ العالمية للنص الجنائي مرهون بضرورة وجود تماثل أو تطابق بين التشريعات العقابية في مختلف الدول، وهذا التماثل لم يحدث نظرا لاختلاف الأنظمة القانونية الجنائية التي تنتمي إليها التشريعات المختلفة. وأيضا عدم تبني العديد من الدول في تشريعاتها العقابية النص على الأخذ بمبدأ عالمية النص الجنائي[3].

---

(1) - أمير فرج يوسف ، المصدر السابق، ص 411.

([1])- ينظر: قرار مجلس القضاء الاعلى/ محكمة التمييز الاتحادية المرقم (31/الهيئة الجزائية/ 2021 تسلسل / 203) والذي يتضمن الحكم بتحديد الاختصاص المكاني لمحكمة التحقيق في الجريمة، وقد قضت محكمة التمييز بان تحديد اختصاص المحكمة يتحدد من خلال الفعل الذي ارتكبت به الجريمة او جزء منها او أي فعل متمم لها أو أي نتيجة ترتبت عليها. ونجد من خلال مضمون هذا الحكم ان المشرع والقضاء العراقي قد اخذ بمبدأ عالمية النص الجنائي او الاختصاص الشامل.

(2) - سهيل محمد العزام، الوجيز في جرائم الانترنت، المصدر السابق، ص 92.

(3) - د. محمد كمال شاهين، المصدر السابق ،ص 201.

ويرى الباحث أن أهمية هذا المبدأ ومدى ملائمته للجريمة الإلكترونية مستمدة من خطورتها من جهة، ومن طبيعتها من جهة أخرى، كونها سهلة الوقوع من أشخاص يحملون جنسيات مختلفة وتمتد عناصرها المادية وسلوكياتها الإجرامية بين أكثر من دولة، كذلك هذا المبدأ العالمي لتطبيق القانون يبقى عاجزا عن معالجة جميع القضايا في هذا الشأن ما لم يكن هناك تعاون دولي، كما أن الفقه يرى بوجوب الأخذ به ولذا أصبح من الضروري الأخذ بهذا المبدأ لمعاقبة الجاني في أي إقليم يتم فيه القبض عليه دون مراعاة لجنسيته ومكان إرتكاب الحريمة.

سادسا: معايير تحديد القانون الواجب التطبيق:

1- معيار الأختصاص المكاني: تعتمد أغلب التشريعات في تحديد الاختصاص المكاني اتباع ثلاث ضوابط هي مكان وقوع الجريمة أو محل إقامة المتهم أو مكان ضبط أو إلقاء القبض على المتهم، وفي حالة إجتماع أكثر من ضابط تكون المحكمة التي ترفع إليها الدعوى أولاً هي المختصة مكانيا بنظر الدعوى ويقصد في مكان إرتكاب جريمة، المكان الذي إرتكب فيه السلوك ليس الذي تتحقق فيه النتيجة، كون السلوك هو التعبير المادي عن إرادة مخالفة للقانون[1]. أما النتيجة فهي حدث خارجية يترتب عن السلوك. وينعقد الأختصاص وفقا لهذا المعيار للمحكمة التي يقع في نطاقها النشاط الاجرامي وليس مكان حصول النتيجة أو الآثار المترتبة عليها، بدعوى أن إتخاذ آثار الفعل كمناط لتحديد مكان وقوع الجريمة تكتنفه بعض الصعوبات. يمكن أجمالها في أنه معيار مرن وفضفاض، فضلا عن أن معيار حصول النشاط يكون أقرب إلى تيسير عملية الاثبات وجمع أدلة الجريمة وأن المحكمة التي لها ولاية نظر الدعوى تكون قريبة من مسرح الجريمة، بالإضافة إلى أن الحكم الذي يصدر في الواقعة يكون أكثر فعالية ويسهل معه ملاحقة الجناة[2]. وأيضا تثير هذه القاعدة بعض الصعوبات عند التطبيق، فبالنسبة للجرائم الوقتية لا تسبب صعوبة، لأنها ترتكب وتتم في لحظة واحدة، ولذلك تُعد من اختصاص المحكمة التي يقع الفعل في دائرتها، أما بالنسبة للجرائم المستمرة والتي تبقى قائمة ما بقي التدخل الإرادي من جانب الفاعل كجريمة حبس الأشخاص بغير حق أو اخفاء الأشياء المتحصلة من جريمة، يتحدد الاختصاص المكاني بالنسبة لهذه الجريمة بأي مكان قامت فيه حالة الاستمرار، أما الجرائم الشبيهة بالجرائم المستمرة بالنظر إلى ما يداخلها من عنصر زمني، ومثالها الإعتياد والجرائم المتتابعة وجرائم الشروع إذ يُعد مكان الجريمة كل محل يقع فيه فعل من أفعال الإعتياد أو التتابع أو البدء في التنفيذ. وأيضاً من ضوابط معيار الاختصاص المكاني لتطبيق النص الجنائي هو مكان إقامة المتهم المحل الذي يوجد فيه محل إقامته الفعلي أو الحكمي وموطن

(1) - رشاد خالد عمر، المصدر السابق، ص 112.

(2) - د. خالد حسن أحمد لطفي الدليل الرقمي، دار الفكر الجامعي، الاسكندرية، 2020 ، ص 78.

الاقامة الفعلي هو المكان الذي يقيم فيه المتهم ويسكنه أما (محل الاقامة الحكمي) فهو المكان القانوني الذي يقيم فيه الشخص عادة أو يتواجد فيه أو تعرف به سيرته وشؤونه. أما مكان إلقاء القبض على المتهم فهو غير المكان الذي يتم فيه توقيفه أو حبسه، الحق ان مكان التوقيف يُعد بمثابة مكان حكمي للمتهم لكن الأمر لن تكون له الأهمية القانونية طالما أن القانون يسوي بين مكان الاقامة ومكان القبض، ومكان ارتكاب الجريمة في تحديد الاختصاص المكاني لتطبيق القانون[1].

2- **معيار القانون الأكثر ملائمة:** يرى أصحاب هذا الإتجاه بأنه نظرا للطبيعة الخاصة للجرائم الإلكترونية والأضرار الناجمة عنها التي تمتد لتشمل أكثر من دولة واحدة، وأحيانا قد تتفاوت نسبة الضرر بين دولة وأخرى، يتوجب علينا القول بأنه يجب التوسع في تفسير قاعدة أختصاص المحكمة ليجعل الأختصاص لمحكمة الدولة الأكثر تعرضاً للضرر بشكل فعلي، ويعتمد هذا المعيار على عدة مبادئ لتحديد القانون الواجب التطبيق[2]، مع التركيز على مبدأ التخلي أو التنازل عن الاختصاص بخلاف ذلك، وإن جعل الاختصاص لقانون دولة ما لمجرد إمكانية الوصول إلى المعلومة من هذه الدولة أو تلك أصبح امراً غير كافٍ من الناحية القانونية، لإعلان اختصاص هذه الدولة أو تلك من التطبيقات القضائية، لذلك ما اعلنته إحدى محاكم ولاية نيويورك بعدم اختصاصها في قضية تزوير ماركات تجارية أقدم عليها موقع ويب، في ولاية ميسوري وعللت المحكمة قرارها بأن صلاحيتها لا تنشأ من داخل هذه الولاية، بل تنشأ فقط إذا لحق هذا الموقع ضرراً فعلياً ضمن نطاقها. ونلاحظ أن هذا المعيار أخذ بعين الإعتبار نقطة الإتصال المميزة والسلطة الفعلية، أي بأختصاص قضاء الدولة التي قانونها هو الأكثر تعرضا للإنتهاك بسبب فعل الجريمة[1].

3- **معيار الضرر المرتقب:** في ظل التطور التكنولوجي وظهور الشبكة العالمية (الإنترنت) ووجود العالم الأفتراضي، إذ تسري فيه مختلف المواد المعلوماتية دون إمكانية تحديد وجهتها وهذا العالم الأفتراضي لا يخضع لأي سلطة إقليمية، ومن ثم يترتب على هذه الحالة أن الضرر الذي تسببه الجريمة الإلكترونية يمكن أن يحدث في أي دولة تكون متصلة بالأنترنت، وهذا هو معيار الضرر المرتقب أو الأفتراضي . ونجد أن المجلس الأوروبي العدلي قدم تفسيرا خاصا بشأن مفهوم قاعدة اختصاص محل وقوع أو حدث الفعل الضار، وذلك بالتأكيد حق وقوع الضرر، ولكن مع اضافة قيد مهم في حالة لجوء المتضرر إلى المحكمة محل وقوع الضرر يقضي بحجب اختصاص هذه المحكمة إذا أثبت المدعي عليه أنه لم يكن قادرا على إثبات وقوع الضرر المرتقب بصورة معقولة، وان الفعل

---

(1) - غازي عبدالرحمن هيان الرشيد، الحماية القانونية من الجرائم المعلوماتية، أطروحة دكتوراه، الجامعة الاسلامية في لبنان، كلية الحقوق، 2004، ص 523 وما بعدها.

(2) - ينظر : رشاد خالد عمر ، المصدر السابق، ص 112 وما بعدها .

(1) - عبدالفتاح بيومي حجازي، مبادئ الاجراءات الجنائية في جرائم الكمبيوتر والانترنت، ط 1، دار الفكر الجامعي، الاسكندرية، 2006 ، ص 51 و 52.

أو الإمتناع كان من شأنه إحداث أو إنتاج ضرر مماثل في دولته[1]. ونجد في حيثيات هذا القرار أن المعلومات المنشورة في شبكة الإنترنت العالمية يمكن معاينتها من قبل جميع الدول الموصولة بها، ومن دون أن تكون موجهة بالضرورة محددة، ولكن طبيعة هذه الوسيلة الإعلامية الجديدة لا يجب ان ينتج عنها تطبيق لجميع القوانين الموجودة بل يجب أن نطبق معيار الضرر المرتقب على المسؤول عن المعلومات الضارة فيها وهذا المعيار لا يمكن اثباته، إلا من خلال إيجاد علاقة للقانون المختص مع مبدأ موضوعي وذلك بمعزل عن تذرع كل دولة باختصاصها المحتمل. وأول المعالم الموضوعية في الاختصاص هي محل تمركز الموقع الذي نشرت الأقوال أو المعلومات بواسطتها وهو أكيد ويمكن التحكم بخلاف مكان تلقيها الذي يبقى احتماليا، وقد وجد هذا المعيار طريقة للتطبيق في بعض الدول ومنها فرنسا، إذ أصدرت محكمة الإستئناف في باريس عام 1999 قرار عُدّ صراحة أن الطبيعة الخاصة لشبكة الإنترنت لا يجب أن تؤدي إلى تطبيق محتمل لجميع القوانين الموجودة، بل ان تطبيق القانون ذي الصلة مع مبدأ موضوعي هو إرتقاب المسؤول للمحتوى الضار الذي ينشره[1].

ونجد أن (التشريع الامريكي) قد عالج إشكالية تطبيق القانون الخاص بالجرائم الإلكترونية، وذلك من خلال تشريع قانون الإحتيال الإلكتروني وإساءة إستخدام الحاسوب، والذي يعرف بأنه قانون جنائي ومدني يحظر العديد من الأفعال المرتبطة بالحاسوب، ويوصف في بعض الأحيان بانه قانون مكافحة القرصنة، إن هذا القانون ذو نطاق واسع يشمل العديد من الجرائم الإلكترونية والتي يمكننا أن نصنفها إلى سبعة أصناف وهي:

1. الحصول على معلومات تتعلق بالأمن القومي من خلال الوصول غير المرخص به للحواسيب الرقمية ومشاركة أو إعادة هذه البيانات.
2. الحصول على معلومات معينة من خلال الوصول غير المرخص به للحواسيب الالكترونية.
3. التعدي على حواسيب حكومية.
4. القيام بسلوك الاحتيال الرقمي من خلال الوصول غير المرخص به لبعض الحواسيب.
5. التسبب بأضرار للحواسيب من خلال نقل برامج أو أوامر أو رمز.
6. التجارة بالرموز السرية أو ما شابهها من سبل الوصول غير المرخص به للحواسيب.

(1) - د. خالد حسن أحمد لطفي، الدليل الرقمي، المصدر السابق ، ص 83.
(1) - د. محمد ممدوح بدير ، المصدر السابق، ص 200.

7. تهديد بتسبب اضرار للحاسوب بناء الحصول على معلومات تم تحصيلها عليها من خلال الوصول غير المرخص به للحاسوب [1].

إن تلك الحالات التي ينطبق فيها القانون تجمع بينهم سمتان وهما: نشاط يقوم به الفرد بترخيص" أو "حينما يتجاوز حدود الترخيص". أما الحالة الثانية فعندما يتضمن وجود حاسوب[2].

ومن الادلة التي تستخدم لتحديد الموقع الجغرافي عن طريق الشهادة لإثبات وجود معيار التجارة بين الولايات وذلك في قضية (United States v. Szymuszkiewicz).[3] بينت وجود أدلة كافية لبيان وجود معيار اتصال الانترنيت بين الولايات[4].

أما فيما يخص الأختصاص القضائي وتطبيق القانون على الجرائم الإلكترونية التي تقع في الخارج، فنجد أن المشرع الامريكي تخلى عن اختصاصه القضائي، ما لم يقمْ دليل خلاف ذلك، فان قوانين الولايات المتحدة لا تنطبق على الجرائم التي تقوم خارج الولايات المتحدة. ويمكن أن يخالف القاضي هذه القرينة عند عرض دليل واضح يبين نوايا الكونجرس ان يمتد الاختصاص القضائي على الجرائم التي تقع خارج الولايات المتحدة Cotten[1] .v United States. وبينت المحكمة في سياق قضية (United States v. Gatlin)[2] بان الكونجرس له صلاحية أن يجعل للقضاء الاتحادي اختصاص على الجرائم التي تقع خارج الولايات المتحدة، حتى في حال ما إذا كان خارج الأختصاص الإقليمي للولايات المتحدة. ويترك تحديد هذه المسألة لنصوص التشريعات وذلك ما تبين في سياق قضية (Equal Employment Opportunity Comm. v Co., . Arabian American Oil)[3]

وحاول المشرع الامريكي أضافة بعض التعديلات في القانون الوطني الأمريكي لسنة 2001 وقد راجع الكونجرس نصوص المادة (1029) والمادة (1030)، بتعديل وأضاف ما يلي:

1- لو ارتكب أي شخص خارج الولايات المتحدة الأمريكية جريمة يمتد تأثيرها لداخل الولايات المتحدة الامريكية، فسيخضع للعقوبات من غرامات أو سجن في حال ما إذا:

---

(1) - Peter G. Berris, Cybercrime and the Law: Computer Fraud and Abuse Act (CFAA) and the 116th Congress, 2020, page 2.
(2) - Peter G. Berris, Op.Citt, page 4.
(3)- United States v. Szymuszkiewicz, 2009 WL 1873657, at *2 n.2 (E.D. Wis. 2009).
(4)- H. Marshall Jarrett & Michael W. Bailie, Op.Cit, Page 115.
(1)- United States v. Cotten, 471 F.2d 744, 750 (9th Cir. 1973).
(2)- United States v. Gatlin, 216 F.3d 207, 211 (2d Cir. 2000).
(3)- Equal Employment Opportunity Comm. v. Arabian American Oil Co., 499 U.S. 244, 248 (1991)

أ- لو استخدم جهازاً، صادراً، أو مملوكاً، أو في حيازة مؤسسة مالية أو مستخدماً لبطاقات ائتمان، أو مستخدماً حساباً، أو مؤسسة في داخل الولايات المتحدة الامريكية.

ب- الشخص الذي يقوم بنقل أو توصيل من أو خلال الأسواق، أو يستخدم أي مادة تُسهم في إرتكاب جريمة أو يرتكب من خلالها جريمة أو من قبيلها [1].

الفرع الثالث

ضمانات المحاكمة الإلكترونية

نجد أن المحكمة الأوروبية لحقوق الإنسان تطرقت لمناقشة الملفات المرتبطة بإستخدام المحاكم لتقنية التواصل عن بعد، إذ قررت هذه الأخيرة في مرات عدة بمناسبة بسط رقابتها على الفصل السادس من الإتفاقية الاوربية، إن اللجوء إلى تقنيات التواصل عن بعد في إجراءات المحاكمة لا ينقص بحد ذاته ضمانات المحاكمة العادلة ما دام أن الهدف من اللجوء إلى هذه الوسائل هدفاً مشروعاً، وان الوسائل المستعملة في ذلك لا تتعارض مع حقوق الدفاع، كما ذهبت المحكمة في بعض القضايا المرتبطة بالمافيا في إيطاليا، إلى أن مشاركة المتهم في المحاكمة عبر تقنية الفيديو (الاتصال المرئي) (videoconference)لا يشكل مساساً بضمانات المحاكمة العادلة خاصة عندما يكون انتقال المتهمين محفوفا بالمخاطر أو يكون الإجراء مبررا لحماية الشهود الضحايا المنصوص عليها في قوانين مستقلة. وفي قضية المواطن الروسي (sakhnovski) صرحت المحكمة الأوروبية لحقوق الإنسان على أن مشاركة المتهم في الجلسة عن طريق التواصل عن بعد لا تشكل في حد ذاتها تعارضا مع مبدأ المحاكمة العادلة ولا مع علنية المحاكمة، ولكن يجب التأكد من تمكن المتهم من متابعة مجريات الجلسة ومن إمكانية الاستماع اليه دون معوقات تقنية ومن تمكنه من التواصل مع محاميه بطريقة فعالة وسرية[1].

وتعتمد المحكمة الإلكترونية على حسابات الية ترتبط ببعضها عن طريق شبكات داخلية وترتبط هذه الشبكات في شبكة الإنترنت العالمية، عن طريق وسائل الإتصالات الحديثة ومن خلال هذه الشبكات يجري تداول بيانات المحكمة ومعلوماتها ومن هنا يعد نظام الحماية المعلوماتية والجنائية لهذه البيانات احد مقومات المحكمة الإلكترونية، إذ يحقق الثقة والفاعلية في نظام المحكمة، ويشجع

(1)- H. Marshall Jarrett & Michael W. Bailie, op.Cit, page 116.

(1) - د. هشام البلاوي، المحاكمة عن بعد وضمانات المحاكمة العادلة، مقال منشور، مجلة رئاسة النيابة العامة، العدد الاول، 2020، ص 26.

المتقاضين بالتعامل معها دون خوف أو تردد وتتمثل هذه الضمانات الخاصة بالمحكمة الإلكترونية من خلال الآتي[1]:

1- الحماية المعلوماتية: يقصد بالحماية المعلوماتية أو الفنية أو التكنولوجية إتخاذ التدابير والإجراءات عن طريق وسائل إلكترونية لتعطل عملية التعدي على بيانات المحكمة الإلكترونية ومعلوماتها مقاومتها، فضلا عن إمكانية الوصول إلى تحديد مرتكب هذه الأفعال، وتتمثل هذه الحماية من خلال عدة طرق، مثل تشفير بيانات المحكمة إلكترونيا ومعلوماتها المتداولة عبر الشبكة والتشفير يعني تحويل الكلمات المكتوبة إلى أرقام أو إلى صورة رقمية لا يمكن معرفة مضمونها إلى عن طريق فك شفرتها وذلك بأن يكون لدى المستقبل القدرة على إستعادة محتوى الرسالة، وذلك في صورته الأصلية قبل التشفير، من خلال إستخدام عملية عكسية لعملية التشفير[2]. وأيضاً تأمين خصوصية المعلومات على أن لا تستخدم المعلومات في غير الغرض المخصص به من صاحب المعلومة، بالإضافة لضرورة تأمين سرية المعلومات والوثائق وتحقيق الحماية لمحتوى البيانات ضد محاولة التغيير أو التعديل أو المحو خلال مراحل تبادل المعلومات والوثائق مع ضمان التحقق من شخصية المرسل أو المستقبل، ومن قبيل ذلك لا يمكن الحصول على تفاصيل الدعوى إلا من قبل أطرافها إذ على الجهة القائمة على إدارة الدائرة القضائية تحديد الأشخاص المصرح لهم بالدخول إلى نظام المعلومات والاطلاع عليها [1].

2- الحماية الجزائية ويقصد بها تجريم أي صورة من صور التعدي على بيانات المحكمة الإلكترونية ومعلوماتها وأموالها متى كان هذا التعدي يشكل جريمة في ذاته، ومن أهم صور التعدي الجزائي على بيانات ومعلومات المحكمة: يتمثل في التزوير للمعلومات ويقصد به تغيير الحقيقة في المحررات أو الوثائق الإلكترونية التابعة للمحكمة الإلكترونية، وهو ما يطلق عليه الوثيقة المعلوماتية، بنية إستعمالها[2].

3- حق المتهم في السكوت والاعتراض على تقنية الاتصال عن بعد، وتُعد هذه إحدى الضمانات المقررة في مرحلة الاستجواب والتي ضمنتها بعض القوانين للمتهم اثناء فترة الإستجواب، فحق الصمت هو

---

(1) - حازم محمد الشرعة، التقاضي الالكتروني والمحاكم الالكترونية، دار الثقافة للنشر، 2010، ص 61.

(2) - د. عمر عبدالمجيد مصبح، ضمانات المحاكمة العادلة على ضوء اعتماد تقنية الاتصال عن بعد في الاجراءات الجنائية في دولة الامارات، بحث منشور ، مجلة كلية القانون الكويتية العالمية، السنة السادسة، العدد 4، العدد التسلسلي 24، 2018 ، ص 404.

(1) - د. مروى السيد الحصاوى، وسائل التقاضي الالكتروني وحجية إجراءاته في ظل جائحة كورونا، بحث منشور، المجلة الجزائرية لقانون الاعمال، المجلد 2، العدد 1، 2021 ، ص 28.

(2) - د. صفاء اوتاني، المحكمة الإلكترونية، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 28 ، العدد الاول، 2012 ، ص 177.

حق مكفول في أغلب القوانين ، والغاية من ضمان هذا الحق، هو للسماح للمتهم لتنظيم شؤونه والتحضير لتقديم دفاعة كما يرغب[1].

4- علانية المحاكمة[2]، ومن الضمانات المقررة لأطراف الدعوى في المحاكمة الإلكترونية علانية إجراءات المحاكمة، بمعنى أن تنعقد جلسة المحاكمة بصورة علنية وشفافة وبإمكان أي شخص ان يطلع ويشاهد تفاصيل المحاكمة دون قيود، والحكمة من علانية المحاكمة هي ضمانة ضرورية لحماية حقوق المتهم، وايضا لضمان سير الاجراءات سيرا طبيعيا، ونجد أن هذه الضمانة قد اقرتها معظم الاتفاقيات الدولية والدساتير والتشريعات المقارنة[3]. ومنها الدستور العراقي الحالي لعام 2005، وتأكيد الاعلان العالمي لحقوق الانسان في المادة (1/10) على علانية اجراء المحاكمة.

ونجد أن المشرع الأمريكي قد عالج موضوع ضمانات التقاضي عن بعد خلال المدة التي حصلت فيها جائحة كورونا وبدأت محاكم في ولاية كاليفورنيا والعديد من الولايات الأخرى باللجوء للمحاكمات عن بعد. لأن الحاجات المحلية وممارسات المحاكم العليا قد شجعت على اتباع هذه الوسائل بكونها وسيلة ملائمة في ظل جائحة كورنا[1]، ومن ضماناتها: يجب أن تجرى المحاكمة بطريقة تراعي قواعد المحاكمة العادلة، وكذلك ألا تقوم المحاكم بإجراء أي تغيير إلاّ إذا أقتضى الحال ذلك، ويجب على المحاكم أن تلتزم بالقواعد الإجرائية ذاتها، بالإضافة إلى ضمان الاستماع لكل أطراف الدعوى من دون أي تمييز[2].

المطلب الثاني

تقنيات التقاضي عن بعد في ظل التطور التكنولوجي

كان للتقدم العلمي والتكنولوجي في العصر الحديث آفاق ضخمة أمام تقدم البشرية و تحقيق مستوى أفضل في الحياة وفي ظل التطور التكنولوجي والمعلوماتي أمام العالم أجمع، فقد أصبحت الأجهزة الإلكترونية عموماً وأجهزة الحاسوب بالأخص تلعب دورا مهماً في الحياة العصرية وفي الحياة القانونية فقد مكن انتشار الإنترنت أشكالاً غير محدودة للأعمال الإلكترونية وخاصة في ضوء التطورات التكنولوجية في تأمين الصفقات على شبكة الإنترنت وفي التثبت من أطراف العلاقة

(1) - حليمة خالد المدافع، التحقيق الإبتدائي بإستخدام تقنية الاتصال عن بعد، بحث منشور ، مجلة جامعة الشارقة للعلوم القانونية، المجلد 17، العدد 2، 2020، ص 184 .

(2) - ينظر : د. ضياء عبدالله جابر الاسدي، حق السلامة في جسم المتهم، المصدر السابق، ص 171. وينظر كذلك: سردار علي عزيز، ضمانات المحاكمة العادلة للمتهم، دار الكتب القانونية، مصر، 2010، ص 103 .

(3) - د. احمد فتحي سرور، الوسيط في قانون الاجراءات الجنائية، المصدر السابق، ص 1319.

(1)- Confress of chief Justice, Remote Hearings and Access to Justice During Covid-19 and Beyond, page 3.

(2)- Ibid, page 4.

والتعامل على كافة الاصعدة، وتوحيد مقاييس تبادل البيانات ويعد رفع الدعوى إلكترونيا و التي في طريقها للإنتشار من أهم هذه الأعمال الإلكترونية، وقد تم تطوير رفع الدعوى عن بعد في أماكن مختلفة ومنها المحاكم الفيدرالي الأمريكي مع وجود تطورات مشابهة في كل من الإمارات والسعودية والصين وغيرها، لذا سنقسم بحثنا في هذا المطلب إلى فرعين، نبحث مفهوم التقاضي عن بُعد في الفرع الاول، ونخصص الفرع الثاني لدراسة الأساس القانوني للتقاضي عن بعد.

الفرع الأول

مفهوم التقاضي عن بُعد

يعد موضوع التقاضي الإلكتروني من الموضوعات الحديثة التي ظهرت بعد التطور التكنولوجي وظهور شبكة الإنترنت التي يشهدها العالم، إذ اقحمت الوسائل التكنولوجية في كل المجالات حتى اصبحت سمة هذا العصر الذي يعرف باسم (تكنولوجيا المعلومات)، وبما ان القضاء يُعد من أهم المرافق العامة السيادية التي تقوم عليها الدولة، لذا كان الإجدر أن يكون للتكنولوجيا الحديثة دور في إدارة السياسة الجنائية لكل بلد متطور في مجال التكنولوجيا، وذلك من خلال الإجراءات القضائية والتي تركزت ولمدة طويلة في بعض البلدان المتمسكة بالكتابة التقليدية على المحررات الورقية والتي في أغلب المرات يتم بطلانها لإخلالها بالإجراءات الشكلية أو عدم مراعاتها، لذلك ظهرت الحاجة الماسة بضرورة الحاجة الماسة بضرورة اللحاق بركب التطور التكنولوجي في مجال العمل القضائي من خلال الإستفادة من تكنولوجيا الحاسوب والإنترنت والكتابة والتوقيع على المحررات الإلكترونية في الإجراءات القضائية[1].

فتعريف التقاضي اصطلاحاً: هو إلزام أمر لم يكن لازماً قبله. وهو فصل الحكم في تصريف أمور الأنام، وفي الدماء، والإبضاع والأموال، والحلال والحرام، وهو أيضاً بيان الحكم والالزام به، وفصل الخصومات[2].

أما تعريف التقاضي عن بعد: بعضهم شبه فكرة التقاضي الإلكتروني مع فكرة الحكومة الإلكترونية التي تعني الإنتقال من تقديم الخدمات والمعلومات إلى الأشخاص بشكلها التقليدي الورقي، إلى الشكل

(1) - د. رباح سليمان خليفة دور التقاضي الإلكتروني في الحد من التضخم الاجرائي، مجلة كلية القانون للعلوم القانونية والسياسية، المجلد 10 ، العدد 39 ، 2021 ، ص 529.

(2) - د. ايمان بنت محمد بن عبد الله القثامي، التقاضي عن بعد، دراسة فقهية تطبيقية على النظام السعودي، بحث منشور، مجلة علوم الشريعة والدراسات الإسلامية، العدد 84 ، مارس، 2021، ص 978.

الإلكتروني عبر الإنترنت فهي عبارة عن تطوير لأداء نظام القضاء، وهي بلا شك وسيلة فاعله للتطوير من خلال اختصار الزمن ضمن الإستراتيجيات الجديدة للتعامل مع الوقت[1]. فالتقاضي عن بعد هو: (عملية نقل مستندات التقاضي الإلكتروني إلى المحكمة عبر البريد الإلكتروني إذ يتم فحص هذه المستندات بواسطة الموظف المختص وإصدار قرار بشأنها بالقبول أو الرفض، وإرسال إشعار إلى المتقاضين يفيد علما بما تم بشأن هذه المستندات)[2]. وأيضا عرف التقاضي عن بعد بأنه: (محاكمة وفق المتطلبات القانونية والإجرائية لأطراف الدعوى الجزائية إذ تبقى الهيئة القضائية في مقرها بدار القضاء وذلك من خلال ربطها عبر وسائل الاتصال الإلكترونية)[3]. ومنهم من قال بأنه: (سلطة لمجموعة متخصصة من القضاة بالنظر في الدعوى ومباشرة الإجراءات القضائية بوسائل إلكترونية مستحدثة ضمن نظام أو أنظمة قضائية معلوماتية متكاملة الأطراف والوسائل تعتمد منهج تقنية شبكة الربط الدولية الإنترنت وبرامج الملفات الحاسوبية الإلكترونية للنظر في الدعوة والفصل فيها بغية الوصول للفصل سريع بالدعوى والتسهيل على المتقاضين)[1]. وآخرون قالوا: (هي تلك الحالات التي يحضر فيها الفرد كطرف أو شاهد أو مشاهد للمحاكمة عن طريق اتصال فديو لا اتصال حضوري. ويحصل ذلك حينما تتصل بالمحكمة بالهاتف أو بتطبيق اتصال فديوي لا ان تحضر شخصياً)[2].

ويرى الباحث أنه يمكن تعريف التقاضي عن بعد: (هو نظام قضائي جديد قائم على أساس التطور التكنولوجي الحديث والذي تطبق فيه كافة إجراءات التقاضي وفق قانون المرافعات بواسطة برامج الإلكترونية متكاملة تعتمد على أجهزة الحاسوب الآلي وشبكة الإنترنت العالمية للنظر في الدعوى والفصل فيها خلال مدد محددة وإجراءات قانونية لتسهيل عمل القضاء، والمتقاضين، من خلال مجموعة إجراءات شكلية وموضوعيه يتم اعتمدها في هذا النظام).

---

(1) - د. صفاء اوتاني ، المحكمة الالكترونية، المفهوم والتطبيق، بحث منشور، مجلة الجامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 28، العدد الاول، 2012، ص 170.

(2) - د. خالد ممدوح إبراهيم، إجراءات التقاضي عن بعد في المواد المدنية والجزائية، دار الفكر الجامعي، 2020 ، ص 15 .

(3) - د. عمر عبد المجيد مصبح، ضمانات المحاكمة العادلة على ضوء اعتماد تقنية الاتصال عن بعد في الإجراءات الجنائية في دولة الإمارات، بحث منشور، مجلة كلية القانون الكويتية العالمية، السنة السادسة، العدد 4، 2018 ، ص 387، وكذلك : راندا اسماعيل عطية، آليات تطبيق نظام التقاضي الإلكتروني وتنفيذ الأحكام القضائية في ضوء الوسائل الإلكترونية، دار الكتب والدراسات العربية، 2022 ، ص 32.

(1) - حازم محمد الشرعة، التقاضي الإلكتروني والمحاكم الالكترونية، الطبعة الأولى، دار الثقافة للنشر والتوزيع الأردن 2010 ، ص 59.

(2) Attending Court Remotely, Provincial Court of British Columbia, the link: ((https://www.provincialcourt.bc.ca/COVID19Conferences#:~:text=Remote(ly)%20%E2%80%93%20the%20method,you%20are%20%E2%80%9Cattending%20remotely%E2%80%9D)), (01-07-2022).

أما تعريف المحكمة الإلكترونية : يرتبط مفهوم المحكمة الإلكترونية بفكرة التقاضي عن بعد، وهي ثمرة للتطور التكنولوجي والتقني في مجال الإتصالات والإنترنت، بمعنى الانتقال من التقاضي التقليدي والحضور في المحاكم التقليدية، وتقديم المستندات والأوراق الخاصة بالدعوى بالشكل التقليدية، والاستفادة من التطور التقني ويكون رفع الدعوى ومستنداتها والتقاضي عن طريق موقع الكتروني خاص بالمحكمة الإلكترونية. وعلى ضوء ما تقدم، تعرف المحكمة الإلكترونية على أنها: (موقع إلكتروني يتم فيها الفصل في المسائل القانونية بحضور قضاة مؤهلين يتمتعون ببنية تحتيه تقنية متطورة تسمح لأصحاب العلاقة بتشغيل بعض الجوانب الإدارية والإجرائية لوظائف المحكمة بشكل أفضل مثل تقديم الأدلة أو إيداع المستندات والمذكرات، والايداع الإلكتروني في المحكمة وتلقي الشهادة عن بعد، وهدفها هو تقليل الإعتماد على الورق والمستندات المطبوعة التقليدية، وزيادة كفاءة المحكمة عن طريق الإسراع في الوصول إلى المعلومات)[1]. كما عرفت المحكمة إلكترونية: (بأنها المحكمة التي تقوم بجمع الأعمال الموكل إليها قانونا باستخدام الحاسب الإلكتروني الذي يحتوي على البرامج الخاصة بتطبيق إجراءات التقاضي عن بعد والموصولة بشبكة الاتصالات الدولية (الإنترنت) لأختصار الوقت والجهد وإصدار الحكم بأبسط وأسرع الطرق دون الحضور الشخصي للمحكمة)[2].

ويمكن تعريف المحكمة الإلكترونية من قبل الباحث على أنها : (نظام قضائي إلكتروني متكامل، يعتمد على برامج تقنية عالية الدقة، يساهم بتقديم الخدمات وسرعة إنجازها، وتتمثل خدمات المحكمة الغلكترونية إلى خدمات المواطنين، وخدمات القطاع الاقتصادي، والخدمات الحكومية، بما يحقق سرعة إنجاز المعاملات والقضايا وتوحيد وتبسيط إجراءات التقاضي في المحكمة).

الفرع الثاني

الأساس القانوني للتقاضي عن بُعد

لا يُعدّ التقاضي عن بعد نوعاً مستحدثاً من القضاء، بل هو القضاء نفسه كما تقررت أحكامه، وغاية الأمر إنما تم إستحداث أدوات جديدة لإجراءاته وخطواته من طلب الدعوى والترافع والدفوع وسماع الشهود إنتهاء بالفصل والنطق بالحكم، فاللفظ المسموع عبر الأدوات الإلكترونية، أو الصورة المرئية

(1) - د. خالد ممدوح إبراهيم، إجراءات التقاضي الإلكتروني في المواد المدنية والجنائية، دار الفكر الجامعي، الإسكندرية، 2021 ، ص 44.

(2) - د. أشرف جودة محمد محمود، المحاكم الإلكترونية في ضوء الواقع الاجرائي المعاصر، بحث منشور، مجلة الشريعة والقانون، العدد الخامس والثلاثون، الجزء الثالث، 2020، ص 33.

عبر الشاشات للأشخاص والمستندات و المحررات ما هي إلاّ وسائل[1]. ومن المعروف أن السلطة القضائية في كل دولة من دول العالم الحديث هي صاحبة الولاية العامة في تولي الوظيفة القضائية داخل الدولة من خلال محاكمها القضائية المختصة التي تهدف من خلالها لحماية الحقوق والمراكز القانونية للأشخاص وتتصدى لكل ما يواجهها من ظروف تعيق اقامة العدل على اقليمها والذي أصبح من أهم واجبات الدولة، لأن قضاء الدولة الرسمي هو السبيل والوسيلة لفض المنازعات وتحقيق العدالة القضائية ولحماية النظام القانوني، ويرجع بعضهم أن أساس نشأة هذا النظام يرجع إلى المؤتمر الذي عقد بين معهد القانون الخاص لحل المنازعات الإلكترونية ومركز (فيلانوفا) للمعلومات في القانون والسياحة في (23/اكتوبر/1995)، بواشنطن[2].

أولا : الأساس القانوني الدولي للتقاضي عن بعد:

أهتمت العديد من المواثيق الدولية التي تعني بالتصدي للجريمة وتيسير التعاون الدولي إلى استعمال تقنية المحاكمة عن بعد، ومن بين هذه الاتفاقيات :

1- إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لسنة 2000 : إذ نصت المادة (18) على أنه عندما يتعين سماع أقوال شخص موجود في إقليم دولة طرف بصفة شاهد أو خبير أمام السلطات القضائية للدولة طرف أخرى، يجوز الدولة الطرف الأولى أن تسمح بناء على طلب الدولة الأخرى، بعقد جلسة إستماع عن طريق الفيديو إذا لم يكن ممكنا مثول الشخص المعني بنفسه في اقليم الدولة الطرف الطالبة، ويجوز للدول الاطراف أن تتفق على أن تتولى إدارة جلسة الإستماع سلطة قضائية تابعة للدولة الطرف الطالبة وتحضر سلطة قضائية تابعه للدولة الطرف متلقية الطلب[1].
2- الإتفاقية العربية الخاصة بمكافحة الإرهاب والمنعقدة عام 1998، حيث جاء بنص المادة (3/14) منها على ان: (يدلي المبلغون والشهود والخبراء والضحايا بأقوالهم على نحو يضمن سلامتهم مثل الإدلاء بالشهادة عن طريق إستخدام تقنية الاتصال والحضور عن بعد). ومن خلال هذا النص نجد أن الإتفاقية العربية لمكافحة جرائم الإرهاب، قد أقرت الاساس القانوني للتقاضي عن بعد، ولكن قد شملت هذه الإتفاقية عملية الإتصال عن بعد فقط للشهود والخبراء والمبلغين والمترجمين، دون شمول المتهم[2].

(1) - د. ايمان بنت محمد بن عبدالله، المصدر السابق، ص 1020.
(2) - حسام فاضل حشيش، التقاضي الإلكتروني (المحاكم عن بعد)، دار مصر للنشر، 2022 ،ص 14.
(1) - د. تامر محمد صالح، الحضور عن بعد في الدعوى الجنائية، دار الفكر والقانون، 2021 ، ص 28.
(2) – تامر محمد صالح، المصدر السابق ، ص 26.

ثانيا : الأساس القانوني للتشريع المقارن للتقاضي عن بعد :

نجد أن التقاضي عن بعد، يحتاج لقاعدة تشريعية يستمد القضاة سلطتهم بموجبها لنظر الدعاوى وإصدار القرارات والأحكام بناءً لهذه الإجراءات التي تحمل صفة الالزام، ومن ثم تتمتع بحجية الأحكام وقاعدة فنية يتم من خلالها إنشاء وتصميم برمجة نظام قضائي الكتروني يشمل مواقع إلكترونية تقدم خدمات إدارية وقضائية، وكذلك للأساس التدريبي والتأهيل للكوادر المتخصصة بهذا النظام، ومنهم القضاة والمحامين والكتبة الإلكترونيين، وهذه المتطلبات تُعد من أهم متطلبات إنشاء هذا النظام (التقاضي عن بعد)[1].

أما أهمية الأساس التشريعي للتقاضي عن بعد، يمكن القول إن أهم أسس إنشاء نظام التقاضي عن بعد، هو وجود التشريع، والذي يعني وجود مجموعة من القواعد القانونية المكتوبة التي تصدر عن سلطة مختصة في الدولة وهي السلطة التشريعية، وتكون منظمة وملائمة لحالة التقدم التقني والعلمي من خلال استخدام وسائل إتصال حديثة وتطبيق إجراءات التقاضي الكترونيا عبر شبكة الاتصال الدولية (الإنترنت)[1]. لأن الطبيعة الخاصة للبيئة الإلكترونية تتطلب قواعد تتناسب مع هذه الطبيعة ويكون ذلك بطريقتين: (الأولى) استبعاد القواعد التقليدية واصدار قانون جديد ينظم تلك القواعد، (الثانية) تطوير ما هو قائم من قواعد أختصاص تقليدية وإنتخاب ما يصلح منها لتطبيق إجراءات التقاضي عن بعد إبتداء من تقديم عريضة الدعوى على موقع المحكمة المختصة عبر البريد الإلكتروني، وانتهاء بصدور قرار الحكم[2]، هذا ونلاحظ أن المشرع الفرنسي أكد على امكانية اللجوء إلى تقنية الاتصال المرئي بواسطة برنامج (كون فرنس) في حالة الضرورة، إذ جاء بمضمون المادة (706 مكرر – 71) المعدلة بالقانون رقم (222) لسنة 2020 بتاريخ (25 مارس 2020) ، (إجراءات جنائية فرنسي) والتي تنص على أنه: لغرض حسن إدارة العدالة الجنائية إذا وجد القاضي لحسن إدارة العدالة الجنائية وقاضي التحقيق أو قاضي المحكمة مبررا لذلك في الحالات المنصوص عليها ، اللجوء إلى أسلوب ووسيلة التواصل السمعي عن بعد[3].

---

(1) - د. هادي حسين عبد علي، نصيف جاسم محمد، مفهوم التقاضي عن بعد ومتطلباته، بحث منشور، مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد الاول، السنة الثامنة، 2016، ص 310.

(1) - عمر لطيف العبيدي، التقاضي الالكتروني وآلية التطبيق، بحث منشور، مجلة جامعة تكريت للحقوق، السنة 1، المجلد 1، العدد 2، ج1، 2017 ، ص 530.

(2) - د. هادي حسين عبد علي، نصيف جاسم محمد، مفهوم التقاضي عن بعد ومتطلباته، المصدر السابق، ص311.

(3) – نقلاً عن مروى السيد الحصاوى، المصدر السابق، ص 21.

أما المشرع العراقي قد أوضح في القانون المدني رقم (40) لسنة 1951 في المادة (88) وتطرق لموضوع التعاقد الإلكتروني، إذ تضمنت هذه المادة يعدّ التعاقد بالتلفون أو بأي طريقة مماثلة كأنه تم بين حاضرين فيما يتعلق بالزمان وبين غائبين فيما يتعلق بالمكان. وهذا يعني أن المشرع أشار ضمنا للعقود الإلكترونية وآليات انعقادها، لذلك وفي ظل التطورات نجد أن هيمنة ثقافة الورق التي كانت هي السمة المعتمدة التقليدية، في ملفات الدعوى من مستندات رسمية وغير رسمية ودفتر سجلات وبرقيات ورسائل وغيرها، كان أمرا طبيعيا فيما مضى، أما اليوم وبعد أن إنتشرت التقنية العلمية في ميدان القانون والتوقيع الالكتروني، فبدأت تظهر مصطلحات حديثة في الكتابة الإلكترونية، والتوقيع الإلكتروني، والمستندات، أو المحرر الإلكتروني، وهذه هي نتيجة التطور التكنولوجي الذي يعيشه العالم في الوقت الحاضر. لذا كان على المشرع العراقي التفاعل مع هذا التطور التكنولوجي، ويعيد النظر في القوانين النافذة والتفكير بشكل جدي لإصدار قوانين جديدة تواكب التطور التكنولوجي فيما يتعلق بالمعاملات الإلكترونية والتجارية والمستندات الإلكترونية وغيرها[1].

ونجد أنّ المشرع العراقي، كان متأخراً لإقرار والعمل بمشروع التقاضي الالكتروني، ولكنه قد مهد للأساس القانوني والتشريعي للتقاضي عن بعد من خلال إقرار بعض القوانين المهمة وهي كالاتي:

1- أجازت المادة (19) من قانون التجارة رقم (30) لسنة 1983 المعدل، الاستعانة بالأجهزة التقنية الحديثة بديلا عن الدفاتر التجارية .
2- أقر المشرع العراقي في قانون النقل رقم (80) لسنة 1983 المفهوم الواسع لإجراء التوقيع صراحة، إذ أجازت المادة (142/ رابعا) من القانون توقيع السند باي طريقة.
3- أجازت المادة (2/38) من قانون المصارف رقم (40) لسنة 2003 والمادة (2/38) من قانون المصارف رقم (94) لسنة 2004 أحتفاظ المصرف بالسجلات بصورة خطية ولأي مصرف أن يحتفظ بالدفاتر والسجلات والبيانات وجميع المراسلات والبرقيات والإشعارات والمستندات الأخرى، من حيث الإثبات للبنك المركزي النظر لائحة تحديد المتطلبات الفصل تلك النظم .
4- شرع قانون التوقيع الإلكتروني والمعاملات الإلكتروني رقم (78) لسنة 2012 ونشر في الجريدة الرسمية بالعدد المرقم (4256) في 2012/11/5 وجاء بنص المادة (1/خامسا) منه وعرف الكتابة الإلكترونية على أنها: كل حرف أو رقم أو رمز أو أي علامة أخرى تثبت على وسيلة إلكترونية أو

(1) - د. هادي حسين عبد علي، نصيف جاسم محمد، المصدر السابق، ص 313. وكذلك : د. مروى السيد الحصاوى، وسائل التقاضي الالكتروني وحجية اجراءاته في ظل جائحة كورونا، المصدر السابق، ص 18.

رقمية أو ضوئية أو أي وسيلة أخرى مشابهة وتعطي دلالة قابلة للإدراك والفهم، وأيضاً تضمنت الفقرة (سادسا) من المادة نفسها تعريف للمستندات الإلكترونية[1].

وتأسيساً على ما تقدم فقد كان للتطور التكنولوجي والتقني الأثر الكبير والأبرز في مجال السياسة الجنائية، ومدى مواكبة السياسة التشريعية لهذا التطور الذي يعيشه الافراد والمجتمع الدولي عامة، وما نتج عن هذا التطور سلبا من جرائم إلكترونية معقدة وبالغة الخطورة، ولكن بالمقابل لهذا التطور التكنولوجي يوجد جانب إيجابي يتمثل بمجموعة من البرامج والاجهزة التقنية الحديثة، والتي قد تسخر في إجراءات التحقيق والمحاكمة، بعيداً عن الإجراءات التقليدية، وقد حاول المشرع العراقي مواكبة هذا التطور من خلال تشريع مجموعة من القوانين، كما ذكرنا سالفا، وأيضاً حاول المشرع العراقي أن يهيئ بيئة تشريعية قانونية مناسبة لتفعيل نظام التقاضي عن بعد، وذلك لكون جميع هذه القوانين تعد البنية الاساس لإمكانية العمل بنظام التقاضي عن بعد وتفعيل المحكمة الإلكترونية.

ونلاحظ مع التطور المتسارع في كافة المجالات يتجه العالم بأسره نحو الحوكمة الإلكترونية وإستعمال التكنولوجيا في الإدارة الإلكترونية وذلك لمواكبة التطور والسرعة الهائلة في شتى مجالات الحياة ومن الآثار التي نتجت عن التطور التكنولوجي ومدى تأثيرها في السياسة الجنائية، نجد موضوع التقاضي عن بعد، إذ يُعد القضاء من السلطات التي ترتبط ارتباطاً وثيقاً بالمواطن، وتقوم فكرة التقاضي الالكتروني على تشبيك الاجهزة القضائية كلها وضمها في إطار تفاعلي واحد، وتقوم فكرة التقاضي الالكتروني على الإنتقال من تقديم الخدمات والمعاملات بشكلها الورقي التقليدي إلى الشكل الإلكتروني وذلك عبر مواقع الإنترنت وإن ملفات الدعاوى الإلكترونية تختلف عما هو موجود حاليا، فتزول الالية التقليدية الورقية إلى إجراءات إلكترونية وتحل محلها آليات برمجية متطورة تختلف من حيث الشكل والمضمون كما تختلف آلية تقديم البيانات، وهذا النوع من التقاضي يؤمن وجود المحكمة في كل مكان وفي كل وقت عبر شبكة الإنترنيت الامر الذي يؤدي إلى سرعة البت في الدعاوى وتوفير الجهد والمال على المتقاضين، كما أن هذه التقنيات تسهل عملية تدقيق الدعاوى عبر الإتصال بملف الدعوى عن بعد وتمكن محاكم الإستئناف ومحكمة التمييز الإتحادية من الدخول إلى ملف الدعوى الاصل عند اللزوم دون أعباء ولا مراسلات بريدية وإن إجراءات التقاضي الإلكتروني يتم من خلال تقديم عريضة الدعوى إلى المحكمة عن طريق الإنترنت ومن ثم دفع الرسم القانوني عنها وتسجيلها في سجل الدعاوى الإلكترونية واجراء التبليغ الإلكتروني للخصم وتبادل اللوائح الالكترونية بين الطرفين وقد عمل القضاء العراقي نظام ارشفة لقرارات المحاكم وفي مقدمتها محكمة التمييز الإتحادية بما يمكن الاطلاع على القرارات التمييزية الصادرة في الدعاوى. إذ بادر

(1) - يراجع : قانون التوقيع الإلكتروني والمعاملات إلكتروني العراقي رقم 78 لسنة 2012، المادة (1/سادسا).

مجلس القضاء الاعلى بفتح منصته الالكترونية وبإمكان المواطنين والمحامين، الاستفسار عن الدعوى الخاصة به من خلال من خلال المنصات الإلكترونية كما أن العمل قد جرى بالتقديم على استمارة عقد الزواج الالكتروني والإستعلام الإلكتروني في جميع المحاكم والارشفة الإلكترونية، وكذلك الحجز على القسام الشرعي وحجج الوصاية، كما تسهم الاتمتة في الاستغناء عن الارشيف القضائي الضخم ويستبدل بأرشفة بسيطة باستعمال أقراص ليزرية ونسخ إحتياطية عنها تتسع المعلومات لجميعها ولأتشغل الأحياز مكانياً بسيطاً بدلاً من المخازن الضخمة التي تشغل أماكن واسعة وفي الوقت ذاته يقلل هذا الاستخدام من فقد ملفات الدعاوى أو تلفها ومن جهة أخرى تخفف إجراءات التقاضي الإلكتروني من الازدحام في المحاكم والمشاحنات بين الخصوم خصوصاً في دعاوى الاحوال الشخصية. ويجدر بالإشارة إلى أن النظام الداخلي للمحكمة الإتحادية رقم (1) لسنة 2022 أشار إلى المهام التي تقع على عاتق قسم تكنولوجيا المعلومات والإعلام ، لإعداد الانظمة والبرمجيات واتمتة الدعاوى والقرارات والإحكام الصادرة من المحكمة وإدخال الإساليب العلمية الحديثة في عمل المحكمة. كما أن من الضروري تحديث التشريعات القانونية بما يمكن تطبيق إجراءات التقاضي الإلكتروني والتقاضي عن بعد لاسيما في قانون المرافعات المدنية وإجراءات التبليغات القضائية الإلكترونية.

الخاتمة

((الخاتمة))

في ظل ثورة التطور التكنولوجي الذي يعيشه العالم المعاصر، فقد أصبح المجتمع يعيش حياة مليئة بالتواصل السريع ونقل المعلومات بوجود شبكة الإتصالات العالمية (الإنترنت) من خلال تبادل المعلومات والبيانات الرقمية سواء الخاصة بمؤسسات الدولة أم الخاصة بحياة الأفراد الخاصة، وقد أصبح المجتمع بصورة عامة يتعامل بوسائل تقنية حديثة ودقيقة ولها آثار خطرة إن لم يتم تنظيمها ومراقبتها من قبل الجهات الأمنية والرقابية المعنية، وعلى الرغم لما لهذا التطور التكنولوجي من مزايا عديدة، إلاّ أنه له آثار سلبية نتيجة الإستخدام الخاطئ له، والذي يتمثل بإرتكاب مجموعة كبيرة من الجرائم الإلكترونية كالتهديد والإبتزاز وجرائم الامن الاسري، بالإضافة الى الجرائم الماسة بالسلامة الجسدية والعديد من الجرائم الناتجة عن التطور التكنولوجي، وقد تبين للباحث أن هنالك فرقاً كبيراً بين الجرائم التقليدية والجرائم الإلكترونية، وفي الختام فقد توصل الباحث لمجموعة من النتائج والمقترحات

اولاً : النتائج :

1-تبين للباحث أن للجرائم الناشئة عن إستخدام التكنولوجيا والإنترنت لها طبيعة من نوع خاص على خلاف الجرائم التقليدية.

2-توصل الباحث إلى أن جرائم التكنولوجيا والإنترنت تزداد خطورة كلما تقدم التطور بالتكنولوجيا وزاد استعمالها، لكون هذه الجرائم ترتكب من خارج الحدود في الأغلب ولكونها لا تحتاج الى مجهود بدني .

3-تبين لنا الى أن التطور التكنولوجي قد أسهم في تطوير السياسة الجنائية العمومية في بعض البلدان الأوربية والعربية بشكل متواضع تقريبا، وذلك من خلال تشريع سياسة قانونية تواكب التطور الذي يعيشه العالم، على الصعيد الأقتصادي والإجتماعي والسياسي .

4-اتضح للباحث أنه لا بد للمشرع أن يعتمد معيارين عند التجريم وهما (معيار الخطورة الاجرامية، ومعيار الخطورة الاجتماعية المتعلق بالجريمة) عند تشريع أي نص جنائي.

5-تبين لنا أنه بسبب النقص التشريعي وعدم تطور السياسة الجنائية ومواكبتها لظهور التكنولوجيا الحديثة فان بعض الدول تلجأ الى تطبيق النصوص التقليدية في قانون العقوبات في مواجهة الجرائم الإلكترونية، رغم ان المشرع العراقي قد صادق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بموجب القانون رقم (31) لسنة 2013 ولكن لغاية الان لم يُشرَع قانونا خاص لمكافحة الجريمة الإلكترونية.

6-تبين للباحث أن هناك أهتماما دوليا وإقليميا لمكافحة جرائم التكنولوجيا والإنترنت وبالأخص من قبل دول الاتحاد الإوروبي ومن قبل منظمة الامم المتحدة.

7-تبين لنا من خلال دراسة خصائص الجريمة الإلكترونية، أن المجرم الإلكتروني يمتاز بذكاء خارق، ويعمل باستمرار على خلق الثغرات الامنية للبرامج الإلكترونية، وسهولة تخفية وتدمير الادلة الخاصة بإرتكاب الجريمة.

8-تبين لنا أن دوافع المجرم الإلكتروني، تختلف لإرتكاب الجريمة باختلاف رغباتهم واختلاف ظروفهم.

9-تبين للباحث أن المشرع العراقي قد وفر ضمانة مهمة للمتهم فيما يتعلق بسلامة جسمه، عندما منح الحماية اللازمة لهذا الحق من خلال تجريم الأفعال التي تشكل مساسا بسلامة الجسم، وذلك لتضمين قانون العقوبات بمجموعة لا بأس بها لضمان الحماية اللازمة لسلامة الجسم، وأورد المشرع العبارة (أي فعل مخالف للقانون)، فهذه العبارة تمثل حرص المشرع العراقي على عدم المساس بأي فعل يعرض السلامة الجسدية للضرر.

10- تبين للباحث أن كل من قانون العقوبات وقانون أصول المحاكمات الجزائية العراقي، لم يتضمن نصا تشريعيا لتعويض المتهم عن الاضرار المادية والمعنوية التي اصابته جراء المساس بسلامة جسده أو الإنتقاص من تكامله الجسدي.

11- تبين لنا أن الجرائم التي تهدد السلامة الجسدية والتكامل الجسدي تزداد خطورة كلما تقدم التطور بالتكنولوجيا، بواسطة استخدام الاجهزة التقنية المتطورة، لكون هذه الاجهزة تحتاج إلى تنظيم وتخصص لما لها من جوانب إيجابية وسلبية.

12- تبين للباحث لا بد من وضع دراسات وأبحاث علمية تواكب التطور التكنولوجي ولدراسة طبيعة الجرائم التي تمس السلامة الجسدية، وذلك لوجود نقص تشريعي ينظم العمليات الجراحية والتجميلية، بواسطة إستخدام مجموعة كبيرة من الاجهزة التقنية الحديثة والتي تدخل في مجال العمليات الطبية .

13- تبين لنا أن الدليل الإلكتروني لا يمكن قبوله ولا يكون دليل اثبات، دون الرجوع الى مبدأ المشروعية والالتزام ببعض الضوابط والشروط عند إستخلاص الدليل الالكتروني.

14- توصل الباحث الى أن البحث والتحقيق في الجرائم الإلكترونية يتطلب وجود اشخاص يمتلكون الخبرة في المجال الفني والتقني ومتخصصين في جرائم الحاسوب، ولا يمكن الاعتماد على الاجراءات التقليدية للكشف عن الجرائم التقليدية.

15- تبين للباحث أن بعض التشريعات قد منحت قاضي التحقيق السلطة التقديرية في اعتماد بعض الأدلة الإلكترونية اثناء نظر الدعوى ، وهذا يساعد في مكافحة الجريمة والحد منها، وذلك من خلال عدم التقييد بالنصوص القانونية التقليدية أو بسبب القصور التشريعي في بعض القوانين الخاصة بالجرائم الإلكترونية.

16- تبين لنا أن دور الاثبات الالكتروني قد تغير وتطور وتبدلت طبيعة أدلة الإثبات ، فقد تبدلت هذه الادلة من السندات العرفية إلى السندات والادلة المادية والورقية، وصولا إلى الادلة الالكترونية، وهذا

نتيجة للتطور التكنولوجي السريع الذي يعيشه العالم أجمع في شتى مجالات الحياة، وهذا يتطلب من المشرع الجزائي أن يواكب هذا التطور التكنولوجي وسن قوانين رادعة لمكافحة الجريمة الالكترونية.

17- ثبت لدينا من خلال دراستنا وبحثنا أن هناك فرقاً ما بين إجراءات المعاينة للأدلة الإلكترونية، وبين إجراءات التفتيش، فالمعاينة هي تثبيت لحالة وللأشياء التي تكون موجودة في موقع ومكان الجريمة وتثبيتها، أما التفتيش فهو الحصول على الأدلة المادية والبيانات التي تفيد في كشف الحقيقة من قبل مأموري الضبط القضائي أو من يخوله القانون بالقيام بذلك، وتدوين هذه الإجراءات بمحضر كشف ويتم توقيعه من قبل أشخاص حددهم القانون.

18- أتفق مع الرأي القائل من الفقه بأن الأدلة الإلكترونية لها صفة الأشياء المادية، وذلك لكون الادلة الإلكترونية أغلبها يظهر للواقع على شكل مطبوعات ورقية أو أدلة وبيانات يتم تنزيلها وتخزينها بواسطة اقراص صلبة، ويمكن الاحتجاج بها والإعتماد عليها أثناء الحكم بالدعوى من قبل المحكمة المختصة بنظر الدعوى، وهذا الأمر لا بد منه في وقتنا الحالي وذلك لطبيعة التطور التكنولوجي الذي يعيشه العالم أجمع، ونتيجة التعامل بهذه التكنولوجيا بكل تفاصيل الحياة ولا يمكن الاعتماد على الادلة التقليدية.

19- تبين للباحث عند إجراء التفتيش الإلكترونية، لا بد من الالتزام بضوابط وشروط وأسباب التفتيش التقليدي، لكي تكون إجراءات التفتيش الإلكتروني صحيحه ، وفي حال تخلف أي سبب أو شرط عند القيام بالتفتيش الإلكترونية، فإن هذا الدليل يمكن الطعن به ويؤدي الى أبطال الحكم الذي استند على هذه الأدلة.

20- تبين لنا أن إجراءات المعاينة والتفتيش في الجرائم الإلكترونية تختلف كليا عن إجراءات التفتيش في الجرائم التقليدية، وذلك لكون الإجراءات في التفتيش عن الادلة الإلكترونية تحتاج الى خبراء فنيين ومختصين في المجال التقني وهناك إجراءات خاصة لحفاظ على تلك البيانات والأدلة الرقمية الجنائية.

21- تبين لنا أن محل التفتيش في الجرائم الغلكترونية يختلف كليا عن محل التفتيش في الجرائم التقليدية، وهذا ما يسبب صعوبة في البحث والتحقيق وضبط الادلة الإلكترونية، وذلك لان محل التفتيش في الجرائم الإلكترونية يتكون من مجموعة كبيرة من الاشياء المادية المحسوسة والاشياء غير المحسوسة، بالإضافة إلى وجود بيانات ذات نهاية طرفية مخزنة في دولة أخرى غير الدولة التي إرتكبت فيها الجريمة.

22- توصل الباحث من خلال دراسة موضوع التحقيق ومراقبة المتهم إلكترونيا، وجود قصورٌ واضح في أغلب التشريعات العربية، وقانون أصول المحاكمات الجزائية العراقي ، لكون هذه القوانين شرعت لمكافحة الجرائم التقليدية وفي الوقت الحاضر لا يمكنها مكافحة الجرائم الالكترونية ولأسباب عديدة،

منها اختلاف الوسائل والدوافع والأسباب، فيما بين الجرائم التقليدية في الماضي والجرائم الإلكترونية في ظل التطور التكنولوجي الذي يعيشه العالم في الوقت الحالي.

23- من خلال البحث ودراسة موضوع التقاضي عن بعد تبين للباحث، لا مساس بمبدأ علانية الجلسات في التقاضي عن بعد من خلال القاعات الإلكترونية، بالإستعانة بالدوائر التلفزيونية المغلقة وباستخدام برامج الاتصال المرئي.

ثانياً : المقترحات :

1-نقترح على المشرع بضرورة تشريع قانون خاص ينظم إستخدام الأجهزة التقنية مهما كان نوعها وطبيعتها وشبكات الإنترنت، وتشريع نصوص جنائية لتجريم الجرائم الإلكترونية أسوة بالدول التي اهتمت في هذا المجال وواكبت في تشريعاتها الجرائم الناشئة عن التطور التكنولوجي. ونقترح على المشرع أن يكون تعريف الجريمة الإلكترونية بهذه الصيغة هي (كل فعل يسبب ضررا ماديا او معنويا للفرد أو للآمن المجتمعي والإلكتروني بواسطة التكنولوجيا الحديثة، سواء عن طريق الحاسوب أم الإنترنت، أم اي تقنية حديثة، على المكونات المادية والمعنوية لأي نظام إلكتروني عام ام خاص).

2-ندعو المشرع العراقي بإجراء التعديل على قانون العقوبات رقم (111) لسنة 1969 المعدل، وكذلك قانون أصول المحاكمات الجزائية رقم (23) لسنة 1971 وذلك لكون القانونين أصبحا تقليديين، ولا يواكبان مجريات الاحداث والتطور الذي يعيشه المجتمع وبالأخص على صعيد السلامة الجسدية وما يتعرض له من مخاطر كبيرة بسبب الاجهزة الحديثة التي تدخل في مجال التجميل أو التعذيب وغيرها، وكذلك قانون أصول المحاكمات الجزائية العراقي يحتاج الى تعديل فيما يخص إجراءات المعاينة والتفتيش، فإجراءات التفتيش وفق قانون أصول المحاكمات الجزائية تُعد تقليدية ولا يمكن أن تساعد المحققين والقضاة في مجال كشف الحقيقة والجريمة.

3-نوصي بتفعيل التعاون الدولي من خلال الانضمام إلى الإتفاقيات الدولية والإقليمية، من أجل تبادل المعلومات وتسليم المجرمين وتسهيل إجراءات المحاكمة.

4-نوصي المشرع بضرورة توفير الحماية الجنائية اللازمة للمعلومات والبيانات الرقمية الخاصة والتي تمثل من أهم المصالح الإجتماعية، لكونها تمثل في بعض الاحيان مساساً لإعتبار وشرف الاشخاص، بالإضافة الى كونها تمثل أحد الأسس لنمو الأقتصاد. ونقترح على المشرع أن يكون نص المادة بهذه الصيغة (يعاقب بالحبس مدة لا تقل على ثلاثة سنوات، وبغرامة مالية لا تزيد على (10000000) عشرة ملايين دينار عراقي، كل من تمكن عن طريق الشبكة المعلوماتية او بإحدى وسائل تقنية المعلومات بغير تصريح رسمي، من الدخول الى موقع إلكتروني او نظام معلوماتي بإحدى أجهزة

الدولة او مؤسساتها أو هيئاتها أو الجهات أو الشركات التابعة لها، ويعاقب بالسجن إذا ترتب على الدخول الحصول على البيانات أو المعلومات الإلكترونية، أو الحصول على البيانات او المعلومات تمس الامن الداخلي أو الخارجي للدولة او اقتصادها الوطني او اي بيانات حكومية سرية بطبيعتها أو بمقتضى تعليمات صادرة بذلك أو الغاء تلك البيانات والمعلومات الإلكترونية أو اتلافها أو تدميرها أو نشرها، أو الحاق الضرر بالمستفيدين أو المستخدمين أو الحصول على أموال او خدمات أو مزايا غير مستحقة أو أي استفادة اخرى).

5-نقترح على المشرع العراقي بتضمين مشروع قانون الجرائم الإلكترونية والمعلوماتية فصلاً خاصاً، لحماية الامن الاسري والوقاية منها قبل وقوعها، ويتم تشديد العقوبة في حال تم إرتكاب الجريمة الإلكترونية الماسة بالأمن الأسري من قبل الإقارب أو من قبل ذوي المهن والاختصاص في مجال الحاسوب والبرمجيات.

6-نقترح على المشرع العراقي أن يشرع نصاً خاصاً ضمن مشروع قانون الجرائم المعلوماتية، يتضمن آلية التعامل مع النفايات الإلكترونية لما لها تأثير مباشر وخطر على جسم الانسان. ونقترح أن يكون نص المادة بالصيغة التالية (يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة مالية لا تزيد على (3000000) ثلاثة ملايين دينار، أو بإحدى هاتين العقوبتين، كل من تسبب باذئ بصورة غير مباشرة أو بسبب الاهمال، عند التعامل مع النفايات الإلكترونية بصورة خاطئة او مخالفة للقانون، وتكون العقوبة أشد في حال كان الفاعل من ذوي المهن أو الأختصاص في مجال الإلكترونيات.

7-نقترح على المشرع ضرورة تحديد المسؤولية الجنائية التي ترتكب من قبل الاطباء والعاملين في بعض مراكز التجميل والمختبرات أثناء التجارب الطبية واستخدام الاجهزة التقنية الحديثة والاضرار الناتجة عنها بسبب الممارسات غير القانونية ويكون ضحيتها الافراد بسبب أوهامهم بنتائج غير حقيقية، وذلك من خلال اضافة نص ضمن مشروع تعديل قانون العقوبات. ونقترح أن يكون نص المادة بالصيغة التالية (يعاقب بالحبس مدة لا تقل عن ثلاث سنوات وبغرامة مالية لا تزيد على (10000000) عشرة ملايين دينار، او بإحدى هاتين العقوبتين، كل من تسبب باذئ لشخص أثناء إستعمال جهاز تقني أو الكتروني يسبب ضررا للسلامة الجسدية أو تهديدً لحياة الناس أو امنهم أو صحتهم. أو تغيير أو تعييب أو شطب فحوص طبية أو تشخيص طبي أو علاج إنسان، بسبب عدم الاختصاص أو لأسباب تخص سوء استعمال هذه الاجهزة، أم بسبب استخدامها خلافا للضوابط وتكون العقوبة السجن المؤبد أو المؤقت إذا ترتب على ارتكاب الجريمة موت إنسان عمدا).

8- نقترح ونرى من الضرورة عقد مجموعة من الإتفاقيات مع الدول المتطورة في مجال مكافحة الجرائم الإلكترونية في سبيل التعاون الدولي لمكافحة الجرائم الإلكترونية.

9-نقترح على المشرع العراقي بتشكيل لجنة قانونية متخصصة، من أجل البحث ودراسة بعض القوانين الناجعة في مجال تجريم الجرائم الإلكترونية والتقنية، ويتم دراسة هذه القوانين وإستخلاص النصوص ذات الفاعلية فيها واعتماده ضمن مشروع قانون الجرائم الالكترونية والتقنية العراقي، وأيضا يتم الاستفادة من الأخطاء التي وقعت بها هذه القوانين ، فضلاً عن ذلك يجب الاحاطة بكافة الجرائم التقنية والإلكترونية من خلال التجارب السابقة، ويكون تشريع النصوص بصياغة تؤخذ بالمفهوم الموسع وعدم التضييق من مفهوم النصوص القانونية.

10- نوصي المشرع العراقي النظر بعين الإعتبار لنص المادة (38) من الدستور العراقي الحالي لعالم 2005 ، وتشريع نصوص تسمح بمراقبة الإتصالات الهاتفية والتطبيقات الإلكترونية عند الضرورة ، ووضع بعض الشروط والقيود للتنصت ومراقبة هذه الاتصالات والتطبيقات الإلكترونية، لكي لا تكون حرمة الحياة الخاصة مباحة بحجة الضرورة.

11- نوصي المشرع الجنائي العراقي بضرورة دعم النصوص الإجرائية بنصوص إجرائية جديدة تواكب التطور التكنولوجي والتقني، لسد النقص التشريعي وخاصة في مجال التفتيش الإلكتروني واعتماد الدليل الرقمي، نتيجة لتطور الجرائم من صورتها التقليدية إلى جرائم إلكترونية اكثر خطورة وتعقيدا.

12- ندعو وزارة الداخلية ووزارة العدل ومجلس القضاء الاعلى، ضرورة تقديم البرامج والورش التدريبية المؤهلة لأعضاء الضبط القضائي والمحققين والقضاة، من اجل التمكن من استعمال الأجهزة التقنية ووسائل الإتصال الحديثة، في مجال التحقيق الالكتروني، وأيضا في مجال التقاضي الإلكتروني.

13- ضرورة تشريع نصوص عقابية خاصة يشدد فيها العقوبة، لملاحقة كل من يتلاعب أو يسعى لدخول النظام الالكتروني الخاص بالمحكمة الالكترونية دون ترخيص قانوني.

المصادر

المصادر

القرآن الكريم

أولا : الكتب القانونية

1. ابراهيم عبد نايل، الحماية الجنائية لحرمة الحياة الخاصة في قانون العقوبات الفرنسي، دار النهضة العربية، 2000 .

2. ابراهيم محمود اللبيدي، السلوك الاجرامي في جرائم الانترنت، اصدارات مركز الاعلام الامني، البحرين، 2013.

3. ابو العلا النمر، الادلة الجنائية في ضوء الفقه واحكام النقض الجنائي، دار الصداقة، 1991.

4. ابي القاسم محمود بن عمر الزمخشري، اساس البلاغة، دار الفكر، بيروت، 1979.

5. احسان محمد الحسن، مدخل إلى علم الاجتماع ، بيروت للنشر والطباعة، 1988.

6. أحسن بوسقيعة، الوجيز في القانون الجزائي العام، الطبعة الثامنة عشرة، دار هومه، 2019.

7. أحمد حمد الله أحمد، المسؤولية الجنائية الناشئة عن الاستعمال غير المشروع لخدمة الهاتف النقال، دار السنهوري، بيروت، 2017 .

8. احمد عادل عبدالله المعمري، المسؤولية الجنائية عن سوء استخدام حرية التعبير الصحفي، وزارة الداخلية، قيادة شرطة الشارقة، ادارة مركز بحوث الشرطة، 2017.

9. أحمد عمر ابو خطوة، شرح القسم الخاص من قانون العقوبات، جرائم الاعتداء على الاشخاص، دار النهضة العربية، 2010.

10. احمد فاروق زاهر، مبادئ علمي الاجرام والعقاب، جامعة الشارقة، الطبعة الاولى، 2013 .

11. احمد فتحي سرور، أصول السياسة الجنائية، دار النهضة العربية، مصر، 1972.

12. احمد فتحي سرور، القانون الجنائي الدستوري، الطبعة الثانية، دار الشروق، 2002.

13. احمد فتحي سرور، الوسيط في قانون الاجراءات الجنائية، الطبعة العاشرة، دار النهضة العربية، القاهرة، 2016.

14. أحمد محمود خليل، التحقيق الجنائي (تحقيق النيابة العامة)، دار الكتاب والدراسات العربية، الاسكندرية، 2017.

15. احمد يوسف الطحاوي، الادلة الالكترونية ودورها في الاثبات الجنائي، دار النهضة العربية، القاهرة، 2015 .

16. أدم وهيب النداوي، الموجز في قانون الاثبات ، مكتبة مدينة العلم، دون سنة نشر.

17. اشرف عبدالقادر قنديل، الاثبات الجنائي في الجريمة الالكترونية، دار الجامعة الجديد، الاسكندرية، 2015.

18. أكرم نشأت ابراهيم ، السياسة الجنائية، دار الثقافة ، ط 1، عمان، 2008.

19. أمير فرج يوسف، الاثبات الجنائي للجريمة الالكترونية والاختصاص القضائي بها، الطبعة الاولى، مكتبة الوفاء القانونية، الاسكندرية، 2016 .

20. أمير فرج يوسف، الجرائم التجارية الالكترونية وأساليب مكافحتها، مكتبة الوفاء القانونية، ط 1، 2013 .

21. أمير فرج يوسف. الجريمة الالكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت، مكتبة الوفاء، الاسكندرية، 2011.

22. ايمان يوسف صبرة، الحقوق الاجرائية للمجني عليه في الجرائم الالكترونية في التشريع الفلسطيني، دراسة مقارنة، الجامعة الاسلامية بغزة، كلية الشريعة والقانون، 2020 .

23. تامر محمد صالح، الحضور عن بعد في الدعوى الجنائية، دار الفكر والقانون، 2021 .

24. تامر محمد صالح، الحماية الجنائية للحق في المعلومات الرسمية، دار الفكر والقانون، ط 1، 2021 .

25. جميل صليبا، المعجم الفلسفي، الطبعة الاولى، دار الكتاب اللبناني، بيروت، 1970 .

26. حازم حسن الجمل، الحماية الجنائية للأمن الالكتروني، دار الفكر والقانون، مصر، 2022 .

27. حازم محمد الشرعة، التقاضي الإلكتروني والمحاكم الالكترونية، الطبعة الأولى، دار الثقافة للنشر والتوزيع الأردن 2010 .

28. حسام فاضل حشيش، التقاضي الإلكتروني (المحاكم عن بعد)، دار مصر للنشر، 2022.

29. حسن فضالة موسى، التنظيم القانوني للإثبات الالكتروني، الطبعة الاولى، مكتبة السنهوري، بغداد، 2016 .

30. حسنين شفيق ، الاعلام الجديد والجرائم الالكترونية، دار الفكر والفن، مصر، 2015.

31. حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، دار النهضة العربية، القاهرة، 2009 .

32. حسين مجباس حسين العزاوي، جرائم القذف والسب عبر القنوات الفضائية والانترنت وموقف القانون العراقي منها، مطبعة السيماء، بغداد، 2016 .

33. جابر فهمي عمران، لوجستيات التقاضي، المكتب الجامعي الحديث، 2022 .

34. خالد حسن أحمد لطفي الدليل الرقمي، دار الفكر الجامعي، الاسكندرية، 2020 .

35. خالد حسن أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، دار الفكر الجامعي، الاسكندرية، 2020.

36. خالد حسن أحمد لطفي، القانون الواجب التطبيق على الجريمة المعلوماتية، دار الفكر الجامعي، الاسكندرية، 2019 .

37. خالد حسن أحمد لطفي، آليات التحقيق الجنائي في جرائم تقنية المعلومات، دار الفكر الجامعي، الاسكندرية، 2020 .

38. خالد رمضان عبدالعال سلطان، المسؤولية الجنائية عن جرائم الصحافة، دار النهضة العربية، القاهرة، 2002.

39. *خالد مجيد عبدالحميد الجبوري ، النظرية العامة للتجريم الوقائي ، الطبعة الاولى، المركز العربي للنشر ، 2018.*

40. خالد ممدوح ابراهيم، ابرام العقد الالكتروني، دار الفكر الجامعي، 2008.

41. خالد ممدوح إبراهيم، إجراءات التقاضي عن بعد في المواد المدنية والجزائية، دار الفكر الجامعي، 2020 .

42. خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، 2009 .

43. خالد ممدوح ابراهيم، أمن الجريمة الالكترونية، الدار الجامعية ، الاسكندرية، 2008.

44. خالد ممدوح ابراهيم، حوكمت الانترنت، دار الفكر الجامعي، الاسكندرية، 2011.

45. مدحت رمضان، جرائم الاعتداء على الاشخاص والانترنت، دار النهضة العربية، القاهرة، 2000

46. دينا عبدالعزيز فهمي، الحماية الجنائية من إساءة استخدام مواقع التواصل الاجتماعي، دار النهضة العربية، 2018 .

47. رامي متولي القاضي، د. عمر سالم، مكافحة جرائم تقنية المعلومات رقم (175) لسنة 2018، مركز الدراسات العربية، ط 1، 2020 .

48. رامي متولي القاضي، شرح قانون مكافحة جرائم تقنية المعلومات، مركز الدراسات العربية، 2020 .

49. راندا اسماعيل عطية، آليات تطبيق نظام التقاضي الإلكتروني وتنفيذ الأحكام القضائية في ضوء الوسائل الإلكترونية، دار الكتب والدراسات العربية، 2022 .

50. رمسيس بنهام ، علم الاجرام، منشأة المعارف، الطبعة الاولى، 1961 .

51. رؤف عبيد، مبادئ الاجراءات الجنائية في القانون، دار الفكر العربي، 1977.
52. زيدان عبدالباقي، الاسرة والطفولة، مكتبة النهضة المصرية، القاهرة، 1998.
53. سامي حارب المنذري، موسوعة العلوم الجنائية، تقنية الحصول على الاثار والادلة المادية، الجزء الاول، مركز بحوث الشارقة، 2007.
54. سردار علي عزيز، ضمانات المحاكمة العادلة للمتهم، دار الكتب القانونية، مصر، 2010.
55. سعد معن ابراهيم، حسام حازم احمد، التحريض في وسائل النشر وكيفية مواجهته أمنيا، مكتبة القانون المقارن، بغداد، 2021 .
56. السعيد بن محمد هراوة، حماية الاسرة في ظل الشريعة الاسلامية والاتفاقيات الدولية، مطبعة سامي، 2022.
57. سلام عيسى العبادي، الإرهاب الإلكتروني أخطاره وخصائصه وأهدافه ومكافحته، الطبعة الاولى، 2018 .
58. سلطان الشاوي، الجرائم الماسة بسلامة الجسم، من دون دار نشر ، 2007.
59. سليمان عبدالله، شرح قانون العقوبات، القسم العام، الجزء الاول، دار المطبوعات الجامعية، 2005.
60. سهيل محمد العزام، الوجيز في جرائم الانترنت، المكتبة الوطنية ، الاردن، ط 1، 2009.
61. شريف يوسف خاطر، الحماية الدستورية للكرامة الانسانية، دار النهضة ، 2006.
62. شمسان ناجي صالح الخيلي، الجرائم المستخدمة بطرق غير مشروعة لشبكة الانترنت، دار النهضة العربية، القاهرة، 2009.
63. صالح عبد الزهرة حسون، احكام التفتيش وآثاره في القانون العراقي، ط1، مطبعة جامعة بغداد، 1979.
64. صدام حسين ياسين العبيدي، جرائم الانترنت وعقوباتها في الشريعة الاسلامية والقوانين الوضعية، ط 1 ، المركز العربي للنشر، 2019 .
65. ضياء عبدالله عبود الاسدي، حق السلامة في جسم المتهم، الطبعة الثانية، منشورات زين الحقوقية، 2011.
66. طوني ميشال عيسى، التنظيم القانوني لشبكة الانترنت، الطبعة الاولى، من دون دار نشر، 2001.
67. عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الاثبات، دار الجامعة الجديد، الاسكندرية، 2010 .

68. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، 2005 .

69. عبدالفتاح بيومي حجازي، علم الجريمة والمجرم المعلوماتي، الطبعة الاولى، منشأة المعارف، الاسكندرية، 2009 .

70. عبدالفتاح بيومي حجازي، مبادئ الاجراءات الجنائية في جرائم الكمبيوتر والانترنت، ط 1، دار الفكر الجامعي، الاسكندرية، 2006 .

71. عبدالفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، دار الفكر الجامعي، الاسكندرية، 2006.

72. عبدالفتاح خضر، النظام الجنائي (اسسه العامة في الاتجاهات المعاصرة والفقه الاسلامي) ، من دون دار نشر، 2007.

73. عبدالكريم نصار، اساسيات علم الاجرام والعقاب، منشورات جامعة جيهان، اربيل، 2011.

74. عبدالمهيمن بكر، إجراءات الادلة الجنائية اثناء التفتيش، الطبعة الاولى، 1996.

75. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، 2007 .

76. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، منشأة المعارف، الاسكندرية، من دون سنة نشر.

77. على عدنان الفيل، إجراءات التحري وجمع الادلة والتحقيق الابتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث، 2011.

78. علي حسين خلف، د. سلطان عبدالقادر الشاوي، المبادئ العامة في قانون العقوبات، الطبعة 2، العاتك لصناعة الكتب، 2010 .

79. علي عدنان الفيل، الاجرام الالكتروني، دراسة مقارنة، ط 1، منشورات زين الحقوقية، 2011 .

80. علي عدنان سلمان الركابي ، جريمة الارهاب المعلوماتي، مكتبة السنهوري، 2020.

81. علي نعمة جواد الزرفي، الجريمة المعلوماتية الماسة في الحياة الخاصة، المكتب الجامعي الحديث، 2020 .

82. علي هاشم عبدالحسن، الحماية الجزائية للأمن الاسري من التطور التكنولوجي (دراسة مقارنة) ، دار مصر للنشر، ط 1، القاهرة، 2021.

83. عمر محمد ابو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، دار النهضة العربية، 2004 .

84. عمر محمد بن يونس، مذكرات في الاثبات الجنائي عبر الانترنت، من غير دار نشر، 2006.

85. عوض محمد، جرائم الاشخاص والاموال، الطبعة الاولى، دار النجاح، الاسكندرية، 1972.
86. فاضل عباس الملا ، اصول التشريع الجنائي الاسلامي ، الطبعة الاولى ، 2005.
87. فايز احمد خليفة احمد بن يعروف، المواجهة التشريعية والامنية للجرائم المتصلة بمواقع التواصل الاجتماعي، أدارة مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، 2019.
88. فريد منعم جبور، حماية المستهلك عبر الانترنت ومكافحة الجرائم الالكترونية، منشورات الحلبي الحقوقية، 2010 .
89. قدري عبد الفتاح الشهاوي، الموسوعة الشرطية القانونية، عالم الكتب للنشر، القاهرة، 1997.
90. قدري عبد الفتاح الشهاوي، ضوابط التفتيش في التشريع المصري والمقارن، منشأة المعارف، الإسكندرية، 2004 .
91. كامل سعيد، جرائم الكمبيوتر والجرائم الاخرى في مجال تكنولوجيا المعلومات، دار الثقافة للنشر، عمان، 2002.
92. لينا محمد الاسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، ط 1 ، دار الحامد للنشر، الاردن، 2015.
93. مأمون محمد سلامة، الاجراءات الجنائية في التشريع المصري، دار النهضة العربية، القاهرة، 2001 .
94. ماهر عبد شويش الدرة، شرح قانون العقوبات القسم الخاص، العاتك للنشر، بغداد، 184.
95. محروس نصار الهيتي، الحماية الجنائية للحق في السلامة الجسدية ، دار السنهوري، بغداد ، 2016.
96. محمد ابو العلا عقيدة، مراقبة المحادثة التلفونية، دار النهضة العربية، 2008.
97. محمد الامين البشري، التحقيق في الجرائم المستحدثة، الطبعة الاولى، الرياض، 2004.
98. محمد الرازقي، علم الاجرام والسياسة الجنائية، الطبعة الثالثة، دار الكتاب الجديد، بيروت، 2004.
99. محمد امين الخرشة، مشروعية الصوت والصورة في الاثبات الجنائي، دار الثقافة للنشر، عمان، 2011.
100. محمد بن المدني بوساق، اتجاهات السياسة الجنائية المعاصرة والشريعة الاسلامية، مركز الدراسات والبحوث ، اكاديمية نايف العربي للعلوم الامنية، الرياض، 2002.
101. محمد حسين منصور، المسؤولية الالكترونية، دار الجامعة الجديد، الاسكندرية، 2007 .

102. محمد حمدان عاشور، أساليب التحقيق والبحث الجنائي، أكاديمية فلسطين للعلوم الامنية، 2010.

103. محمد عبدالظاهر موسى، الحماية الجنائية للجسم البشري في ظل التطورات الطبية الحديثة، الطبعة الاولى، دار مصر، 2021 .

104. محمد فالح حسن، مشروعية استخدام الوسائل العلمية الحديثة في الاثبات الجنائي، الطبعة الأولى، بغداد، 1987 .

105. محمد كمال شاهين، الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي، دار الجامعة الجديدة، 2018

106. محمد كمال محمود السوقي، الحماية الجنائية لسرية المعلومات الالكترونية (دراسة مقارنة)، دار الفكر والقانون، المنصورة، 2021.

107. محمد ماضي، التحضير للجريمة في التشريع العراقي، الطبعة الاولى، مكتبة السنهوري، بيروت، 2012.

108. محمد ممدوح بدير ، مكافحة الجريمة المعلوماتية عبر شبكات الانترنت، مركز الدراسات العربية، الطبعة الاولى، 2019 .

109. محمود احمد طه، المواجهة التشريعية لجرائم الكمبيوتر والانترنت، دار الفكر والقانون، مصر، 2012 .

110. محمود محمود مصطفى، شرح قانون العقوبات العام، الطبعة الاولى، دار النهضة العربية، القاهرة، 1984 .

111. محمود نجيب حسني، الدستور والقانون الجنائي، دار النهضة العربية، القاهرة ، 1992.

112. محمود نجيب حسني، النظرية العامة للقصد الجنائي، دار النهضة العربية، القاهرة، 1988

113. محمود نجيب حسني، شرح قانون الاجراءات الجنائية، دار النهضة ، 1998.

114. محمود نجيب حسني، شرح قانون العقوبات الخاص، دار النهضة العربية، القاهرة، 1988.

115. محمود نجيب حسيني، علم العقاب، دار النهضة العربية، طبعة 3 ، القاهرة ، 1973.

116. مصطفى الخشاب، المدخل إلى علم الاجتماع، مكتبة الانجلو المصرية، القاهرة، 1980.

117.مصطفى محمد موسى ، اساليب إجرامية بالتقنية الرقمية (ماهيتها مكافحتها)، دار الكتب القانونية ، 2005 .

118. مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، مطابع الشرطة، القاهرة، 2009.

119. مصطفى محمد موسى، المراقبة الالكترونية عبر شبكة الانترنت، الطبعة الاولى، بدون دار نشر، 2003.

120. منذر الفضل، التصرف القانوني في الاعضاء البشرية، دار الشؤون الثقافية العامة، بغداد، 1990.

121. منذر كمال الشاوي، السياسة الجنائية في قانون العقوبات العراقي، الرسالة للطباعة، بغداد،

122. منصور رحماني، الوجيز في القانون الجنائي العام، دار العلوم للنشر، الجزائر، 2006.

123. منى كامل تركي، التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، الاسكندرية، 2009 .

124. موسى مسعود ارحومة، قبول الدليل العلمي امام القضاء الجنائي، الطبعة الاولى، من غير دار نشر، 1999 .

125. نادر عبد الكريم غزواني، الحماية الجنائية من جرائم الإنترنت ، دار الجامعة الجديد، من دون سنة نشر.

126. نبيلة هبة هورال، الجوانب الاجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات ، دار الفكر الجامعي، الاسكندرية، 2013.

127. نسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي ، منشأة المعارف، الاسكندرية، 2008.

128. نورس أحمد كاظم الموسوي، السياسة الجنائية في حماية الامن الفكري، المركز الديمقراطي العربي، المانيا، برلين، 2022.

129. هشام محمد فريد رستم، الجوانب الاجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، اسيوط، 1994.

130. هلالي عبدالله أحمد، جرائم المعلوماتية عابرة الحدود، دار النهضة العربية، القاهرة، 2007.

131. هلالي عبدالله، حجية المخرجات الكمبيوترية في المواد الجنائية، دار النهضة العربية، القاهرة، 1997.

132. واثبة داود السعدي، الاسس النظرية لعلمي الاجرام والسياسة الجنائية، مكتبة الرسالة ، من غير سنة نشر.

133. يعيش تمام شوقي، الجريمة المعلوماتية، مطبعة الرمال، الجزائر، 2019.

ثانيا : الكتب الشرعية

1. اسراء أسد، المرأة في القرآن الكريم، التعاونية الثقافية للمجمع العالمي لاهل البيت عليهم السلام، الطبعة الاولى، 1430 هـ
2. حسين الراضي، مقالات ودراسات الآداب الزوجية، القسم الثالث عشر، 2016

ثالثا : الأطاريح والرسائل الجامعية

1. ابراهيمي جمال، التحقيق الجنائي في الجرائم الالكترونية، اطروحة دكتوراه، جامعة مولود معمري – تيزي وزو، كلية الحقوق والعلوم السياسية، 2018
2. أحمد عمراني، حماية الجسم البشري في ظل الممارسات الطبية والعلمية الحديثة، اطروحة دكتوراه، جامعة وهران، كلية الحقوق، الجزائر، 2010
3. آمين اعزان ، الحماية الجنائية للتجارة الالكترونية، أطروحة دكتوراه، جامعة عين شمس، كلية الحقوق، 2011
4. أمينة دير، أثر التهديدات البيئية على واقع الامن الانساني في افريقيا، رسالة ماجستير، جامعة محمد خيضر، بسكرة، كلية الحقوق والعلوم السياسية، 2014
5. باقر غازي حنون، المسؤولية الجنائية الناشئة عن الابتزاز الالكتروني، رسالة ماجستير، جامعة البصرة، كلية القانون، 2020
6. حازم زياد طالب دغمش، دور السياسة الجنائية في مواجهة الانحراف الفكري، رسالة ماجستير، الجامعة الاسلامية بغزة، كلية الشريعة والقانون، 2018
7. حامد احمد مال. العولمة في ظل التطور التقني واثارها في مستقبل الوطن العربي، اطروحة دكتوراه، جامعة سانت كليمنتس، قسم العلوم السياسية، 2009
8. حبيبه سيف سالم راشد ، (النظام القانوني لحماية جسم الانسان)، أطروحة دكتوراه ، جامعة عين شمس، كلية الحقوق، 2005
9. حفصي عباس، جرائم التزوير الإلكتروني، اطروحة دكتوراه، جامعة وهران - 1 ، كلية العلوم الإنسانية، الجزائر، 2014
10. حيدر راجي علي ، السياسة الجنائية في قانون مكافحة الارهاب ، رسالة ماجستير ، جامعة كربلاء ، كلية القانون ، 2018

11. حيدر علي نوري، سياسة التجريم دراسة مقارنة، رسالة ماجستير، جامعة النهرين، كلية القانون، 1999

12. خالد مشتهى، الجرائم الالكترونية المؤثرة على امن الدولة، رسالة ماجستير، جامعة جندوبة، كلية العلوم القانونية والاقتصادية، تونس، 2021.

13. د. محمد سامي السيد الشوا، الحماية الجنائية لحق الانسان في سلامة جسمه، أطروحة دكتورته، جامعة القاهرة، كلية الحقوق، 1985

14. رشيدة فاريش ، نورة قاوش، تأثير مواقع التواصل الاجتماعي في أنتشار الجريمة الالكترونية في وسط المراهقين، رسالة ماجستير، جامعة أكلي محند والحاج البويرة، كلية العلوم الانسانية والاجتماعية، 2018

15. زهير خريبط خلف، الحماية الجزائية لسلامة الجسد في ضوء الاعمال الطبية الحديثة، أطروحة دكتوراه، الجامعة الاسلامية في لبنان، كلية الحقوق والعلوم السياسية، 2018

16. زيد محمود سلمان، موضوعات الارهاب في مواقع التواصل الاجتماعي وعلاقتها بإشاعة الخوف لدى الجمهور، أطروحة دكتوراه في فلسفة الاعلام، جامعة بغداد، 2018.

17. سعداوي محمد صغير ، السياسة الجزائية لمكافحة الجريمة ، اطروحة دكتوراه ، جامعة ابو بكر بلقايد ، كلية الآداب والعلوم الاجتماعية ، الجزائر ، 2010

18. سعود علي عبدالله اللوغاني، السياسة الجنائية في مكافحة الجريمة الالكترونية، أطروحة دكتوراه، جامعة الشارقة، كلية القانون، 2016

19. سليمان نبيل زعرب، الحماية الشرعية للحق في الخصوصية الالكترونية في الفقه الاسلامي، رسالة ماجستير، الجامعة الاسلامية بغزة، كلية الشريعة والقانون، 2020

20. شرحبيل غالب حميد ابو سويلم، اعتماد طلبة الجامعة الاردنية على شبكات التواصل الاجتماعي للحصول على الاخبار والمعلومات، رسالة ماجستير، جامعة الشرق الاوسط، كلية الاعلام، الاردن، 2015

21. صباح سامي داود، المسؤولية الجنائية عن تعذيب الاشخاص، اطروحة دكتوراه، جامعة بغداد، كلية القانون، 2000

22. صغير يوسف، الجريمة المرتكبة عبر الانترنت، رسالة ماجستير، جامعة مولود معمري وزو، كلية الحقوق والعلوم السياسية، 2013

23. الطاهر بن احمد، المسؤولية الجنائية للحق في حرية التعبير والصحافة، أطروحة دكتوراه، جامعة الحاج لخضر باتنة، كلية العلوم الانسانية والاجتماعية، شريعة القانون، الجزائر، 2015

24. عاقلي فضيلة، الحماية القانونية للحق في حرمة الحياة الخاصة، أطروحة دكتوراه، جامعة الاخوة منتوري – قسنطينة، كلية الحقوق، الجزائر، 2012

25. عبد المنعم محمد إبراهيم رضوان موضع الضرر في البنيان القانوني للجريمة، اطروحة دكتورة، جامعة القاهرة، كلية القانون، 1993

26. عبدالله دغش العجمي، المشكلات العملية والقانونية للجرائم إلكترونية ، رسالة ماجستير، جامعة الشرق الاوسط، كلية القانون، الاردن، 2014

27. غازي عبدالرحمن هيان الرشيد، الحماية القانونية من الجرائم المعلوماتية، أطروحة دكتوراه، الجامعة الاسلامية في لبنان، كلية الحقوق، 2004

28. فايز محمد راجح غلاب، الجرائم المعلوماتية في القانون الجزائري واليمني، أطروحة دكتوراه، جامعة الجزائر، كلية الحقوق ، 2010

29. فايز محمد راجح غلاب، الجرائم المعلوماتية في القانون الجزائري واليمني، اطروحة دكتوراه، جامعة الجزائر، كلية الحقوق، 2010

30. فيروز عوض الكريم صالح، إجراءات التحري والضبط في الجريمة الالكترونية، أطروحة دكتوراه، جامعة شاندي، كلية القانون، 2017

31. لهوى رابح، الشرعية الإجرائية للأدلة المعلوماتية المستمدة من التفتيش، أطروحة دكتورة جامعة بابنه 1 كلية الحقوق والعلوم السياسية قسم الحقوق 21 20

32. مبروك اساسي، مشروعية الصوت والصورة في الاثبات الجنائي، اطروحة دكتوراه، جامعة الحاج لخضر ، باتنة 1، كلية الحقوق والعلوم السياسية، 2017

33. محمد رشاد ابراهيم مفتاح، الحماية الجنائية للحق في حرمة الاتصالات الشخصية، أطروحة دكتوراه، جامعة الاسكندرية، كلية الحقوق، 2009

34. مراد رايس، أثر تكنولوجيا المعلومات على الموارد البشرية في المؤسسة، رسالة ماجستير ، جامعة الجزائر، فرع الادارة، 2006

35. ميلود رابح، أثر العولمة على سياسة التجريم والعقاب، رسالة ماجستير، جامعة مولود معمري، تيزي وزو، كلية الحقوق، الجزائر، 2017

36. نداء نائل فايز، خصوصية الجرائم المعلوماتية، رسالة ماجستير، جامعة النجاح الوطنية، كلية القانون، فلسطين، 2017

37. هدام ابراهيم ابو كاس. السياسة الجنائية بين الفقه التقليدي والاتجاه الحديث، رسالة ماجستير، جامعة د. الطاهر موالاي ، كلية الحقوق والعلوم السياسة ، الجزائر، 2016

38. هورال هبه نبيلة، جرائم الانترنت، أطروحة دكتوراه، جامعة ابي بكر بلقايد، الجزائر، 2014

رابعا : البحوث العلمية

1. أحمد عبد الموجود ابو الحمد زكير، المواجهة الجنائية لظاهرة التنمر، المجلة القانونية، المجلد 9، العدد 8، 2021.

2. احمد عبدالمجيد الحاج، المسؤولية الجنائية لجرائم النشر الالكتروني في ضوء قانون مكافحة جرائم تقنية المعلومات الاماراتي، بحث منشور، مجلة المنهل، وزارة الداخلية، ابو ظبي، 2012.

3. اردلان نور الدين محمود ، سياسة التجريم والعقاب في قانون مكافحة الارهاب ، بحث منشور ، جامعة سوران ، 2013.

4. أزاوا عبدالقادر، دهيمي نجاة، السياسة الجنائية في جرائم الأعمال، بحث منشور ، المجلة الافريقية للدراسات القانونية والسياسية، جامعة أحمد دراية، ادرار، الجزائر، مجلد، 3، العدد، 2، 2019 .

5. أسامه بن غانم العبيدي، الجهود الدولية في مكافحة الجرائم المعلوماتية، بحث منشور ، مجلة الحقوق، العدد 4، السنة 39، 2015.

6. إسحاق صلاح ابو طه، الحرية الشخصية في ضوء مراقبة المراسلات والتنصت على المحادثات الهاتفية، بحث منشور ، مجلة البحوث والدراسات العربية، مصر، العدد 53، 2016

7. أسود ياسين ، بحث منشور، بعنوان (حق الانسان في الحياة وسلامة الجسد والحق في بيئة نظيفة)، كتاب صدر عن المؤتمر الدولي الافتراضي ، بعنوان (انعكاسات التطور التكنولوجي على حق الانسان في السلامة الجسدية)، برلين - المانيا ، 2021 .

8. أشرف جودة محمد محمود، المحاكم الالكترونية في ضوء الواقع الاجرائي المعاصر، بحث منشور، مجلة الشريعة والقانون، العدد الخامس والثلاثون، الجزء الثالث، 2020.

9. أشرف علي عقلة القواقزة، دور التشريع الاردني في مواجهة الجريمة الالكترونية وأثرها في أمن معلومات المكتبات، بحث منشور، مجلة دراسات علوم الشريعة والقانون، المجلد 47، العدد 1 ، 2019.

10. أكرم سلام عبدالرؤوف سلام، الجرائم الالكترونية في الفقه الاسلامي والقانون الوضعي، بحث منشور، كتاب صدر عن اعمال المؤتمر الدولي الافتراضي، بعنوان (الجرائم الالكترونية في الفقه الاسلامي والقانون الوضعي)، برلين- المانيا، 2022.

11. اكرم محمود حسين البدو، أ. بيرك فارس حسين، الحق في سلامة الجسم، بحث منشور، مجلة الرافدين للحقوق، مجلد 9 ، العدد 33، 2007.
12. امحمد أبو زينة آمنة، إجراءات التحري الخاصة في مجال مكافحة جرائم المعلوماتية، بحث منشور، مجلة جيل لحقوق الإنسان، 2017 ، ضمن اعمال مؤتمرات الملتقى الوطني، اليات مكافحة الجرائم الالكترونية في التشريع الجزائري
13. أميل جبار عاشور ، المسؤولية الجنائية عن جريمة الابتزاز الالكتروني في مواقع التواصل الاجتماعي، مجلة أبحاث ميسان، المجلد السادس عشر، العدد 31، حزيران، 2020
14. ايمان بنت محمد بن عبد الله القثامي، التقاضي عن بعد، دراسة فقهية تطبيقية على النظام السعودي، بحث منشور، مجلة علوم الشريعة والدراسات الإسلامية، العدد 84 ، مارس، 2021
15. بلقيس عبد الرحمن حامد، المخدرات الرقمية، بحث منشور، مجلة العدل، العدد 48، السنة 19، 2017.
16. بلقيس غازي عيدان الفلاحي . د. رحمة الله حبوب، الجهات المختصة بإجراء التحريات الجنائية في القانون العراقي، بحث منشور، مجلة كلية المعارف الجامعة، العدد ، المجلد ، 2018
17. بن زرفة هوارية، العولمة وتأثيرها على الجريمة والعقاب، بحث منشور ، مجلة المعيار، المركز الجامعي بجامعة تيسمسيلت، الجزائر ، مجلد 25، العدد 56، 2021.
18. التوجي محمد عثمان عبد القادر، السياسة الجنائية لمكافحة الإشاعة عبر مواقع التواصل الاجتماعي، بحث منشور، مجلة الاجتهاد الدراسات القانونية والاقتصادية، المجلد 9 ، العدد 4، 2020
19. تيانتي مريم، ورقة عمل بعنوان، الجريمة الالكترونية بين القيام والتجريم، اصدار المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، برلين، الجزء الاول، 2020
20. جاسم خريبط خلف، التفتيش في الجرائم المعلوماتية، بحث منشور ، مجلة الخليج العربي، المجلد 41، العدد 3 – 4 ، 2013
21. جغدم محمد الامين، جرائم الارهاب الالكتروني والجرائم المنظمة، بحث منشور، مجلة كلية الحقوق، جامعة عبدالحميد ابن باديس، العدد 6، 2018 .
22. الحاج علي بدر الدين، بوعكاز خليل، الاستغلال الجنسي عبر شبكة الانترنت، بحث منشور، اصدار المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، برلين، الجزء الاول، 2020 .

23. حسين فريجه، الجرائم الإلكترونية والإنترنت، بحث منشور، مجلة المعلوماتية، العدد 36، 2011

24. حليمة خالد المدافع، التحقيق الابتدائي باستخدام تقنية الاتصال عن بعد، بحث منشور ، مجلة جامعة الشارقة للعلوم القانونية، المجلد 17، العدد 2، 2020

25. حميد عبدحمادي ضاحي، سياسة المشرع العراقي في مكافحة الفساد الاداري ، بحث منشور، مجلة جامعة الانبار للعلوم القانونية، العدد الخامس ، سنة 2018

26. حواسة جمال، دور الاسرة في تحقيق الامن الاجتماعي، بحث منشور، مجلة دراسات ، جامعة 8 ماي 1945 قالمة، الجزائر ، المجلد 7، العدد 3، 2018.

27. حيدر كاظم الطائي، المراقبة كإحدى طرق البحث الجنائي، بحث منشور، مجلة القانون للدراسات والبحوث القانونية، العدد التاسع عشر، 2019

28. خرشي عثمان، المفهوم الفقهي للجريمة المعلوماتية، بحث منشور، اصدار المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية ، بعنوان ، الجريمة المعلوماتية وأثرها على التنمية الاقتصادية، الجزء الاول، برلين، 2020 .

29. خليل سعيد خليل، القالب التشريعي لجرائم انتحال الصفة والشخصية الالكترونية، بحث منشور، مجلة العلوم الانسانية والادارية، العدد 22، 2021

30. خميخم محمد ، (تأثير التطور التكنولوجي على التمتع بالحق في الصحة والحياة- النفايات الالكترونية نموذجا)، ورقة عمل، مقدمة ضمن المؤتمر الدولي الافتراضي، بعنوان (انعكاسات التطور التكنولوجي على حق الانسان في السلامة الجسدية)، برلين - المانيا ، 2021 .

31. خوالدية فؤاد، الحق في سلامة الجسد في القانون الدولي والوطني في ظل التطور التكنولوجي، بحث منشور، كتاب صدر عن اعمال المؤتمر الدولي (انعكاسات التطور التكنولوجي على حق الانسان في السلامة الجسدية ، برلين - المانيا ، 2021 .

32. ذياب موسى البداية، ورقة عمل بعنوان، الجرائم الالكترونية (المفهوم والاسباب) الملتقى العلمي (الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية، المقام في الاردن، 2014.

33. رابح فغرور، حق تأديب الزوجة والاولاد والضمانات الواردة عليه، بحث منشور، مجلة جامعة الامير عبدالقادر للعلوم الاسلامية، الجزائر، المجلد 33، العدد 2، 2019.

34. راشد محمد المري، المهارات الفنية رجال الأمن في التحقيق والبحث الجنائي، بحث منشور، مجلة روح القانون، العدد الثاني والتسعون، 20 20 .

35. رباح سليمان خليفة دور التقاضي الإلكتروني في الحد من التضخم الاجرائي، مجلة كلية القانون للعلوم القانونية والسياسية، المجلد 10 ، العدد 39 ، 2021

36. رزق سعد علي، انعكاسات التحول الرقمي على السياسة الجنائية المعاصرة، بحث منشور، مجلة الدراسات القانونية والاقتصادية، المجلد 7، العدد 2، 2021.

37. رياض أحمد، وسائل التواصل الاجتماعي ودورها في تعبئة الرأي العام العالمي في الحد من انتشار وباء كورونا ، المجلد 3، العدد 1، 2020.

38. زروقي فايزة، بوراس عبدالقادر، السياسة الجنائية المعاصرة بين انسنة العقوبة وتطوير قواعد العدالة، بحث منشور، مجلة الحقوق والعلوم الانسانية، المجلد 14، العدد 3، 2021.

39. زورال معزوزة، الإرهاب الإلكتروني نمط الأمن المعلوماتي الجرائم المعلوماتية وأثرها على التنمية الاقتصادية، ورقة عمل، ضمن اعمال المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، بعنوان ، الجريمة المعلوماتية وأثرها على التنمية الاقتصادية، الجزء الاول، برلين، 2020

40. زيباري الشاذلي، اتجاهات السياسة الجنائية الدولية كألية قانونية لمواجهة الجريمة المنظمة العابرة للحدود، بحث منشور، مجلة البحوث القانونية والاقتصادية ، مجلد 2، العدد 2، 2020.

41. سامي حارب المنذري، موسوعة العلوم الجنائية (تقنية الحصول على الاثار والادلة المادية)، الجزء الاول، مركز بحوث الشرطة، الشارقة، 2021.

42. سامية عبد الرزاق خلف، التعدي على حرمة الحياة الخاصة باستخدام التكنولوجيا الحديثة، بحث منشور، مجلة الدراسات القانونية، العدد 25، 2010.

43. سحر فؤاد مجيد، جريمة التحرش الجنسي بالاطفال عبر الانترنيت، بحث منشور، المجلة الاكاديمية للبحث القانوني، العدد الخاص، 2017.

44. سديرة نجوى ، أ. منار صبرينة، (أثر تطور التكنولوجيا الحيوية في تقرير المسؤولية القانونية عن الاخلال بشروط التجارب على الاجنة البشرية)، ورقة عمل، ضمن اعمال المؤتمر الدولي الافتراضي ، بعنوان (انعكاسات التطور التكنولوجي على حق الانسان في السلامة الجسدية) ، برلين - المانيا ، 2021 .

45. سعاد بومايله وفارس بوباكور، أثر التكنولوجيا الحديثة للإعلام والاتصال في المؤسسة الاقتصادية، مجلة الاقتصاد المناجمت، العدد 3، 2004.

46. سعد صالح شكطي، الخروج عن القاعدة في الظروف المشددة للجرائم، بحث منشور، مجلة جامعة تكريت للعلوم القانونية، المجلد 1، العدد 28، 2015.

47. سعيد زيوش ، ظاهرة الابتزاز الالكتروني وأساليب الوقاية منها، بحث منشور، مجلة العلوم الاجتماعية، العدد 22، 2017.

48. سكوتي خالد، (التهديد التكنولوجي على حق الانسان في سلامة جسده)، ورقة عمل مقدمة، ضمن اعمال المؤتمر الدولي الافتراضي ، بعنوان (انعكاسات التطور التكنولوجي على حق الانسان في السلامة الجسدية ، برلين - المانيا ، 2021 .

49. سلام سميرة، د. سلام محمد أمين، التكنولوجيا الرقمية وتأثيرها على السلامة الجسدية والعقلية للطفل، بحث مقدم، ضمن اعمال المؤتمر الدولي الافتراضي، بعنوان، انعكاسات التطور التكنولوجي على حق الانسان في السلامة الجسدية ، برلين - المانيا ، 2021 .

50. صباح كزيز ، د. سمير قط، أثر الجرام الإلكترونية على من واستقرار الدول، قرصنة الموقع الإلكتروني لوكالة الأنباء القطرية نموذجا ، مجلة الناقد للدراسات السياسية، العدد الثالث، 2018.

51. صفاء اوتاني، المحكمة الإلكترونية، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 28 ، العدد الاول، 2012 .

52. صلاح حسن احمد، الدفاع الاجتماعي ضد الجريمة بين الشريعة الاسلامية والقانون الوضعي، بحث منشور ، مجلة كلية العلوم والسياسة ، جامعة كركوك ، 2011.

53. ضياء عبدالله الجابر، ناصر خضر الجوراني، القناعة القضائية في الاثبات الجنائي، بحث منشور، مجلة جامعة كربلاء، المجلد الثالث، العدد الثالث عشر، 2005

54. طالب محمد جواد، د. عبدالجبار ضاحي، جرائم تقنية المعلومات واثباتها، بحث منشور، مجلة كلية الرافدين الجامعة، العدد 28، 2013

55. عادل يوسف عبدالنبي، الجريمة المعلوماتية وازمة الشرعية الجزائية، بحث منشور، مجلة مركز دراسات الكوفة، العدد 7، 2011.

56. عاطف محمد ابو هربيد، أ. نجوان نبيل، جريمة استغلال الاطفال جنسيا عبر الانترنت، بحث منشور، مجلة الجامعة الاسلامية للدراسات الشرعية والقانونية، المجلد 30 ، العدد 1، 2022.

57. عاطف محمد ابو هربيد، أ. نجوان نبيل، جريمة استغلال الاطفال جنسيا عبر الانترنت، بحث منشور، مجلة الجامعة الاسلامية للدراسات الشرعية والقانونية، المجلد 30، العدد 1، 2022

58. عبد السميع بالعيد محمد، (الاثار المترتبة عن التطور التكنولوجي على حق الانسان في سلامة جسده) ورقة عمل مقدمة، ضمن اعمال المؤتمر الدولي بعنوان (انعكاسات التطور التكنولوجي على حق الانسان في السلامة الجسدية) ، برلين - المانيا ، 2021 .

59. عبدالصمد الكنا، ضوابط التجريم والعقاب ضمانه للحقوق والحريات، بحث منشور ، مجلة المنار للدراسات القانونية والادارية، العدد (5) ، 2017 .

60. عبدالفتاح مصطفى الصيفي، المطابقة في مجال التجريم (محاولة فقهية لوضع نظرية عامة للمطابقة) بحث منشور، مجلة كلية الحقوق للبحوث القانونية والاقتصادية، جامعة الاسكندرية، كلية الحقوق، المجلد 13، العدد الخاص، 2018 .

61. عبدالقادر الشيخلي، الجهود والاتفاقيات العربية والدولية لمكافحة الجريمة، بحث مقدم إلى الدورة التدريبية لمكافحة الجريمة الاقتصادية، جامعة نايف العربية للعلوم الامنية، 2007

62. عبدالناصر محمد فرغلي، المسماري محمد عبيد، الاثبات الجنائي بالادلة الرقمية من الناحية القانونية والفنية ضمن وقائع المؤتمر العربي الاول لعلوم الادلة الجنائية والطب الشرعي، المقام في جامعة نايف العربية للعلوم الامنية، 2007.

63. عبدالهادي درار، نظام المراقبة الالكترونية في ظل تطورات النظم الاجرائية الجزائية، بحث منشور، جامعة جيلالي اليابس، كلية الحقوق، مجلة الدراسات والبحوث القانونية، العد الثالث، 2017

64. عبدالوهاب عبدالرزاق التحافي، اتجاهات السياسة الجنائية لمواجهة الجرائم الاجتماعية، مقالة منشورة، مجلة الزمان 24 الدولية ، العدد 1764 ، 2016 .

65. عزالدين عثماني، إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلومات، بحث منشور، مجلة دائرة البحوث والدراسات القانونية والسياسية، العدد الرابع، 2018

66. عصماني ليلى، نظام التقاضي الإلكتروني آلية لإنجاح الخطط التنموية، مجلة المفكر، العدد الثالث عشر، جامعة وهران 2، 2016

67. عفاف خذيري ، الحماية الجزائية لحق الانسان في سلامة جسده في ظل التطور التكنولوجي، بحث منشور، ضمن اعمال المؤتمر الدولي الافتراضي، بعنوان (انعكاسات التطور التكنولوجي على حق الانسان في السلامة الجسدية ، برلين - المانيا ، 2021 .

68. علي حمزة عسل، د. خالد ماجد ، التجريم الوقائي في قانون حماية المستهلك العراقي، بحث منشور، مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد الاول، السنة التاسعة، 2017.

69. عمر عبدالمجيد مصبح، ضمانات المحاكمة العادلة على ضوء اعتماد تقنية الاتصال عن بعد في الاجراءات الجنائية في دولة الامارات، بحث منشور ، مجلة كلية القانون الكويتية العالمية، السنة السادسة، العدد 4، العدد التسلسلي 24، 2018

70. عمر لطيف العبيدي، التقاضي الالكتروني وآلية التطبيق، بحث منشور، مجلة جامعة تكريت للحقوق، السنة 1، المجلد 1، العدد 2، ج1، 2017 .

71. عيساني رفيقة، بحث بعنوان (الحماية القانونية للسلامة الجسدية للإنسان في ظل التطور التكنولوجي الطبي)، كتاب صدر عن المؤتمر الدولي الافتراضي ، بعنوان (انعكاسات التطور التكنولوجي على حق الانسان في السلامة الجسدية ، برلين - المانيا ، 2021 .

72. فاطمة عبد الله علي عمران، دور التشريعات الداخلية في حماية حق الانسان في السلامة الجسدية من الاثار السلبية للتطور التكنولوجي، بحث منشور، كتاب صدر عن المؤتمر الدولي الافتراضي ، بعنوان (انعكاسات التطور التكنولوجي على حق الانسان في السلامة الجسدية ، برلين - المانيا ، 2021 .

73. فضيلة عاقلي ، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري ورقة عمل مقدمة، ضمن أعمال المؤتمر الدولي الرابع عشر بعنوان (مكافحة الجرائم إلالكترونية)، طرابلس 2017

74. فيلالي أسماء، ورقة عمل بعنوان، المجرمون المعلوماتيون خطر حقيقي يهدد عالم المعلوماتية، اصدار المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، برلين، الجزء الاول، 2020 .

75. كاظم عبدالله الشمري، زينة عبدالجليل عبد، سياسة التجريم في القوانين الخاصة، بحث منشور ، مجلة العلوم القانونية، جامعة بغداد، كلية القانون، العدد الخاص، المجلد 36، 2021.

76. لخضر رابحي، ابراهيم سويسي ، مجابهة جريمة التحريض الالكتروني في ضوء مبدأ مسؤولية الحماية، بحث منشور، مجلة الدراسات القانونية والسياسية، المجلد 6، العدد 2، 2020.

77. لورنس سعيد الحوامدة، حجية الادلة الرقمية في الاثبات الجنائي، بحث منشور، مجلة البحوث الفقهية والقانونية، العدد السادس والثلاثون، 2021

78. ماشاءالله الزوي، بعنوان الجرائم الالكترونية ، بحث مقدم ضمن اعمال المؤتمر الدولي الرابع عشر، ، بعنوان، المواجهة الجنائية للبريد الالكتروني العدائي المزعج أو المضلل، مارس، 2017

79. محمد الامين البشري، التحقيق في جرائم الحاسب الالي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، كلية القانون والشريعة، جامعة الامارات، 2005.

80. محمد بومديان، الاستخدام السلبي للتطور التكنولوجي في التحقيق مع المتهم، بحث منشور، كتاب صدر عن المؤتمر الدولي الافتراضي ، بعنوان (انعكاسات التطور التكنولوجي على حق الانسان في السلامة الجسدية ، برلين - المانيا ، 2021 .

81. محمد شاكرالحمادي، نظرات في السياسة العقابية لقانون مكافحة المخدرات الاماراتي بين النص التشريعي والتطبيق القضائي، بحث منشور، مجلة العلوم القانونية والاقتصادية، المجلد 60، العدد 2، مصر، 2018 .

82. محمد علي سالم. حسون عبيد، الجريمة المعلوماتية، بحث منشور، مجلة جامعة بابل، العلوم الانسانية، مجلد 14، العدد 2، 2007.

83. محمد لموسخ ، تنازع الاختصاص في الجرائم الالكترونية، بحث منشور، مجلة دار المنظومة، جامعة قاصدي مرباح، كلية الحقوق والعلوم السياسية، العدد 2، 2009

84. محمد، ورضوان العنبي، السياسة الجنائية بالمغرب وانواع العقوبات البديلة لمكافحة الجريمة، بحث منشور، مجلة المنار للدراسات القانونية والادارية، العدد الخاص، 2017.

85. محمود صالح العادلي، البحث والتحقيق الجنائي في الإرهاب الإلكتروني، بحث منشور، مجلة دراسات تربوية، العدد 6، 2021

86. محمود نجيب حسني، الحق في سلامة الجسم ومدى الحماية التي يكفلها له قانون العقوبات، مجلة القانون والاقتصاد، العدد 3، السنة، 29، 1959.

87. مروى السيد الحصاوى، وسائل التقاضي الالكتروني وحجية إجراءاته في ظل جائحة كورونا، بحث منشور، المجلة الجزائرية لقانون الاعمال، المجلد 2، العدد 1، 2021

88. مشنف أحمد، د. قايد حفيظة، بحث منشور (دراسة تحليلية لتأثير التقدم التكنولوجي على سلامة الانسان)، كتاب صدر عن المؤتمر الدولي الافتراضي ، بعنوان (انعكاسات التطور التكنولوجي على حق الانسان في السلامة الجسدية ، برلين - المانيا ، 2021 .

89. معالي حميد الشمري، السياسة الجنائية التشريعية في قوانين الاحزاب السياسية ، مجلة كلية التربية، العدد التاسع والثلاثون، الجزء الثاني، 2020 .

90. مفيدة مباركية ، الادلة الجنائية الرقمية والحق في الخصوصية، بحث منشور، مجلة المعيار، المجلد 25، العدد 58، 2021.

91. ملاطي هشام، السياسة الجنائية في علاقتها مع السياسات العمومية للدولة، بحث منشور، المجلة المغربية للسياسات العمومية، المجلد 12، العدد 22، 2017.

92. ممدوح حسن مانع العدوان، نادر عبدالحليم السلامات، مشروعية وحجية الدليل المستخلص من التفتيش الالكتروني في التشريع الجزائي الاردني، بحث منشور، مجلة علوم الشريعة والقانون، المجلد 45، العدد 4، ملحق 2، 2018.

93. ميسون خلف أحمد الحمداني، مشروعية الادلة الإلكترونية في الاثبات الجنائي، بحث منشور، مجلة البحوث والدراسات العربية، المجلد 18، العدد 2، 2016 .

94. نور الدين الخادمي، القواعد الفقهية والامن الشامل، المجلة العربية للدراسات الامنية والتدريب، المجلد 21، العدد 42، 2006.
95. نور الدين زمام، أ. صباح سليماني، تطور مفهوم التكنولوجيا واستخداماته العلمية، بحث منشور، مجلة العلوم الانسانية والاجتماعية، جامعة محمد خيضر بسكرة، الجزائر، العدد الحادي عشر ، 2013.
96. هادي حسين عبد علي، نصيف جاسم محمد، مفهوم التقاضي عن بعد ومتطلباته، بحث منشور، مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد الاول، السنة الثامنة، 2016.
97. هشام البلاوي، المحاكمة عن بعد وضمانات المحاكمة العادلة، مقال منشور، مجلة رئاسة النيابة العامة، العدد الاول، 2020
98. هيام محمد الهادي، بحث منشور بعنوان، تعرض المراهقين للجرائم الالكترونية عبر وسائل الاعلام الرقمي وتأثيرها على ادراكهم للأمن الاجتماعي المصري، المجلة العربية لبحوث الاعلام والاتصال، العدد 30، يوليو، 2020
99. ياسر محمد عبدالله، م. احمد مصطفى علي، جرائم العنف الاسري وسبل مواجهتها في التشريع العراقي، بحث منشور، مجلة الرافدين للحقوق، المجلد 15، العدد 55، 2012
100. ياسمينة بونعارة، الجريمة الالكترونية، مجلة المعيار ، العدد 39، 2015.
101. يوسف بو غرارة، الامن السيبراني (الاستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبراني)، بحث منشور، مجلة الدراسات الافريقية وحوض النيل، المركز الديمقراطي العربي، مصر، العدد 3، 2018.
102. يونس عرب، جرائم الكمبيوتر والانترنت، بحث مقدم إلى مؤتمر الامن العربي، المركز العربي للدراسات والبحوث الجنائية، ابو ظبي. 2002.

خامسا : التقارير والمؤتمرات والإتفاقيات الدولية

1. التقرير الصادر عن الامم المتحدة/ الجمعية العامة ، الدورة الرابعة والسبعون، مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الاجرامية، 2019
2. توصيات مؤتمر الامم المتحدة الثالثة عشر حول الجريمة والعدالة الجنائية، بعنوان (الجهود السياسة الجنائية المغربية في التصدي للجريمة)، سلسلة دراسات وابحاث جنائية، صدرة عن مركز الدراسات وابحاث السياسة الجنائية، المملكة المغربية، وزارة العدل ، العدد 3 ، 2020
3. اتفاقية بودابست لسنة 2001 الخاصة بمكافحة الجريمة الإلكترونية.

سادسا : الدساتير

1. دستور جمهورية العراق لعام 2005
2. دستور جمهورية مصري العربية لعام 2014
3. دستور دواة الإمارات العربية المتحدة لعام 1971

سابعا : القوانين

1. قانون العقوبات العراقي رقم 111 لسنة 1969 المعدل.
2. قانون اصول المحاكمات الجزائية العراقي رقم 23 لسنة 1971 وتعديلاته.
3. القانون المدني العراقي رقم 40 لسنة 1951 وتعديلاته.
4. قانون العقوبات المصري رقم 58 لسنة 1937 وتعديلاته.
5. قانون العقوبات الفرنسي رقم لسنة 1994 المعدل .
6. قانون مكافحة جرائم تقنية المعلومات الكويتي رقم 63 لسنة 2015
7. قانون تصديق الاتفاقية العربية العراقي لمكافحة جرائم تقنية المعلومات رقم (31) لسنة 2013 .
8. قانون التوقيع الإلكتروني والمعاملات الإلكتروني العراقي رقم 78 لسنة 2012.
9. قانون مكافحة جرائم تقنية المعلومات المصري رقم (175) لسنة 2018.
10. قانون مكافحة جرائم المعلوماتية السعودي رقم 79 لسنة 1428 هـ.
11. قانون مكافحة الجرائم الالكترونية القطري رقم 14 لسنة 2014 .
12. قانون جرائم أنظمة المعلومات الاردني رقم 30 لسنة 2010.

ثامنا : المعاجم والموسوعات

1. ابن منظور، أبو الفضل جمال الدين محمد بن مكرم، لسان العرب، بيروت.
2. المعجم الوسيط، صادر عن مجمع اللغة العربية بجمهورية مصر، ط 4، مكتبة الشروق الدولية، 1435 هـ، 2004 م
3. المنجد في اللغة. لويس المعلوف، الطبعة الرابعة، انتشارات ذوي القربى، أيران، 1429هـ .
4. محمد بن أبي بكر بن عبدالقادر الرازي، مختار الصحاح، المطبعة الاميرية، القاهرة ، 1338 .
5. مجمع اللغة العربية، المعجم الوسيط، اخرجة مجموعة من العلماء، الطبعة الثانية، المكتبة الاسلامية

تاسعا : المصادر باللغة الانكليزية

1. Attending Court Remotely, Provincial Court of British Columbia, thelink: ((https://www. provincialcourt. bc.ca/COVID19Conferences #:~:text= Remote(ly) %20%E2%80%93%20the%20method,you%20are%20%E2%80%9Cattending%20remotely%E2%80%9D)), (01-07-2022).
2. Confress of chief Justice, Remote Hearings and Access to Justice During Covid-19 and Beyond
3. Peter G. Berris, Cybercrime and the Law: Computer Fraud and Abuse Act (CFAA) and the 116th Congress, 2020
4. United States v. Szymuszkiewicz, 2009 WL 1873657, at *2 n.2 (E.D. Wis. 2009).
5. United States v. Cotten, 471 F.2d 744, 750 (9th Cir. 1973).
6. United States v. Gatlin, 216 F.3d 207, 211 (2d Cir. 2000).
7. Equal Employment Opportunity Comm. v. Arabian American Oil Co., 499 U.S. 244, 248 (1991)
8. Gary R. Gordon, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, January 2003
9. Secretary of State for the Home Department, Cyber Crime Strategy, 2010, the United Kingdom
10. Computer Fraud and Abuse Act 18 U.S.C. § 1030.
11. H. Marshall Jarrett & Michael W. Bailie, Op.Cit
12. United States v. Drew, 259 F.R.D. 449, 457.
13. United States v. Trotter, 478 F.3d 918, 921 (8th Cir. 2007).
14. Paradigm Alliance, Inc. v. Celeritas Technologies, LLC, 248 F.R.D. 598, 602, 2008.
15. Daniel A. Reilly, Finding the Truth with Criminal Investigation: Suspect, Subject, Defendant, Rowman & Littlefield Publishers August 15, 2019.

16. The editors of Britannica, Criminal Investigation, Britannica, the link:
17. ((https://www.britannica.com/topic/criminal-investigation)), Accessed at ((23-05-2022)).
18. K. S. Dharmasiri, K.G.N.U Rannaweera, Anuruddhika Buddhadasa, K.B.N and De Silva, Criminal Investigation: A Brief Review of Importance of Biological Evidence, European Scholar Journal (ESJ), Vol. 2 No. 8, 2021.
19. Whitney D. Gunter and Christopher A. Hertig, an Introduction to Theory, Practice and Career Development for Public and Private Investigators, International Foundation for Protection Officers, 2005.
20. Peter W. greenwood & Joan Petersilia, the Criminal Investgeation Process Voulume Summary and Policy Implications, Rand Institution, 1975.
21. Dr Amber McKinley, Criminal Investigative Failures, Volume 6, Number 1, 2018
22. Hakan Hekim, INFORMATION TECHNOLOGY AND CRIMINAL INVESTIGATIONS: DOES IT
23. MATTER?, The University of North Carolina, 2009
24. Dr. Jarrod Sadulski, Unintended consequences of technology in policing, American Military University, 2017, the link:
25. ((https://www.police1.com/american-military-university/articles/unintended-consequences-of-technology-in-policing-EQhuM6wsvpCNKqYF/)).
26. U.S. Department of Justice Office of Justice Programs National Institute of Justice, Investigative Uses of Technology: Devices, Tools, and Techniques, 2017, October 07.
27. James I. Walsh and James A. Piazza, Why Respecting Physical Integrity Rights Reduces Terrorism, Comparative Political Studies, 2010
28. A Nienaber, The right to physical integrity and informed refusal: Just how far does a patient's right to refuse medical treatment go?, SAJBL, Vol. 9, No. 2, 2016
29. Bodily Integrity, Child Rights international Network, the link:

30. ((https://archive.crin.org/en/home/whatwedo/policy/bodilyintegrity.html#:~:text=The%20principle%20of%20bodily%20integrity,as%20a%20human%20rights%20violation.)), Accessed at (04-07-2022).
31. Ashley Watters, 5 Ethical Issues in Technology to Watch for in 2021, CompTIA, 2021, the link:
32. ((https://connect.comptia.org/blog/ethical-issues-in-technology)), Accessed at (03-07-2022).
33. Eurojust and Europol, Common challenges in combating cybercrime, OINT REPORT
34. Europol and Eurojust Public Information, 2019
35. Susan W. Brenner, State Cybercrime Legislation in the United States of America: A Survey, Richmond Journal of Law and Technology, Volume 7, Issue 3
36. Xiobang LI & Yongfeng Qin, Research on Criminal Jurisdiction of Computer cybercrime, 8th International Congress of Information and Communication Technology, 2018.
37. Sophie Victoria Ann Richardson and Nicholas Gilmour, Cyber Crime and National Security: A New Zealand Perspective, Studying Group on Organised Crime.
38. Jonathan Clough, Principles of Cybercrime, Cambridge Univesity Press, United States.
39. Sahira Jati Pratiwi, Steven Adinda Destaloka and Putri Permatasar, The Application of e-Court as an Effort to Modernize the Justice Administration in Indonesia: Challenges & Problems, Indonesian Journal of Advocacy and Legal Services, Vol. 2, No. 1, 2020.
40. Cyber threats to family offices How a resilient approach in the family office can thwart today's cyber threats, Deloitte private.

41. Rob van den Hoven van Genderen, Cybercrime investigation and the protection of personal data and privacy, Economic Crime Division Directorate General of Human Rights and Legal Affairs Strasbourg, France, 2008.

عاشرا : المواقع الالكترونية

عماد أكضيض، إشكالية السياسة الجنائية والعقابية ودور التوجهات الحديثة في مكافحة ومنع الجريمة، بحث منشور، على الموقع ، https://lm.facebook.com/l.php?u=https%3A%2F%2Fdrive.google.com، تم زيارة الموقع بتاريخ 2021/10/17

Abstract

The expansion and development of the framework of electronic crimes have become a reality in view of the information revolution and the tremendous development in modern means of communication, to the point that there are objective and procedural problems raised by electronic crimes at the legislative and practical levels.

This research aim was compared to some contemporary Arab legislation as well as to French and American legislation to assess the extent of the legislative deficiency to confront and combat cybercrime.

In the first chapter, we discussed the scope of the objective protection established in view of the current state of technological and technical development in the world. In addition, we discussed the nature of the electronic crime as well as the implications of this technological development and its unfavourable uses, which significantly compromised physical safety. Where the right to physical integrity is regarded as a fundamental reason that the criminal legislator seeks to ensure its protection, whether in terms of physical harm to the integrity of the body or on the moral, psychological, and environmental levels, The researcher discovered that there is a significant distinction between traditional crimes and electronic crimes. The former is distinguished by being crimes of a special essence, as they are among the soft crimes that are challenging to prove and trace evidence of committing, as well as being among the crimes that are committed quickly and easily across borders, and it is challenging to search for evidence stating Proving the criminal incident.

In the second chapter on prescriptive security and techniques of investigation and inspection of electronic crimes in view of technological development, the research topic was discussing the processes of searching for and

investigating electronic evidence and what challenges the competent agencies face in proving electronic crime both at the local and international levels. We also discussed the mechanisms of primary investigation. What are the most recent techniques for proving cybercrime, how can the accused be followed up on using electronic monitoring, and how different are the methods of investigation for cybercrime and traditional crimes?

The researcher's investigation led to several findings, the most significant of which is that, in view of this extensive and swift technological and technical development, the traditional texts in the penal laws cannot address the apparent spread of electronic crimes. conventional offences. The proposed law of a legal policy that keeps up with the development experienced by the world on the economic, social, and political levels has also played a small but significant role in the development of public criminal policy in some European and Arab countries.

University of Kerbala

College of Law

Branch of Public law

Crimes arising from technological development and their impact on criminal policy

A thesis submitted to the Council (college of Law)
University of Karbala

It is part of the requirements for a PhD in Philosophy in Public Law

Written by student

Ahmed Sabah Abdul Kareem

Supervised by

Prof. Dr. Ali Hamza Asal Al-Khafaji

1444 A. H. **2023 A. D.**