جامعة زيان عاشور بالجلفة
كلية الحقوق والعلوم السياسية
قسم الحقوق (قانون عام)

عنوان المذكرة :

مكافحـــة الجريمـــة الإلكترونيـــة

مذكرة ضمن متطلبات نيل شهادة الماستر في الحقوق

تخصص : **القانون الجنائي والعلوم الجنائية**

من إعداد الطالبين :
- لمعـــرق منيـــر
- عمـــارة خليـــل

تحت إشراف الأستاذة:
- خلـــدون عيشـــة

لجنـــة المناقشة

أ/د	فيرم فطيمة الزهرة	رئيســـا
أ/د	خلـدون عيشـــة	مشرفا ومقررا
أ/د	عسالـي صبـاح	ممتحنـــا

السنة الجامعية : 2022/2021

{فَأَمَّا الزَّبَدُ فَيَذْهَبُ جُفَاءً وَأَمَّا مَا يَنْفَعُ النَّاسَ
فَيَمْكُثُ فِي الْأَرْضِ كَذَلِكَ يَضْرِبُ اللَّهُ الْأَمْثَالَ}

سورة الرعد ، الآية 17.

إهـــداء

الحمد لله و الصلاة على أشرف خلق الله سيدنا محمد صلى الله عليه وسلم

أهدي ثمرة جهدي هذا إلى من أعطاني الحب و الحنان

و التي لا تقدر بثمن ..... والدتي

أقدم هذا العمل

إلى سبب وجودي في الحياة .... أبي الحبيب

لك كل التجلي و الإحترام

الدكتور دحية عبد اللطيف

إلى الدكتورة المشرفة" خلدون عيشة "الذي أمدتنا بتوجيهات طيلة بحثنا

فكانت نعم المشرف حيث وجهتنا حين الخطأ وشجعنا عند الصواب

إلى كل من وقف بجانبي ولا أنسى جميع أصدقائي

إلى كل من كان له فضل علي في هذا العمل ولو بكلمة طيبة

أهدي هذا البحث المتواضع راجيا من المولى عز وجل

أن يجد القبول والنجاح.

مقدمـــــــة

مقدمة :

إن الجريمة ظاهرة قديمة ، عرفتها المجتمعات البشرية منذ القدم ، وظهرت في المجتمعات السلطة الحاكمة إنطلاقا من رب الأسرة إلى شيخ القبيلة ، حيث وضعت بعض القيود على تصرفات الأفراد لإستتباب الأمن لدى الفرد والمجتمع ، وإعتبرت أن كل فعل يمس أمن الجماعة أو حياة الفرد أو ماله أو سلامته الجسدية فعلا مجرما يستوجب العقاب المناسب .

لكن بعد ظهور وتطور فكرة الدولة تولت هذه الأخيرة بنفسها سلطة تجريم الأفعال ، حيث أصدرت القوانين والتشريعات ، منها ماهو موضوعي يجرم الأفعال ويحدد العقوبات لها ، ومنها ما هو إجرائي حيث يحدد الإجراءات الواجب إتباعها .

غير أنه وبتطور المجتمعات في مجال التكنولوجيا العلمية والآلية ، ظهر الكمبيوتر والشبكات الإلكترونية ، حيث غزت هاتين الوسيلتين جميع المجالات ، لما تتسم بها من الدقة في إنجاز الأعمال والسرعة في التنفيذ ، كل هذا أدى إلى ظهور نوع جديد من الجرائم ، وكذا نوع آخر من المجرمين وهو ما يعرف بالجرائم الإلكترونية والمجرم الإلكتروني ، كما أنه يعتبر الإنعكاس السلبي لهذه الثورة العلمية ، حيث تعتبر الجريمة الإلكترونية الإبن الغير شرعي الذي جاء نتيجة للتزاوج بين الثورة التكنولوجية والعولمة .

ولم يتفق الفقه على تعريف جامع للجريمة الإلكترونية نظرا لغياب تعريف قانوني لهذا النوع من الجرائم في أغلب التشريعات بالإضافة إلى غيب مصطلح موحد للدلالة على الجرائم الناشئة عن الإستغلال الغير قانوني لتقنية المعلومات وإستخدامها ، ومن هنا برز لنا إتجاهين مختلفين لمفهوم الجريمة الإلكترونية ، مفهوم ضيق يميل إلى حصر هذه الجريمة في الحالات التي تتطلب كبير من المعرفة وما سواها جرائم عادية ، ومفهوم واسع جاء نتيجة لإنتقاد المفهوم الأول ليشمل إستخدام الكمبيوتر كأداة لإرتكاب الجريمة بالإضافة إلى الحالات المتعلقة بالولوج الغير مصرح به لكمبيوتر أو حساب المجني عليه ، والإطلاع على بياناته أو التعديل فيها أو حذفها .

وما يميز مرتكبي هذه الجرائم دهائهم ونفوذهم وتحكمهم الكبير في هذه التكنولوجيا، مما يصعب إثبات هذه الجريمة ويعيق تحديد هوية مرتكبيها و حتى القبض عليهم، هذا ما أدى إلى تفطن المجتمع الدولي والمنظمات الدولية والإقليمية والذهاب إلى وجوت تعاون شرطي لمواجهة هذه الجرائم من خلال تنسيق الجهود بين الدول والمنظمات، و اتخاذ الإجراءات اللازمة لذلك، خاصة بعد فشل الدول في مواجهة هذا النوع من الجرائم، مما أوجب عليها الدخول في علاقات تعاونية فيما بينها من خلال قواعد القانون الدولي بما لا يتنافى مع مبدأ السيادة الدولية، وهو ما تضمنته العديد من الإتفاقيات والمعاهدات الدولية .

وفي هذا السياق أولت منظمة الأمم المتحدة مسألة مواجهة الجرائم الإلكترونية إهتماما كبيرا ، وهذا من خلال مؤتمرها العاشر الذي كان عنوانه منع الجريمة الإلكترونية ومعاملة المجرمين ، الذي أنعقد في فينا 2000 ، وكذا المؤتمر الحادي عشر لمنع الجريمة الإلكترونية والعدالة الجنائية الذي أنعقد في بانكوك عام 2005 ، كما قامت اللجنة الأوربية بشأن مشاكل الجرائم الإلكترونية ولجنة الخبراء في مجال جرائم الكمبيوتر بإعداد مشروع إتفاقية دولية تتعلق بجرائم الكمبيوتر وهذا في آفريل 2000 ، وقد جاء هذا نتيجة لكثرة الإعتداءات على مواقع الأنترنيت التجارية .

إن الجزائر بإعتبارها واحدة من الدول التي مستها أو تعرضت لمثل هذا النوع من التطور التكنولوجي سواءا بالسلب أو الإيجاب ، فهي أيضا معنية بمكافحة الجرائم الإلكترونية ، فكان لابد من إيجاد إيطار قانوني مناسب لسد الفراغ الإجرائي ، لذلك وضعت مجموعة من الإجراءات منها ما يعتبر قاسما مشتركا بين الجرائم التقليدية والجرائم الإلكترونية عن طريق تعديل قانون الإجراءات الجزائية لتقنين إجراءات ووسائل خاصة تتماشى وطبيعة الجرائم المستحدثة ومنها الجرائم الإلكترونية ، وكذا قانون العقوبات من خلال النصوص والمواد المستحدثة لهذا الغرض .

وبناءا عليه كان لابد من مواكبة التشريعات المختلفة هذا التطور الإجرامي الملحوظ المتمثل في إستخدام الكمبيوتر والشبكات الإلكترونية مثل شبكات الأنترنيت ، فأحيانا قد يؤدي هذا الإستخدام إلى خلق شلل كامل للأنظمة المدنية وحتى العسكرية ، وتعطيل المعدات الإلكترونية ، واختراق النظم المصرفية ، وإرباك حركة الطيران ، وشلل محطات الطاقة ، وبذلك يصل الجاني إلى أي مكان يرغب فيه دون أن يترك أثرا ملموسا ، وهذا من الآثار السلبية للثورة التكنولوجية .

أهمية الدراسة :

تكمن أهمية البحث أساسا في كون الجريمة الإلكترونية جريمة يمتد تأثيرها إلى جميع الأصعدة لإرتباطها بتطور تكنولوجيا الإعلام والإتصال ، والتي تستخدم في جميع مجالات الحياة ، سواءا من طرف الأفراد أو المؤسسات ، وإتخاذ جميع التدابير والإجراءات اللازمة لحماية المجتمع من هذه الجريمة وردع مرتكبيها .

ولعل من أهم الأسباب التي تستوجب التعاون الدولي الأمني والقضائي بين مختلف الدول لمكافحة الجريمة الإلكترونية هو كونها جريمة عابرة للحدود ، وذات إنتشار واسع ، وهذا ما يشكل تحديا يواجه أجهزة الأمن والقضاء ليس في دولة واحدة بل في جميع دول العالم ، مما يستوجب زيادة خبر وتدريب رجال الشرطة الجنائية ليكونو أكثر قدرة على فهم طبيعة وأنشطة الجرائم الإلكترونية ، ومن ثم تدبير أساليب مكافحتها والقضاء عليها .

أسباب إختيار الموضوع :

هناك أسباب ذاتية وأسباب موضوعية

أسباب ذاتية : نذكر منها

- وجود رغبة شخصية في دراسة جانب من جوانب الجرائم المستحدثة
- الزيادة في الرصيد المعرفي
- تعلق الموضوع بعدة جوانب من الحياة (المعاملات التجارية والبنكية والإدارية ... إلخ)
- الموضوع له بعد وطني ودولي وفي غاية كبيرة من الأهمية
- البحث في مثل هذه المواضيع من شأنه تحقيق مكاسب وخبرة في مجال تقنيات البحث العلمي

أسباب موضوعية : نذكر منها

- حداثة الموضوع وكما يطلق عليها الجرائم المستحدثة حيث أن الإنسان لم يعهدها من ذي قبل
- حيوية الموضوع
- إثراء المكتبة الجزائرية بمرجع جديد بسبب وجود نقص فاذح في المراجع المختصة في هذا الموضوع
- كثر وتنوع هذا النوع من الجرائم تستوجب وجود أبحاث تحد منها .

الدراسات السابقة :

نظرا لحداثة الموضوع ، ومن خلال عملية البحث عن المراجع المعلقة بموضوع مكافحة الجريمة الإلكترونية وجدنا البحوث التالية :

-بحث مقدم في مجلة "القانون الدولي للدراسات البحثية" بعنوان : التعاون الدولي في مكافحة الجرائم المعلوماتية ، للدكتورة صورية بوربابة .

-دردور نسيم ، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن ، مذكرة لنيل شهادة الماجستير شعبة القانون الجنائي ، جامعة منتوري قسنطينة ، 2012-2013 .

-معتق عبد اللطيف ، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن ، مذكرة ماجستير ، جامعة الحاج لخضر باتنة ، 2015-2016 .

طرح الإشكالية :

تنتشر الجرائم الإكترونية في العالم إنتشارا سريعا يتماشى مع سرعة التطور التكنولوجي والمعلوماتي ، ما شكل خطرا حقيقيا على الأفراد والمؤسسات سواءا على المستوى المحلي أو الدولي ، فكان لزاما على الدول

والمنظمات الدولية والإقليمية إتخاذ إجراءات حماية من هذه الجرائم ووسائل ردع لمرتكبيها ، وعليه فالإشكالية الرئيسة التي تطرح في هذا الصدد هي :

ماهي السبل القانونية و الآليات المتبعة للحد من الجريمة الإلكترونية سواءا على الصعيد الدولي أو المحلي ؟

وتتفرع هذه الإشكالية إلى طرح بعض الأسئلة فرعية وهي :

- ما مدى نجاعة الإتفاقيات الدولية والإقليمية في مكافحة الجريمة الإلكترونية ؟
- ما هو دور الميكانزمات الدولية في مكافحة الجريمة الإلكترونية ؟
- هل ترقى القوانين والنصوص إلى مستوى الحد من الجرائم الإلكترونية في الجزائر ؟
- ما هي المؤسسات المختصة في مكافحة الجرائم الإلكترونية في الجزائر ؟

منهج الدراسة :

لقد حرصنا في هذه الدراسة ونزولا عند موجبات البحث العلمي ، وكما هو متعارف عليه فإن طبيعة البحث في المواضيع القانونية التي تفرض علينا نوعية المنهج المتبع ، فلقد إخترنا منهجا يلم بدراسة الموضوع بكل جوانبه وهو المنهج الوصفي التحليلي الذي يهدف إلى بيان إجراءات مكافحة الجريمة الإلكترونية ،وكذلك من خلال تحليل المواد والنصوص القانونية والدراسات السابقة ، وتفسير بعد المواد المتعلقة بموضوع الدراسة .

خطة البحث :

لقد تناولنا في بحثنا هذا فصلين الأول يتحدث عن مكافحة الجريمة الإلكترونية على الصعيد الدولي ، حيث بينا الجهود الدولية لمكافحة الجريمة الإلكترونية على صعيد الإتفاقيات (الإتفاقيات الدولية في مطلب أول والإتفاقيات الإقليمية في مطلب ثاني) كل هذا في المبحث الأول ، أما المبحث الثاني فقد تناولنا فيه دور الميكانيزمات الدولية في مكافحة الجريمة الإلكترونية (التعاون الدولي في المطلب الأول ودور الهيئات الدولية في مكافحة الجريمة الإلكترونية في المطلب الثاني)

أما الفصل الثاني فقد تم التركيز على مكافحة الجريمة الإلكترونية في ضل القانون الوطني ، ومنه تناولنا المكافحة التشريعية في المبحث الأول (مكافحة الجريمة الإلكترونية في ضل قانون العقوبات وقانون الإجراءات الجزائية في المطلب الأول وخصص المطلب الثاني لمكافحة الجريمة الإلكترونية في ضل القوانين الخاصة) ، أما المبحث الثاني فقد خصص للمكافحة المؤسساتية (فقد تم تبيان عمل الهيئة الوطنية للوقاية من الجرائم المتصلة

بتيكنولوجيا الإعلام والإتصال في المطلب الأول ، ودور الضبطية القضائية في مكافحة الجريمة الإلكترونية في مطلب ثاني) .

الفصل الأول :

مكافحة الجريمة الإلكترونية على الصعيد الدولي

تمهيد :

تعد الجرائم الحاسوب أو ما يطلق عليها بالجريمة الالكترونية من الجرائم المعلوماتية المعاصرة والعابرة للحدود و التي ظهرت مؤخرا مع الانتشار التكنولوجي خاصة لارتباطها بجهاز الحاسب الآلي، و أداة الجريمة تتمثل في شبكة الانترنت هذه الجريمة التي تثير في مجملها الكثير من الإشكاليات من مختلف النواحي كصعوبة اكتشافها وكذا إثباتها لا سيما و أنها تتسم بطابع الحيلة و الدهاء من طرف مرتكبيها من خلال استعمال تقنيات معلوماتية عالية الكفاءة مما يؤدي إلى اختراق الشبكات وأجهزة الحاسب الآلي المرتبطة بالانترنت حيث يتم اختراق نظام الأمن بالشبكة و الدخول إلى الجهاز للكشف عن محتوياته أو إتلافها و التلاعب بالمعلومات المخزنة فيها.

بالنظر لخطورة هذه الجريمة و صعوبة الكشف عنها و غياب الدليل المادي الذي يدين مرتكبها فإنها أصبحت تطغى على ساحة الإجرام و بشكل كبير نتيجة لغياب إستراتيجية فعالة لمحاربتها و التقليل منها خاصة على المستوى الدولي في ظل قلة الاتفاقيات الدولية وصعوبة التعاون الدولي للحد منها و هذا طبعا بالنظر لطبيعتها الخاصة ، لذا فقد إخترنا في هذا الفصل أن نتحدث على جهود مكافحة الجريمة الإلكترونية على صعيد الإتفاقيات الدولية والإقليمية في المبحث الأول، و دور الميكانيزمات الدولية في مكافحة الجريمة الإلكترونية في المبحث الثاني .

المبحث الأول : جهود مكافحة الجريمة الإلكترونية على صعيد الإتفاقيات الدولية والإقليمية

أصبحت الجرائم الإلكترونية تتصدر قائمة الجرائم العابرة للحدود والتي لا تعترف بالإقليم ، وتهدد الأمن السياسي والاقتصادي والاجتماعي في كافة دول العالم ، لكن وعلى الرغم من تغيير المفاهيم القانونية في سبيل محاربة هذه الجرائم فلازالت هناك مجموعة من الإشكالات والصعوبات التي تعرقل وتقلص من الجهود الدولية الرامية إلى وضع حد لهذه الجرائم ، لذا وجب وضع إتفاقيات دولية وأخرى إقليمة تضمن الحد الأدنى من مكافحة هذا النوع من الجرائم .

المطلب الاول : الإتفاقيات الدولية

تعد الاتفاقيات والمعاهدات الدولية من أهم صور التعاون الدولي بصفة عامة وفي مجال مكافحة الجرائم الإلكترونية بصفة خاصة .ومن بين المعاهدات والاتفاقيات التي تعمل على التعاون الدولي في مجال مكافحة الجرائم الإلكترونية إتفاقية برن ومعاهدة الويبو وإتفاقية تريبس .

الفرع الاول : إتفافية برن

أولا : تعريف الإتفاقية

تعتبر إتفاقية برن الموقعة بتاريخ 1971 في سويسرا حجر الأساس في مجال الحماية الدولية لحق المؤلف ووقعت عليها 120 دولة ، بحيث تم تعديلها سنة 1979 وإرتفع عدد الدول فيها إلى 140دولة في 1999 [1].

وتمنح هذه الإتفاقية صاحب حق المؤلف حق إستئثاري في التصريح بعمل نسخ من المصنفات بأي طريقة وبأي شكل كان ، كما تمنحه الحق في أن يرخص أو يمنح أي ترجمة أو إقتباس أو بث إذاعي أو توصيل إلى الجمهور لمصنفه ، كما تلزم بتوقيع جزاءات سواء كان المؤلف المعتدى عليه وطنيا أو أجنبيا[2].

وبموجب هذه الإتفاقية تتمتع برامج الحاسب الآلي "الكمبيوتر" سواء كانت بلغة المصدر أوبلغة الآلة بالحماية بإعتبارها أعمالا أدبية وفقا لما جاء فيها .

وتهدف هذه الإتفاقية إلى حماية حقوق المؤلفين على مصنفاتهم الأدبية و الفنية ، التي لها أحكاما خاصة لتحديدها مع توضيح شروط حمايتها[1].

---

[1] د. صورية بوربابة ، مجلة "القانون الدولي للدراسات البحثية" بعنوان : التعاون الدولي في مكافحة الجرائم المعلوماتية ، ص ص 11-12 .

[2] د. خلدون عيشة ، محاضرات في الجريمة المعلوماتية ، ملقات على طلبة سنة أولى ماستر قانون جنائي ،كلية الحقوق جامعة الجلفة ، 2021-2022 ، ص 28 .

ثانيا : المبادئ الأساسية لإتفاقية برن

وتقوم هذه الإتفاقية الدولية على مجموعة من المبادئ الأساسية التي تحدد نطاق الحماية الواجبة و أسلوب تطبيقها و المتمثلة في:

1- مبدأ المعاملة الوطنية : أي تمتع كافة المصنفات الخاضعة لحماية الإتفاقية في إقليم دولة عضو بنفس الحماية المتمتعة بها المصنفات الوطنية لدى الدولة الأخرى الطرف في هذه الإتفاقية.

2- الحد الأدنى للحماية : مبدأ هدفه مواجهة التفاوت التشريعي بين مستويات الحماية في الأنظمة القانونية المختلفة ، و بمقتضاه يتمتع المؤلفون بحقوق مادية وأدبية إنطلاقا من تطبيق المساواة بين الوطني والأجنبي ، زيادة على وضع حد أدنى يتعين أن لا تقل عنه الحماية التي تلقاها أي من المصنفات المتمتعة بحماية إتفاقية برن .

الفرع الثاني : معاهدة الويبو

لتوفير الحماية للملكية الفكرية تم تشكيل المنظمة العالمية للملكية الفكرية "ويبو" التي تعتبر منظمة دولية غير حكومية وإحدى الوكالات المتخصصة التابعة لمنظمة الأمم المتحدة ، مقرها جنيف تأسست بموجب اتفاقية ستوكهولم المبرمة سنة 1967 ودخلت حيز التطبيق 1970 وبلغ عدد الدول الأعضاء فيها سنة 1999 170 دولة .

وتهدف هذه المنظمة لدعم الملكية الفكرية في جميع أنحاء العالم و حماية الملكية الصناعية و كذا حماية المصنفات الأدبية و الفنية[2].

وتنقسم معاهدة الويبو إلى ثلاث معاهدات الأولى بشأن حق المؤلف والثانية بشأن الأداء والتسجيل الصوتي والثالثة بشأن الحماية الدولية لحق المؤلف والحقوق المجاورة.

وتهدف منظمة الويبو العالمية للملكية الفكرية إلى :

- تدعيم إتخاذ الإجراءات التي تهدف إلى تسيير الحماية الفاعلة للملكية الفكرية في جميع أنحاء العالم.
- تنسيق التشريعات الوطنية للدول الأعضاء في إطار الحماية الفاعلة للملكية الفكرية على الصعيد العالمي.
- تقديم الخدمات الفنية والقانونية والتدريجية في مجال العمل على الحماية الدولية للملكية الفكرية .

[1] د محمد عد الله أبو بكر سلامة ، موسوعة جرائم المعلوماتية "جرائم الكمبيوتر و الانترنت" ، المكتب العربي الحديث ، الإسكندرية ، 2014 ، ص 155 .

[2] حسف جميعي ، مدخل إلى حق المؤلف و الحقوق المجاورة ، عمل الويبو التمهيدية ، المنظمة العالمية للمكية الفكرية ، القاهرة ، 2004 ، ص ص 3-4 .

– النهوض بأعباء التسجيل في مجال الحماية الدولية للملكية الفكرية ، و أن تنشر البيانات الخاصة بالتسجيلات حيثما كان ذلك ملائما.

مع ملاحظة أنه لمعاهدة الويبو الخاصة بحماية حق المؤلف دور هام في حماية البرمجيات ، إنطلاقا من مادتها الرابعة التي نصت على تمتع برامج الكمبيوتر بالحماية بإعتبارها مصنفات أدبية بالمعنى الوارد في المادة الثانية من إتفاقية برن[1] .

الفرع الثالث : إتفاقية تريبس

أولا : تعريف الإتفاقية

هي إتفاقية مجالها حماية الملكية الفكرية من عمليات السطو الإلكتروني على الأعمال الفنية و تم التوقيع عليها من قبل الدول الأعضاء سنة 1994[2].

لقد تناولت هذه الإتفاقية تحرير التجارة العالمية مع الأخذ في الإعتبار بأمرين هامين

–الأمر الأول : ضرورة توفير جزاءات و تدابير لإنقاذ حقوق الملكية الفكرية دون أن تقف عائقا أمام التجارة الدولية المشروعة.

–الأمر الثاني : العمل على تشجيع الحماية الفاعلة في مجال حقوق الملكية الفكرية بجميع فروعها.

وقد نصت هذه الإتفاقية على مكافحة الجريمة المعلوماتية بالنص من خلال مادتها العاشرة في فقرتها الأولى على أنه تتمتع برامج الحاسب الآلي أو الكمبيوتر سواء كانت بلغة المصدر أو بلغة الآلة بالحماية بإعتبارها أعمال أدبية بموجب معاهدة برن لسنة 1971.

كما نصت ذات المادة العاشرة في فقرتها الثانية على حماية البيانات المجمعة أو المواد الأخرى بشروط معينة.

ولفاعلية هذه المكافحة إشترطت مواد الإتفاقية على الدول الأعضاء لحماية حقوق الملكية :

المادة 41 : إتخاذ إجراءات سريعة لمنع التعديلات و الإنتهاكات الحالة.

المادة 42 : ضرورة توافر إجراءات قضائية ومدنية إلى جانب إجراءات إدارية أخرى .

[1] يتوجي سامية ، معاهدة الويبو بشأن حق المؤلف ، مذكرة تخرج لنيل شهادة الماستر ، جامعة محمد خيضر ، بسكرة ، الجزائر ، 2008-2009 ، ص ص 55-56 .

[2] فاتن حسين حوى، المواقع الإلكترونية وحقوق الملكية الفكرية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن ، 2010 ، ص 139 .

المادة 09 : على الدول الأعضاء الإلتزام بأحكام المواد من 01 إلى 21 من معاهدة برن لسنة ، 1971 مع مراعاة سريان الحماية على المنتوج و ليس على مجرد الأفكار أو الإجراءات أو أساليب العمل و الحماية الزمنية لعديد المصنفات المحددة بطول حياة المؤلف بالإضافة إلى مدة خمسين عاما بعد وفاته .

ثانيا : المبادئ الأساسية لإتفاقية تريبس

وتقوم هذه الإتفافية على عدة مبادئ تتمثل في[1]:

1- مبدأ المعاملة الوطنية : ألزمت المادة الثالثة من الإتفاقية كل دولة عضو بأن تمنح الأجانب المنتمين إلى دولة أخرى من الدول الأعضاء معاملة لا تقل عن تلك الممنوحة لمواطنيها في شأن حماية الملكية الفكرية[2].

2- مبدأ الدولة الأولى بالرعاية : أوجبت المادة الرابعة من الإتفاقية على الدول الأعضاء أن تمنح المنتمين إلى كافة الدول فوار وبدون أية شروط ، أية مزايا ، أو حصانات أو معاملة تفضيلية تمنحها للمنتمين إلى أي دولة أخرى متعلقة بحماية حقوق الملكية الفكرية .

3- وضع حد أدنى من الحماية القانونية : مكنت الإتفاقية أي دولة عضو من تقديم حماية قانونية تفوق الحماية المقدرة في إتفاقية تريبس ، ولكن لا يجوز لها أن تقرر حماية أدنى مما قررته الإتفافية .

4- وقت إنفاذ إتفاقية تريبس : بسبب كون الدول الصناعية المتقدمة المتضررة الأولى من قرصنة الملكية الفكرية ، فقد حاولت إجبار العديد من الدول النامية لتطبيق الإتفاقيات والحد من القرصنة والتزوير والتقليد ، ولكنها لم تتوصل إلى عقد إتفاقية تريبس بسبب ما يتطلبه الأمر من مرونة في إلزام الدول بأحكامها التي يتطلب تطبيقها فترات زمنية إنتقالية .

5- المعاملة التفضيلية للدول النامية : أرادت إتفاقية تريبس من خلالها تمكين الدول النامية من إنشاء قاعدة تكنولوجية متطورة تخدم مصالحها الإقتصادية وتمكنها من اللحاق بعجلة التجارة الدولية .

[1] محمود فياض، المعاصر في قوانين التجارة الدولية، د ط، مؤسسة الوراق للنشر والتوزيع، الأردن ، 2012 ،ص 370.

[2] عماد الدين محمود سويدات، الحماية المدنية للعلامات التجارية، الطبعة الأولى، دار الحامد للنشر والتوزيع، الأردن، 2012 ، ص 157 .

المطلب الثاني : الإتفاقيات الإقليمية

لعبت المنظمات الإقليمية دور جد مهم في مكافحة الجريمة الإلكترونية وذلك من خلال مساهمتها في عقد مؤتمرات وإتفاقيات بغرض مكافحة الجريمة الإلكترونية ، وبهذا سوف نبين أهم الجهود الإقليمية في هذا المجال.

الفرع الأول : معاهدة بوادست

أولا : تعريف المعاهدة

شهدت العاصمة المجرية بودابست في أواخر عام 2001 أولى المعاهدات الدولية التي تكافح الجرائم الإنترنت وتبلور التضامن والتعاون الدولي في محاربتها ، ومحاولة الحد منها خاصة وأن هذه الجرائم أصبحت تهدد الأملاك و الأشخاص[1].

وقد قام بصياغتها عدد كبير من الخبراء القانونيين في مجلس أوروبا بمساعدة دول أخرى ، لاسيما الولايات المتحدة الأمريكية بعد مشاورات عديدة بين الحكومات وأجهزة الشرطة وقطاع الكمبيوتر على مستوى العالم ، وصولا في النهاية للتوقيع عليها من قبل 30 دولة بتاريخ 2001/11/23 لمواجهة ما يسمى بالجرائم المعلوماتية[2].

ورغم أن هذه المعاهدة أوروبية حديثة الميلاد إلا أنه تم التوقيع عليها من قبل دول لا تعتبر أعضاء في مجلس أوروبا مثل كندا واليابان والولايات المتحدة الأمريكية و جنوب إفريقيا .

تكونت هذه الاتفاقية من 48 مادة تؤكد من خلالها على ضرورة اتخاذ تدابير تشريعية لمكافحة جرائم الحاسوب و مخاطرها على الدول ، كما تضمنت العديد من التوصيات للدول الأعضاء من أجل محاربة الجريمة المعلوماتية بإعتبارها مرجعا في ميدان محاربة الإجرام السيبيرياني ، سواء بالنسبة للإتفاقيات اللاحقة ذات الصلة بها أو بالنسبة للتشريعات الداخلية لبعض الدول.

ثانيا : العناصر الأساسية لاتفاقية بودابست:

1/أهمية التدابير التشريعية الموضوعية أي نصوص التجريم الموضوعة لهذا المجال

2/أهمية التدابير التشريعية الإجرائية المتلائمة مع طبيعة الجرائم الإلكترونية.

---

[1] منير محمد الجهيني، ممدوح محمد الجهيني، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر العربي، الإسكندرية ، ط ، 2004 ، ص9 .

[2] علي جبار الحسناوي ، جرائم الحاسوب و الانترنت ، دار اليازوري ، الاردن ، 2009 ، ص ص 147-148 .

3/أهمية تدابير التعاون الدولي والإقليمي في مجال مكافحة هذه الجرائم والانطلاق مما أنجز من جهود دولية وإقليمية في هذا المجال.

ثالثا : فصول اتفاقية بودابست

الفصل الأول : تضمنت مواده تعريف للمصطلحات الأساسية.

الفصل الثاني :عنوانه الخطوات الواجب اتخاذها على الصعيد الوطني و يضم ثلاثة أقسام

القسم الأول: تضمن المواد من 2 إلى 13 والتي تعالج النصوص الموضوعية لجرائم الحاسوب.

القسم الثاني : يتكون من المواد 14 إلى 21 والتي تتعلق بالقواعد الإجرائية.

القسم الثالث : يتكون من المادة 22ويتعلق بالاختصاص.

الفصل الثالث : عنوانه التعاون الدولي و يضم المواد من 23 إلى 35 .

الفصل الرابع : يتضمن الأحكام الختامية و يضم المواد من 36 إلى 48 .

رابعا : تصنيف الجرائم المعلوماتية في الاتفاقية :تم من خلال 5 عناوين في قسمها الأول تتمثل في :

الطائفة الأولى: الجرائم التي تستهدف عناصر أمن المعلومات

تضم جوهر جرائم الحاسوب والتي تعرف بالجرائم ضد سرية البيانات وسلامتها وسلامة النظام و إتاحة البيانات والنظم.

الطائفة الثانية:الجرائم المرتبطة بالكمبيوتر

تضم الانتهاكات الممارسة بواسطة الحاسب الآلي التي تمس بعض المصالح القانونية التيتحميها قوانين العقوبات ، و تضم أيضا جرائم الغش المعلوماتي و التزوير المعلوماتي[1].

الطائفة الثالثة : الجرائم المرتبطة بالمحتوى

تشمل الإنتهاكات و الجرائم المرتبطة بالمحتوى و التي تخص الإنتاج و النشر غير المشروع للمواد الإباحية الطفولية عبر النظم المعلوماتية.

الطائفة الرابعة: الجرائم المرتبطة بحق المؤلف و الحقوق المجاورة

تشمل الجرائم الجنائية التي تعد إعتداء على المصنفات المحمية بحق المؤلف والحقوق المجاورة .

الطائفة الخامسة: المساهمة الجرمية و العقوبة

[1] اسامة مهمل ، الاجرام السيبيراني ، مذكرة لنيل شهادة الماستر ، جامعة محمد بوضياف ، المسيلة ، 2017-2018 ، ص 33 .

بها أحكام إضافية تخص عملية الشروع والاشتراك في هذه الجرائم وكذا الجزاءات والتدابير طبقا للمعايير الدولية الحديثة بالنسبة لمسؤولية الأشخاص المعنوية.

خامسا : أنواع الجرائم الإلكترونية التي تضمنتها تصنيفات إتفاقية بودابست:

أوجبت الإتفاقية نوع جديد من التقسيمات بشأن جرائم الكمبيوتر المختلفة و أحكامها (القواعدالموضوعية) ، بحيث تتضمن أربع طوائف رئيسية لجرائم الكمبيوتر وأخرى خامسة تتعلق بأحكام المساهمة والعقوبات لهذه الجرائم الأربعة ، بحيث تقسم هذه الطوائف إلى تسع جرائم في ميدان الجرائم المعلوماتية تلزم الإتفاقية الدول الأعضاء فيها وأي دولة توقع عليها أو تريد الإنضمام إليها بإتخاذ الإجراءات والتدابير التشريعية الملائمة بتجريمها.

الطائفة الأولى: الجرائم التي تستهدف عناصر أمن المعلومات : وتشمل على[1] :

1/جريمة الدخول غير القانوني المتعمد : مصطلح إستعملته الإتفاقية في حين أن غالبية التشريعات الوطنية تستخدم تعبير الدخول غير المصرح به ، و ذلك بالدخول المتعمد إلى نظام كمبيوتر أو جزء منه دون حق أو إذن سواء كان بنية إنتهاك وسائل الأمن أو بنية الحصول على معطيات الكمبيوتر أو لأية نية غير مشروعة.

2/جريمة الإعتراض غير القانوني : المتعمد و دون حق بواسطة وسائل تكنولوجية للبيانات المرسلة غير العامة إلى أو من نظام كمبيوتر ، وكذلك إعتراض الإشعاعات الكهرومغناطيسية المنبعثة من أي نظام كمبيوتر تحمل هذه المعطيات .

3/جريمة التدخل المتعمد أو الإرادي في المعطيات : بالتدمير أو الحذف أو التشويه والإفساد أو تبديلها أو تغييرها أو تعديلها أو تعطيلها أو كبتها أو إخمادها.

4/جريمة التدخل المتعمد في نظم الحاسوب :عن طريق إرسال ذات الأفعال المشار إليها في المادة الرابعة من الإتفاقية والمتعلقة بالتدخل في المعطيات من أجل تعطيل أداء وعمل الأنظمة بالتدمير والحذف و التعديل و التعطيل.

5/جريمة إساءة إستخدام الأجهزة : وهي جريمة تحتوي نوعين من الأفعال ، النوع الأول يتعلق بالأفعال المنصوص عليها في الفقرة الأولى من المادة السادسة ، وتشمل الإنتاج المتعمد أو بيع أو شراء أو إستخدام أو إستيراد أو توزيع أو غير ذلك أدوات ووسائل توفير الأجهزة بما فيها برامج الكمبيوتر لإرتكاب أي جريمة من المذكورة في المواد من 2 إلى 5 السالفة الذكر، و كذلك كلمات السر ورموز الدخول أو أية برامج مشابهة تتيح

[11] د. خلدون عيشة ، المرجع السابق ، ص 32 .

إختراق نظام الكمبيوتر و الدخول إليه أو أي جزء منه بنية إرتكاب أي جرم من الجرائم المذكورة في المواد من 2 إلى 5 السالفة الذكر.

كما تشمل هذه الجريمة وفق الفقرة الثانية من المادة السادسة الحيازة والتملك لأي عنصر أو أداة لإرتكاب أي من الأفعال المشار إليها في المواد من 2 إلى 5 من الإتفاقية .

الطائفة الثانية: الجرائم المرتبطة بالكمبيوتر : و تشمل على :

1/جريمة التزوير المتعمد بإستخدام جهاز الكمبيوتر :عن طريق إدخال أو تعديل أو حذف أو إخفاء بيانات الكمبيوتر على نحو يظهر بيانات غير أصلية وكأنها أصلية وقانونية بغض النظر عن كونها مقروءة أو غير مقروءة.

2/جريمة الإحتيال المتعمد بإستخدام الكمبيوتر : بدون حق و على نحو يسبب خسارة الغير لممتلكاته عن طريق إدخال أو حذف أو تعديل أو كتم بيانات الكمبيوتر ، أو من خلال التنقل بعمليات نظام الكمبيوتر أو برامجه بنية الحصول على منفعة إقتصادية لنفسه أو لغيره.

الطائفة الثالثة: الجرائم المرتبطة بالمحتوى : وتشمل على:

–الجرائم المرتبطة بدعارة الأطفال : وهي جرائم كثيرة المحتوى ترتكز على ضرورة تجريم أي شخص و بشكل عمدي عرض أو توزيع أو نقل أو غير ذلك من الأفعال التي توفر أو تتيح توفير المواد الإباحية المتعلقة بالأطفال.

الطائفة الرابعة : الجرائم المرتبطة بحق المؤلف و الحقوق المجاورة : وتشمل على[1] :

–الجرائم المرتبطة بحق المؤلف :تناولت الإتفاقية وجوب إتخاذ الدول المنظمة لها تدابير تشريعية تجرم الإخلال أو الإعتداء على حق المؤلف أو الحقوق المجاورة وفقا لمدة تحددها القوانين الوطنية للدول الأعضاء المتوافقة مع إتفاقية برن لحماية المصنفات الأدبية والفنية ، وإتفاقية تريبس وإتفاقية الويبو لحق المؤلف وإتفاقية الأداء والمنفوغرامات ، بشرط أن تكون هذه الأفعال قد ارتكبت عمدا و بغرض تجاري و بإستخدام نظام الكمبيوتر.

الطائفة الخامسة : المساهمة الجرمية و العقوبة : ويعالج هذا الجزء كل من :

1/الشروع و المساعدة و التحريض :أوجبت الإتفاقية على الدول الأعضاء إتخاذ تدابير تشريعية للنص على المسؤولية عن الشروع والتدخل والتحريض في إرتكاب هذه الجرائم وما تتخذه من إجراءات ردعية .

2/مسؤولية الأشخاص المعنوية : نصت الإتفاقية على مسؤولية الأشخاص المعنوية على الأفعال التي ترتكب لمصلحة الشخص المعنوي ، من قبل أي شخص الذي يتصرف لمصلحته سواء كان إستنادا إلى تمثيل قانوني أو

[1] نفس المرجع ، ص 33 .

بإعتباره مناطا به إتخاذ القرار عن الشخص القانوني ، أو لأنه خاضع لسلطته بما في ذلك أفعال التحريض والتدخل والمساعدة الجنائية .

3/معايير العقاب : أوجبت الإتفافية على الدول الأعضاء فيها إقرار العقوبات الملائمة والفعالة لهذه الجرائم ، بما فيها العقوبات المانعة للحرية بالنسبة للأشخاص الطبيعيين مثل ما هو الحال في القانون الأمريكي والغرامات المالية للأشخاص المعنوية.

سادسا : الشروط الواجب توفرها في الأفعال لكي تأخذ وصف الجريمة المعلوماتية

1/أن ترتكب الجرائم المذكورة في الاتفاقية دون وجه حق.

2/أن ترتكب الجرائم المذكورة بطريقة عمدية من أجل إقرار المسؤولية الجنائية.

سابعا : الإلتزامات المفروضة من قبل إتفاقية بودابست على الدول الأعضاء

أكدت الاتفاقية على الدول عند وضعها لتشريعاتها الداخلية الخاصة بالجرائم المعلوماتية مراعاة الاتفاقيات الدولية لحقوق الإنسان، مثل الاتفاقية الأوروبية لحماية حقوق الإنسان والحريات الأساسية لعام ، 1950 والميثاق الدولي للحقوق المدنية و السياسية لسنة 1966 وكذلك الاعتماد على معايير معينة لتقرير الاختصاص القضائي حول الجرائم المقررة في هذه الاتفاقية و المتمثلة في مبدأ الإقليمية و مبدأ نسبية الاختصاص المكاني ومبدأ الجنسية.

ثامنا : أهداف اتفاقية بودابست

1/السعي لتحقيق وحدة التدابير التشريعية بين دول الأوروبية و دول المنظمة لهذه الاتفاقية من غير الدول الأوروبية.

2/التأكيد على أهمية التعاون الدولي والإقليمي في ميدان مكافحة الجرائم الالكترونية ، وإيجاد مرجعية ودليل إرشادي للتدابير التشريعية الوطنية في ميدان مكافحة الإجرام الإلكتروني[1].

3/ضرورة فعالية خطط العمل لمكافحة الأنشطة التي تستهدف سرية و سلامة و توفر المعلومات و أنظمة الكمبيوتر و شبكاته ، و أنشطة إساءة استخدامها بما في ذلك تحديد الإطار الموضوعي لهذه الأنشطة و الإطار الإجرائي لها.

4/تحقيق التوازن بين حماية حقوق الإنسان الأساسية المعترف بها بموجب اتفاقية مجلس أوروبا لحماية حقوق الإنسان و حرياته لعام 1950 و العهد الدولي للحقوق المدنية والسياسية لعام 1966 والاتفاقيات الأخرى الدولية الخاصة بالحقوق المتصلة بالرأي وحرية الوصول إلى المعلومات وحرية البحث والتلقي والنقل للمعلومات

[1] نفس المرجع ، ص 36 .

والأفكار، ومراعاة الحق في الخصوصية وحيازة المعلومات والاستفادة من عناصر الملكية الفكرية فهي معاهدة تسعى لإحترام حقوق الإنسان و الحد من تعرضه لجرائم الإنترنت.

تاسعا : الاجراءات الجنائية الجديدة لمكافحة الجريمة الالكترونية في اتفاقية بودابست:

وضعت هذه الاتفاقية مجموعة من الإجراءات الجديدة التي تقوم على مبدأ أساسي يتمثل في التزام الدول الأعضاء بإقرار الإجراءات التشريعية، و إجراءات أخرى عند الضرورة بما يتناسب مع قوانينها الداخلية ومجالها القضائي والمتمثلة خاصة فيما يلي :

1/الحفظ السريع للمعطيات المخزنة : إجراء نصت عليه المواد 16 و 17 من الاتفاقية ، و يقصد به الاحتفاظ بالمعلومات السابقة و تخزينها مع حمايتها مما يفسدها أو يتلف نوعيتها وهو إجراء قانوني جديد لكشف الجريمة المعلوماتية والمرتكبة بواسطة شبكة الانترنت.

وسبب إستحداث هذا الإجراء الجديد هو سرعة تغير البيانات المعلوماتية و فاعليتها للتلاشي و التلاعب بها بمحوها أو تدميرها، فيسهل فقدان أدلة إرتكاب الجريمة المعلوماتية ، لذا أكدت المادة 16 من الاتفاقية على تمكين السلطات الوطنية المختصة من إصدار أمر بحفظ البيانات عن طريق أمر قضائي أو أمر إداري أو أي طريق مماثل للتفتيش أو إصدار أمر بالاطلاع.

2/تجميع المعلومات الخاصة بالمشتركين : نصت هذه الاتفاقية على أهمية المعلومات الخاصة بالمشتركين لتحديد هوية الفاعل في الجريمة المعلوماتية ، بحيث تتضمن هذه المعلومات حفظ رقم الهاتف أو عنوان البريد الالكتروني أو عنوان الموقع أو ... الخ.

3/التفتيش المعلوماتي : و قد نصت عليه المادة رقم 19 من الاتفاقية التي بينت أنه يجب توفر شرط الحصول على إذن رسمي للتفتيش ، بعد الإعتماد بتوفر بيانات في مكان محدد يساعد على إثبات وقوع جريمة معلوماتية محددة بمقتضى القوانين الداخلية ، وتفتيش البيانات المعلوماتية والمعطيات المجمعة بعد الحصول على الإذن الرسمي للتفتيش .

كما نصت المادة رقم 31 على وجوب وجود أحكام إجرائية إضافية لضمان الحصول على البيانات المراد إستعمالها كدليل[1].

4/اجراءات التنصت : هو إجراء جديد في إطار المكافحة الإجرائية للجريمة المعلوماتية ، ويتميز بأنه خاص قد يمس بحقوق الأفراد الخاصة لذا لا يعتد به كإجراء قانوني إلا إذا اتخذ بموافقة السلطات القضائية ، و مفاده اعتراض

[11] نفس المرجع ، ص 37 .

المراسلات التي تتم عن طريق وسائل الاتصال السلكية و اللاسلكية كالخطوط الهاتفية مثلا ، و وضع الترتيبات التقنية بدون موافقة المعنيين من أجل التقاط اتصالات و تسجيلات كلامية لشخص أو عدة أشخاص في أماكن عمومية أو خاصة أو التقاط صور لشخص أو عدة أشخاص يتواجدون في أماكن خاصة لوصول وذلك كله من أجل التحري وإلى أدلة تثبت قيام جريمة معلوماتية .

5/التعاون الدولي : لتفعيل الإجراءات السابقة نصت الاتفاقية في مادتها 23 على ضرورة تعاون الدول فيما بينها في أوسع نطاق ممكن لكشف هذا النوع من الجرائم مع مراعاة تقليل الصعوبات التي تواجه تبادل المعلومات والأدلة حتى تتم بصورة سريعة على المستوى الدولي.

كما قامت هذه الاتفافية بتحديد المفهوم العام لإلتزام التعاون الدولي في مجال الجرائم المعلوماتية، و كذا الأحكام الخاصة بتسليم المجرمين وأحكام خاصة وشروط أخرى في حالات جرائم معلوماتية معينة.

6/**الطابع التوجيهي الملزم لهذه الاتفاقية** :نصت عليه المادة 2 منها والتي أقرت أنه يلتزم كل عضو فيها بإصدار تشريع و اتخاذ الإجراءات الضرورية لكشف الجريمة و تطبيق الجزاءات المقررة قانونا في حالة الارتكاب المعدي لها.

7/التأكيد على التحديد الدقيق للمصطلحات الجديدة :أثارت هذه الاتفاقية مشكلة تحديد المصطلحات القانونية المستعملة في مجال المكافحة الإجرائية للجريمة المعلوماتية ، من حيث كونها تستعمل المصطلحات المستعملة في الجرائم التقليدية كمصطلح التفتيش والضبط أو تستخدم مصطلحات جديدة تتماشى مع ما يحدث من تطور تكنولوجي.

وكنتيجة تعد اتفاقية بودابست المنعقدة سنة 2001 بمثابة إرساء لإتفاق دولي يمثل رؤية موحدة للإجرام التقني أو المعلوماتي و إحاطته بسياج قانوني يسمح بالتعامل معه ومواجهته.

الفرع الثاني : إتفافية المجلس الأوروبي لسنة 2004

أولا : تعريف الإتفاقية

تعد إتفافية الجرائم المعلوماتية للمجلس الأوروبي من أحدث الإتفاقيات لمكافحة الجريمة المعلوماتية على المستوى الدولي، و التي صدرت عن المجلس الأوروبي بعد أن وقعت عليها 32 دولة ودخلت حيز التطبيق بتاريخ 2004/07/01 .[1]

[1] عبد الله سيف الكيتوب ، الاحكام الاجرائية لجريمة الاحتيال المعلوماتي ، دار النهضة العربية ، القاهرة ، 2013 ، ص 190 .

ثانيا : الجرائم المتناولة من خلال هذه الإتفاقية

نصت على الجرائم الماسة بالنظام المعلوماتي مبينة أساليب التحقيق فيها ، و المتمثلة في كل من الجرائم المرتكبة ضد سرية و تكامل وتوافر البيانات أو نظم الحاسبات كجرائم التدخل و الإختراق عل أجهزة الحاسبات الآلية ، والجرائم المتصلة بالمحتوى والمتعلقة بالجرائم الخاصة بالإنتاج أو النشر غير المشروع للمواد الإباحية الطفولية عبر النظم المعلوماتية ، والجرائم المتضمنة إنتهاكا لحقوق الملكية الفكرية .

ثالثا : الأساليب الإجرائية في هذه الإتفاقية

وتتمثل في :

1-إرساء كل من إجراء التفتيش و ضبط أنظمة الحاسبات الآلية.

2-إجراء الحفظ السريع لبيانات الحاسب المخزونة التي تم جمعها و حفظها فعليا بمعرفة حائز البيانات.

3-إجراء الأمر بإصدار نسخة من البيانات و الذي يمكن السلطات من إجبار الشخص على تقديم بيانات الحاسب المخزنة أو أحد عناوينISP (Internet Service Provider) المعنية و التي تساهم في التوصل إلى معلومات حول المشترك.

4-إجراء إعتراض بيانات المحتوى و التي تعني إعتراض محتوى الإتصال سواء كان رسالةأو معلومة منقولة.

5-المساهمة في إنشاء وحدة(EUROJUT) والتي مهمتها التعاون بين دول الإتحاد الأوروبي، المجسد بتعاون السلطات القضائية في مكافحة الجريمة المعلوماتية بإصدار إجراء جديد جماعي يتمثل في أمر القبض الأوروبي MandatdarrêtEuropéen الذي يسمح بتسليم المجرم المعلوماتي بسرعة في أي دولة من دول الإتحاد الأوروبي .

الفرع الثالث : القانون العربي النموذجي الإسترشادي لمكافحة الجريمة المعلوماتية

أولا : تعريف القانون

يعد هذا القانون خطوة فعالة في مجال مكافحة الجريمة المعلوماتية خاصة في المجتمعات العربية التي عرفت كغيرها من الدول إنتشار هذه الجريمة العابرة للحدود.

و قد كان هذا القانون ثمرة عمل مشترك قدم بشكل مشروع لمكافحة الجريمة المعلوماتية منقبل كل من مجلس وزراء الداخلية العرب و مجلس وزراء العدل العرب في نطاق الأمانة العامة لجامعة الدول العربية[1].

[1] عبد الله عبد الكريم عبد الله ، جرائم الكمبيوتر والمعلوماتية ، الجرائم الإلكترونية دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والانترنت مع الإشارة إلى جهود مكافحتها محليا ودوليا ، منشورات الحلبي الحقوقية، بيروت، لبنان، 2007 ، ص 140 .

وقد تم إعتماد هذا القانون النموذجي من قبل مجلس وز اراء العدل العرب في دورته 19بالقرار رقم 495د ، 19-08/10/2003 ومجلس وزراء الداخلية العرب في دورته 21 بالقرار رقم -417د-. 21/2004 ويعتبر بمثابة قرار بشأن مشروع قانون عربي إسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها و يتكون من 27 مادة .

ثانيا : الجرائم المدرجة ضمن القانون العربي النموذجي

تتمثل في :

1- جريمة غسل الأموال عبر الوسائط الإلكتروني :

تنص المادة رقم 19 من القانون العربي النموذجي لمكافحة الجريمة المعلوماتية على أنه : كل من قام بتحويل الأموال غير المشروعة أو نقلها أو تمويه للمصدر غير المشروع لها أو إخفائه أرقام بإستخدام أو إكتساب أو حيازة للأموال ، مع العلم بأنها مستمدة من مصدر غير مشروع أو بتحويل الموارد أو الممتلكات مع العلم بمصدرها غير المشروع وذلك عن طريق إستخدام الحاسب الإلكتروني أو شبكة المعلومات الدولية بقصد إضفاء الصفة المشروعة على نلك الأموال يعاقب ، وتترك العقوبة وفقا لتقدير كل دولة .

2- جريمة التزوير المعلوماتي :

نصت المادة رقم 04 من القانون العربي النموذجي الموحد بشأن مكافحة الجريمة المعلوماتية في فقرتها الأولى على أنه : "كل من زور المستندات المعالجة آليا أو البيانات المخزنة في ذاكرة الحاسوب أو على شريط أو إسطوانة ممغنطة أو غيرها من الوسائط يعاقب ، و تترك العقوبة وفقا لتقدير الدولة...".

كما تضيف ذات المادة في فقرتها الثانية على أنه كل من استخدم المستندات المعالجة آليا مع علمه بتزويرها يعاقب بنفس عقوبة فعل التزوير.

3- جريمة إختراق النظم المعلوماتية :

تنص المادة رقم 03 من القانون العربي النموذجي الموحد لمكافحة الجريمة المعلوماتية على أنه : "كل من توصل بطريقة التحايل لإختراق نظم المعالجة الآلية للبيانات يعاقب بالحبس والغرامة (تترك العقوبة لتقدير كل دولة) ، و إذا نتج عن هذا الفعل محو أو تعديل للبيانات المخزنة بالحبس أو تعطيل تشغيل النظام بسبب تسريب للفيروسات أو غيرها من الأساليب المعلوماتية ، تكون العقوبة الحبس و الغرامة المالية"[1].

و تتحقق جريمة إختراق النظم المعلوماتية بإرتكاب :

[1] د. خلدون عيشة ، المرجع السابق ، ص 40 .

أ-كل من جريمة أو البقاء غير المشروع في النظام المعلوماتي بأي وسيلة تقنية كإنتهاك كلمة السر الحقيقية أو عن طريق إستخدام برنامج أو شفرة خاصة.

ب-فعل إعاقة تشغيل نظم معالجة البيانات بفعل التعطيل بأي وسيلة كانت كتسريب الفيروسات.

ج-المحو بإزالة جزء من المعطيات المسجلة على الدعامة الموجودة داخل النظام أو تحطيم تلك الدعامة أو نقل أو تخزين المعطيات إلى المنطقة الخاصة بالذاكرة.

د-التعديل و المتمثل في تغيير المعطيات الموجودة داخل النظام و إستبدالها بمعطيات أخرى ، و يتم التلاعب في المعطيات عن طريق إستبدالها أو التلاعب في البرنامج أو إعداده بمعطيات مغايرة تؤدي إلى نتائج غير التي صمم لها البرنامج.

4- السرقة العلمية.

نصت المادة رقم 14 من ذات القانون النموذجي على سرقة المعلومات بتجريم كل من عمليات نسخ و نشر المصنفات الفكرية أو الأدبية أو الأبحاث العلمية أو ما في حكمها إذا ما أرتكب دون وجه حق ، و الحكم بعقوبة الحبس التي يترك تقديرها وفقا لقانون كل دولة ودون الإخلال بالنصوص الخاصة بالملكية الفكرية لكل بلد.

كما حدد هذا القانون النموذجي الإطار التجريمي و العقابي للأفعال التي من شأنها أن تشكل خطرا على المنظومة المعلوماتية أو سلامة نقل البيانات عبر شبكة الإنترنت .

الفرع الرابع : الإتفاقية العربية لمكافحة الجريمة الإلكترونية لسنة 2010

أولا : تعريف الإتفاقية

جاءت هذه الإتفاقية العربية التي وافق عليها مجلسي وزراء الداخلية و العدل العرب في إجتماعهما المشترك المنعقد بمقر الأمانة العامة بجامعة الدول العربية بتاريخ ، 2010/12/21 كمبادرة عربية لمكافحة الجرائم الإلكترونية و ذلك في إطار مواكبة الجهود المبذولة على المستوى الدولي ، بهدف تعزيز التعاون بين الدول العربية و تدعيمه في مجال مكافحة جريمة تقنية المعلومات[1].

وقد أدت هذه الإتفاقية لميلاد قوانين عديدة لمكافحة ما يسمى بالجرائم الإلكترونية في السعودية و الأردن و قطر و الإمارات و العراق و سلطنة عمان... الخ

[1] براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم، تخصص: القانون، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو ، 2018 ، ص 289 .

وجاءت مضامين الإتفاقية العربية مطابقة لأحكام إتفاقية بودابست خاصة على مستوى القواعد الإجرائية ، التي أوجبت على الدول الأطراف ملاءمتها مع قوانينها الوطنية فيما يخص الأبحاث الجنائية لتدابير التحفظ على بيانات الكمبيوتر المخزنة و كشفها وإصدار أوامر.

ثانيا : الجرائم المدرجة ضمن الإتفاقية العربية لمكافحة جرائم تقنية المعلومات

لقد ألزمت هذه الإتفاقية كل دولة طرف بتجريم الأفعال المبينة في الفصل الثاني منها المعنون بالتجريم ، وذلك وفقا لتشريعاتها و أنظمتها الداخلية على النحو التالي[1]:

1/جريمة الدخول غير المشروع:

- الدخول أو البقاء و كل إتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الإستمرار به.
- شدد العقوبة إذا ترتب على هذا الدخول أو البقاء أو الإتصال أو الإستمرار أو بهذا الإتصال .
- محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة و للأجهزة والأنظمة الإلكترونية و شبكات الإتصال و إلحاق الضرر بالمستخدمين و المستفيدين.
- الحصول على معلومات حكومية سرية.

2/جريمة الإعتراض غير المشروع:

الإعتراض المتعمد بدون وجه حق لخط سير البيانات بأي من الوسائل الفنية و قطع بث أو إستقبال بيانات تقنية المعلومات.

3/جريمة الإعتداء على سلامة البيانات:

- تدمير أو محو أو إعاقة أو تعديل أو حجب بيانات تقنية المعلومات قصدا و بدون وجه حق.
- للطرف أن يستلزم لتجريم الأفعال المنصوص عليها في القرة(1) من هذه المادة أن تتسبب بضرر جسيم.

4/جريمة إساءة إستخدام وسائل تقنية المعلومات:

أ- إنتاج أو بيع أو شراء أو إستيراد أو توزيع أو توفير:

* أية أدوات أو برامج مصممة أو مكيفة لغايات إرتكاب الجرائم المبينة في المادة السادسة إلى المادة الثامنة.

* كلمة سر نظام معلومات أو شيفرة دخول أو معلومات مشابهة يتم بواسطتها دخول نظام معلومات ما بقصد إستخدامها لأية من الجرائم المبينة في المادة السادسة إلى المادة الثامنة.

[11] د. خلدون عيشة ، المرجع السابق ، ص 41 .

ب- حيازة أية أدوات أو برامج مذكورة في الفقرتين أعلاه، بقصد إستخدامها لغايات إرتكاب أي من الجرائم المذكورة في المادة السادسة إلى المادة الثامنة.

5/جريمة التزوير:

إستخدام وسائل تقنية المعلومات من أجل تغيير الحقيقة في البيانات تغييرا من شأنه إحداث ضرر ، وبنية إستعمالها لبيانات صحيحة.

6/جريمة الإحتيال:

التسبب بإلحاق الضرر بالمستفيدين و المستخدمين عن قصد و بدون وجه حق بنية الإحتيال لتحقيق المصالح و المنافع بطريقة غير مشروعة ، للفاعل أو للغير عن طريق[1] :

- إدخال أو تعديل أو محو أو حجب المعلومات و البيانات.
- التدخل في وظيفة أنظمة التشغيل و أنظمة الإتصالات أو محاولة تعطيلها أو تغييرها.
- تعطيل الأجهزة و البرامج و المواقع الإلكترونية.

7/جريمة الإباحية:

- إنتاج أو عرض أو توزيع أو توفير أو نشر أو شراء أو بيع أو إستيراد مواد إباحية أو مخلة بالحياء بواسطة تقنية المعلومات.
- شدد العقوبة على الجرائم المتعلقة بإباحية الأطفال والقصر.
- يشمل التشديد الوارد في الفقرة (2) من هذه المادة ، حيازة مواد إباحية الأطفال و القصر أو مواد مخلة بالحياء للأطفال و القصر على تقنية المعلومات أو وسيط تخزين تلك التقنيات.

8/الجرائم الأخرى المرتبطة بالإباحية:

المقامرة والإستغلال الجنسي.

9/جريمة الإعتداء على حرمة الحياة الخاصة:

الإعتداء على حرمة الحياة الخاصة بواسطة تقنية المعلومات.

10/الجرائم المتعلقة بالإرهاب و المرتكبة بواسطة تقنية المعلومات:

- نشر أفكار و مبادئ جماعات إرهابية و الدعوة لها.
- تمويل العمليات الإرهابية و التدريب عليها و تسهيل الإتصالات بين التنظيمات الإرهابية.

[1] نفس المرجع ، ص 43 .

- نشر طرق صناعة المتفجرات و التي تستخدم خاصة في عمليات إرهابية.

- نشر النعرات و الفتن و الإعتداء على الأديان و المعتقدات.

11/الجرائم المتعلقة بالجرائم المنظمة والمرتكبة بواسطة تقنية المعلومات:

- القيام بعمليات غسل أموال أو طلب المساعدة أو نشر طرق القيام بغسل الأموال.

- الترويج للمخدرات و المؤثرات العقلية أو الإتجار بها.

- الإتجار بالأشخاص.

- الإتجار بالأعضاء البشرية.

- الإتجار غير المشروع بالأسلحة.

12/الجرائم المتعلقة بإنتهاك حق المؤلف و الحقوق المجاورة :

إتنهاك حق المؤلف كما هو معرف حسب قانون الدولة الطرف ، و ذلك إذا ارتكب الفعل عن قصد ولغير الإستعمال الشخصي ، و إنتهاك الحقوق المجاورة لحق المؤلف ذات الصلة كما هي معرفة حسب قانون الدولة الطرف ، و ذلك إذا ارتكب الفعل عن قصد ولغير الإستعمال الشخصي.

13/جريمة الإستخدام غير المشروع لأدوات الدفع الإلكترونية :

- كل من زور أو إصطنع أو وضع أي أجهزة أو مواد تساعد على تزوير أو تقليد أي أداة من أدوات الدفع الإلكترونية بأي وسيلة كانت.

- كل من استولى على بيانات أي أداة من أدوات الدفع و استعملها أو قدمها للغير أو سهل للغير الحصول عليها.

- كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول بدون وجه حق إلى أرقام أو بيانات أي أداة من أدوات الدفع.

- كل من قبل أداة من أدوات الدفع المزورة مع العلم بذلك.

14/الشروع و الإشتراك في إرتكاب الجرائم:

- الإشتراك في إرتكاب أية جريمة من الجرائم المنصوص عليها في هذا الفصل مع وجود نية إرتكاب الجريمة في قانون الدولة الطرف.

- الشروع في إرتكاب الجرائم المنصوص عليها في الفصل الثاني من هذه الإتفاقية.

- يجوز لأي دولة طرف الإحتفاظ بحقها في عدم تطبيق الفقرة الثانية من هذه المادة كليا أو جزئيا.

15/المسؤولية الجنائية للأشخاص الطبيعية و المعنوية:

تلتزم كل دولة طرف مع مراعاة قانونها الداخلي ، بترتيب المسؤولية الجزائية للأشخاص الإعتبارية عن الجرائم التي يرتكبها ممثلوها بإسمها أو لصالحها دون الإخلال بفرض العقوبة على الشخص الذي يرتكب الجريمة شخصيا.

16/تشديد العقوبات على الجرائم التقليدية المرتكبة بواسطة تقنية المعلومات:

تلتزم كل دولة طرف بتشديد العقوبات على الجرائم التقليدية في حال إرتكابها بواسطة تقنية المعلومات .

المبحث الثاني : دور الميكانيزمات الدولية في مكافحة الجريمة الإلكترونية

للجريمة الإلكترونية طبيعة إزدواجية كونها ترتكب في عالم افتراضي لا يعترف بالحدود الجغرافية للدول ، هذا ما سهل إرتكابها من أيّ مكان في جميع بقاع الكرة الأرضية ، وهو الأمر الذي مكّن المجرم الإلكتروني من استهداف أشخاص ومؤسسات خارج نطاق إقليمه الوطني ، لذا لم تعد التشريعات الوطنية قادرة على مواكبة سرعة وتطور الجا رئم الإلكترونية مما أدى بالمجتمع الدولي إلى تبني فكرة التعاون لوضع حدّ لهذه الجريمة من خلال تكاتف الجهود الدولية لمكافحتها .

المطلب الأول : التعاون الدولي في مجال مكافحة الجرائم الإلكترونية

تتعدد أوجه وصور التعاون الدولي في مكافحة الجريمة الالكترونية فالتعاون الأمني الدولي والتعاون القضائي الدولي والتعاون الدولي بشأن تسليم المجرمين من أهمها[1]:

الفرع الأول : التعاون الأمني الدولي

أولا : تعريف التعاون الأمني الدولي

بالنظر إلى التعاون الأمني الدولي بمفهومه الواسع نجد أنه يشمل مجالات مختلفة كالمجال الشرطي و المجال القانوني و المجال القضائي، ومرد ذلك أن تحقيق الأمن يتطلب تنفيذ إجراءات تتعلق بتلك المجالات مجتمعة ، وهذا الأخير لا يقتصر على إجراءات ملاحقة الأشخاص المطلوبين للعدالة وحسب بل يتعدى الأمر ذلك ليشمل مكافحه الجريمة بشقيها الوقائي والقمعي بما يشمل العناية بحقوق المتهمين والضحايا ومراعاة حقوق الدول وسيادتها[2] .

ويعد التعاون الدولي الأمني أهم صور التعاون الدولي في مكافحة الجريمة بصفة عامة والجرائم الالكترونية على وجه الخصوص وفي هذا الصدد تقوم المنظمة الدولية للشرطة الجنائية الانتربول بدور أساسي في ترسيخ دعائم هذا التعاون .

ثانيا : أهميته :

يمثل التعاون الأمني الدولي بين أجهزة الشرطة الجنائية المتخصصة لمكافحة الجرائم الالكترونية في الدول احد الوسائل الهامة التي يمكن من خلالها منع هذه الجرائم والإقلال منها ،وتؤكد التحقيقات في الجرائم –عامة–

[1] جعفر جاسم الطائي، جرائم تكنولوجيات المعلومات ، رؤية جديدة للجريمة الحديثة ، دار البداية ناشرون موزعون ، الأردن، 2007 ، ص 234 .

[2] براهيمي جمال ، التحقيق الجنائي في الجرائم الإلكترونية ، أطروحة لنيل شهادة الدكتوراه في العلوم ، تخصص: القانون ،كلية الحقوق والعلوم السياسية، جامعة تيزي وزو، 2018 ، ص 296 .

والالكترونية خاصة على أهمية التعاون الأمني الدولي ،حيث يستحيل على دولة بمفردها القضاء على هذه الجرائم الدولية العابرة للحدود، لان جهاز الأمن فيهذه الدولة أو غيرها لا يمكنه تعقب المجرمين وملاحقتهم إلا في حدود الدولة التابعة لها.

فملاحقه مرتكبي هذه الجرائم وتقديمهم للعدالة لتوقيع العقاب يستلزم القيام بإجراء التحريات خارج حدود الدولة حيث ارتكبت الجريمة أو جزء منها ومن هذه الإجراءات معاينة مواقع الانترنت في الخارج أو ضبط الأقراص الصلبة أو تفتيش نظم الحاسب الآلي .

-كما تتضح أهميته بوجود تكتيك متطور لإجراء التحريات والتحقيقات في مجال مكافحة الجريمة الالكترونية باستخدام التكنولوجيا الحديثة في الاتصال مثل الدوائر التلفزيونية واستخدام أساليب خاصة للتحري والمراقبة ، واستحداث قنوات للاتصال والتنسيق الأمني والقضائي بين الجيهات المختصة عن طريق الأقمار الصناعية وشبكة الانترنت في تبادل المعلومات سريعا وانتقال القاضي إلى الدولة المعنية للتحقيق وإتخاذ ما يلزم من إجراءات ، ليس فقط في مرحلة التحقيق الابتدائي ولكن في مرحلة الحكم أيضا ، ومراعاة تنفيذ الأحكام الأجنبية وفقا للضوابط التي تتفق عليها الدول فيما بينها من خلال التوفيق بين الإجراءات الجنائية في كل من الدولتين .

ثالثا : التعاون الأمني و جهود المنظمة الدولية للشرطة الجنائية

إن المنظمة الدولية للشرطة الجنائية تهدف إلى تعزيز وتشجيع التعاون الأمني الدولي ، أيمساعده الأجهزة الأمنية أو الشرطية في الدول الأعضاء على التعاون فيما بينها في مجال مكافحة الجريمة بأشكالها المختلفة ، وبصفة خاصة لجرائم الطابع عبر الوطني كالجرائم الالكترونية ، دون التدخل في الشؤون ذات الطابع السياسي أو العسكري أو الديني أو العرقي أو ممارسة أي نشاط من هذا القبيل[1] .

-الانتربول هو اكبر منظمة شرطية دولية أنشئت عام 1923 بـ "فيينا" النمسا ،ومقرها الرئيسي في مدينة ليون بفرنسا وكما هو معروف من دستور الانتربول الدولي فهي تتكون من: الجمعية العامة واللجنة التنفيذية ، الأمانة العامة ، المكاتب المركزية الوطنية ، المستشارون ، لجنة ضبط ملفات الانتربول .

فقد بدأت ظهور الملامح الأساسية لهذه المنظمة عبر العديد من المؤتمرات ففي عام 1914 انعقد المؤتمر الأول للشرطة الجنائية الدولية في موناكو من ضباط الشرطة ورجال القانون والقضاة من 81 دولة ، وذلك للتباحث بشأن إجراءات التوقيف وأساليب التبيين والسجلات المركزية للمجرمين الدوليين وإجراءات التسليم .

[1] عادل عبد العال إبراهيم خراشي ، اشكالية التعاون الدولي في مكافحة الجرائم الالكترونية وسبل التغلب عليها، ,كلية الشريعة والقانون ، القاهرة ، ص 190 .

وفي عام 1926 انعقدت الجمعية العامة في برلين واقترحت أن تقيم كل دولة جهة اتصال مركزية ضمن بنية الشرطة وتم اعتماد ذلك عام 1927 وفي عام 1930 تم أنشاء أقسام متخصصة في مكافحة تزييف العملة و السجلات الجنائية وتزوير جوازات السفر.

وفي عام 1935 تم إطلاق شبكة الانتربول الدولية للاتصالات اللاسلكية وهكذا توالى تطوير هذه المنظمة وقد تم نقل مقرها إلى ليون فرنسا عام1989، وطريقة العمل داخل المنظمة تتم بتبادل أعضاء الشرطة الدولية المعلومات عن المجرمين الدوليين ويتعاونون في ما بينهم في مكافحة الجرائم الدولية مثل جرائم التهريب وعمليات البيع والشراء غير المشروع للأسلحة والجرائم الالكترونية وقد ركز الانتربول في السنوات الأخيرة بصورة أساسية على الجريمة المنظمة والأنشطة الإجرامية ذات الصلة بها مثل غسل الأموال ويحتفظ أفراد المنظمة بسجلات الجرائم الدولية[1] .

ولذا تعد هذه المنظمة أهم واكبر شبكة اتصالات لتبادل المعلومات الشرطية على مستوى العالم بين أجهزة الشرطة في الدول الأعضاء .

وتطبيقا لذلك حددت المادة الثانية من ميثاق المنظمة أهدافها الأساسية في أمرين أساسيين:

1-تأكيد وتشجيع المساعدة المتبادلة على أوسع نطاق ممكن، بين سلطة الشرطة الجنائية في حدود القوانين المعمول بها في الدول المختلفة واهتداء بروح الإعلان العالمي لحقوق الإنسان.

2-إقامة وتطوير النظم التي تسهم على نحو فعال ومؤثر في منع ومكافحة جرائم القانون العام .

وبهذا فان شرطة الانتربول تعد منظمة عالمية تختص في مكافحة الجرائم الدولية العابرة للحدود الوطنية للدول بما فيها الجرائم الالكترونية ، وذلك ما أكدته نتائج الدورة رقم 22 للجمعية العامة لمنظمه الانتربول ، حيث دعا الآمين العام للانتربول "السيد بونالد نوبل" جميع الحكومات والدول لدعم وتطوير نظم تبادل المعلومات حول المشتبه بهم ومحاربة الإرهاب المتنامي في كل أنحاء العالم بكل صوره بما فيه الإرهاب المعلوماتي، وقد نجحت المنظمة الدولية للشرطة الجنائية الانتربول خلال الأعوام الأخيرة في جعل اسمها من أكثر الأسماء التي يخشاها المجرمون[2] .

[1] نفس المرجع ، ص 191 .
[2] نفس المرجع ، ص 192 .

الفرع الثاني : التعاون القضائي الدولي

أولا : تعريف التعاون القضائي الدولي

تعد المساعدة القضائية المتبادلة في المسائل الجنائية أو ما يعرف بالتعاون القضائي الدولي من أهم صور التعاون الدولي في مكافحه الجريمة وأكثرها فعالية في مجال تعقب مرتكبي الجرائم وملاحقتهم والقبض عليهم ، ومحاكمتهم وإنزال العقاب بهم[1].

-وتعرف المساعدة القضائية الدولية بأنها كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دوله أخرى بصدد جريمة من الجرائم.

وقد تناولت المادتان (15- 11) من اتفاقية بودابست لمكافحة الجرائم الالكترونية لسنة 2001 أهم مظاهر التعاون الدولي في مجال مواجهه الجرائم الالكترونية إذ نصت المادة 111 من هذه الاتفاقية على تسليم المجرمين وحددت شروطه وإجراءاته وفصلت المادة 15 من هذه الاتفاقية أحكام المساعدة القضائية المتبادلة في مجال مكافحه هذه الجرائم .

-ولقد نص المشرع الجزائري في القانون 01/09 على مبدأ المساعدة القضائية الدولية المتبادلة في المادة 81 منه معتبرا أنه في إطار التحريات والتحقيقات القضائية الجارية لمعاينة الجرائم الإلكترونية يمكن للسلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الالكتروني.

وترتبط الجزائر بالعديد من المعاهدات والاتفاقيات الثنائية في مجال التعاون القضائي التي تتضمن أحكام متعلقة بتسليم المجرمين نذكر منها :

- إتفاقية تنفيذ الأحكام وتسليم المجرمين بين الجزائر وفرنسا.
- إتفاقية تسليم المجرمين والتعاون القضائي بين الجزائر والمملكة البلجيكية.
- إتفاقية تسليم المجرمين بين الجزائر وجمهورية جنوب إفريقيا.
- إتفاقية تسليم المجرمين بين الجزائر وباكستان.
- إتفاقية تسليم المجرمين بين الجزائر وجمهورية نيجريا الاتحادية.
- إتفاقية تسليم المجرمين بين الجزائر وإيران.
- إتفاقية تسليم المجرمين بين الجزائر والمملكة المتحدة وايرلندا الشمالية.
- إتفاقية تسليم المجرمين بين الجزائر والصين.

[1] خالد ممدوح إبراهيم ، أمن الجريمة الإلكترونية ، الدار الجامعية للطباعة ، الإسكندرية ، مصر ، 2008 ، ص 407 .

– إتفاقية تسليم المجرمين بين الجزائر والبرتغال.

– إتفاقية تسليم المجرمين بين الجزائر وكوريا.

– إتفاقية التعاون القضائي والإعانات والانابات القضائية وتنفيذ الأحكام وتسليم المجرمين بين الجزائر ودولة الإمارات العربية .

– إتفاقية تسليم المجرمين بين الجزائر وإسبانيا.

وهناك عدة أشكال للتعاون الدولي القضائي في مكافحة الجريمة تتمثل فيما يلي :

1/ تبادل المعلومات : يقصد بتبادل المعلومات تقديم المعلومات والوثائق التي تطلبها سلطة قضائية أجنبية بصدد جريمة من الجرائم عن الاتهامات التي وجهت إلى رعاياها في الخارج والإجراءات التي اتخذت ضدهم كما أن هناك مظهر أخر لتبادل المعلومات يتعلق بالسوابق القضائية للجناة من خلالها تتعرف الجهات القضائية بدقة على الماضي الجنائي للفرد المحال إليها وقد جاء هذا في العديد من الاتفاقيات الوطنية والدولية لعل من أهمها[1] :

– ما جاء على المستوى الشرعي الوطني حيث نصت المادة 82من قانون 09/01على أن الدولة الجزائرية تستجيب لطلبات المساعدة القضائية الدولية الرامية لتبادل المعلومات وذلك في إطار الاتفاقيات الدولية ذات الصلة ومبدأ المعاملة بالمثل.

– وما ورد في الفقرة الثانية من المادة الأولى في معاهدة الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجنائية وكذا ما ورد في البند الثالث والرابع والخامس من المادة الثامنة لاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للوطنية إذ أوجبت على الدول الأطراف تيسير تبادل المعلومات المتعلقة بكافة جوانب النشاط الإجرامي.

– أيضا ما ورد في المادة الأولى من اتفاقية الرياض للتعاون القضائي العربي بشأن ضرورة تبادل المعلومات بين الدول الأطراف والتنسيق بين الأنظمة القضائية.

– وفي هذا الإطار أيضا صاغ اتفاق "شنجن" للاتحاد الأوروبي نظام متكامل لتبادل المعلومات.

2/ نقل الإجراءات : ويقصد بهذه الصورة قيام دولة ما بمقتضى إتفاقية أو معاهدة باتخاذ إجراءات جنائية وهي بصدد التحقيق في جريمة الكترونية إرتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة متى توفرت مجموعة من الشروط أهمها[2]:

[1] خالد ممدوح إبراهيم ، المرجع السابق ، ص 407 .

[2] براهيمي جمال، مرجع سابق ، ص 319 .

– أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة و المطلوب منها.

– أن تكون الإجراءات المطلوب اتخاذها مقررة في قانون الدولة المطلوب منها عن ذات الجريمة.

– أن يكون الإجراء المطلوب اتخاذه يؤدي إلى الوصول إلى الحقيقة كأن تكون أدلة الجريمة موجودة بالدولة المطلوبة منها .

ولقد أقرت العديد من الاتفاقيات الدولية منها والإقليمية هذه الصورة كإحدى صور المساعدة القضائية الدولية منها : معاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية وكذا اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للوطنية .

3/ الإنابة القضائية : تعد الإنابة القضائية الدولية في المسائل الجنائية من أهم أشكال التعاون القضائي الدولي ، حيث تهدف إلى تفعيل الحماية القانونية استجابة إلى متطلبات العدالة الجنائية ، وذلك بالوصول إلى استكمال كافة إجراءات التحقيق المختلفة حتى لو كانت خارج نطاق سلطة القاضي الوطني الإقليمية ، هذا الدور الوظيفي للإنابة يصطدم بصعوبات في التنفيذ تتعلق بسيادة الدولة والتي حاولت الاتفاقيات الدولية التغلب عليها من خلال التوسع في موضوع الإنابة و أيضا طرق التنفيذ وخلصت هذه الدراسة إلى نتيجة مهمة هي أن الإنابة القضائية الدولية أصبحت صورة للتخفيف من غلو مبدأ الإقليمية للقوانين الجنائية حيث ساهمت في تطوير آليات المساعدة القضائية بين الدول في المسائل الجنائية فأصبح بإمكان القاضي الوطني التعويل على نتائج الإنابة القضائية الدولية التي تمت بواسطة سلطة قضائية أجنبية[1].

وتستلزم الإنابة القضائية الدولية إرسال الملف الخاص بالدعوة الجنائية بمرفقاته من مستندات ووثائق و محاضر التحقيق التي أجريت بمعرفة السلطة القضائية في الدولة المطلوب فيها إتخاذ بعض إجراءات التحقيق وهي في ذلك تتشابه إلى حد كبير مع الندب (الإنابة القضائية الداخلية) .

4/ تسليم المجرمين : تسليم المجرمين يعني قيام دولة ما (الدولة المطلوب منها التسليم) بتسليم شخص موجود في إقليمها إلى دولة أخرى (الدولة طالبة التسليم) بناء على طلبها بغرض محاكمته عن جريمة نسب إليه إرتكابها أو لتنفيذ حكم صادر ضده من محاكمها[2].

[1] نفس المرجع ، ص 321 .

[2] أمير فرج يوسف ، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت ، مكتبة الوفاء القانونية ، الإسكندرية، مصر ، 2011 ، ص 445 .

ويقوم مبدأ تسليم المجرمين على أساس أن الدولة التي يتواجد على إقليمها المتهم بارتكاب إحدى الجرائم العابرة للحدود مثل جرائم الانترنت عليها أن تقوم بمحاكمته إذا كان تشريعها يسمح بذلك وإلا عليها أن تقوم بتسليمه لمحاكمته بمعرفة دولة أخرى مختصة .

وقد تناولت العديد من الاتفاقيات والمؤتمرات الدولية موضوع تسليم المجرمين تدعوا فيها إلى إبرام معاهدة عالمية لتسليم المجرمين من بينها المؤتمر الأول للشرطة القضائية في موناكو عام 1924 ، والمؤتمر الدولي للعقاب في لندن عام 1945 شروط تسليم المجرمين في الواقع أن تسليم المجرمين لا يتم هكذا دون وجود ضوابط وشروط تحكمه بل أن هناك عددا من الشروط التي ينبغي توافرها من بين هذه الشروط :

أ/إزدواجية التجريم : وهو أن يكون الفعل المطلوب التسليم من اجله مجرم في الدولة المطلوب منها التسليم والدولة الطالبة للتسليم والعبرة بالتجريم فقط دون الوصف القانوني للفعل لأنه من الممكن أن يختلف التكييف القانوني لفعل معين في دولة عن أخرى حسب تشريع كل منها ، ويتبع شرط ازدواجية التجريم في الدولة طالبة التسليم والدولة المطلوب منها التسليم ألا تكون الدعوى الجنائية قد إنقضت أو سقطت بالتقادم وفق قانون أي من الدولتين لأن الغرض من التسليم هو محاكمة الشخص أو تنفيذ عقوبة محكوم بها عليه ، وهذا الإجراء يقوم أساسا على أن الدولة التي يتواجد على إقليمها المتهم بارتكاب جريمة الكترونية عليها أن تقوم بمحاكمته إذا كان تشريعها يسمح بذلك وإلا كان عليها أن تقوم بتسليمه لمحاكمته بمعرفه دولة أخرى مختصة.

– أن يشكل الفعل جريمة من الجرائم الجائز بشأنها التسليم حيث هناك قائمة سلبية للجرائم أو الأحوال التي لا يجوز التسليم فيها ومن الجرائم التي تم استبعادهم من نطاق مبدأ تسليم المجرمين الجرائم التي تندرج تحت الصور الآتية:

–الجرائم التي لا يكون معاقبا عليها بمقتضى قانون الدولتين.

–الجرائم السياسية.

–الجرائم العسكرية.

–الجرائم قليلة الأهمية.

–الجرائم المحكوم فيها على المتهم المطلوب تسليمه بعقوبة الإعدام.

ومن الجرائم التي يجوز فيها التسليم وترتبط بالمعلوماتية:

–الدخول غير مشروع.

–الاعتراض غير المشروع.

-التدخل غير المشروع في المنظومة.

-إساءة استخدام الأجهزة.

-جريمة التزوير والتدليس المتعلقة بالكمبيوتر.

- الجرائم المتعلقة بالأعمال الإباحية وصور الأطفال الفاضحة.

-الجرائم المتعلقة بالانتهاكات الخاصة بحقوق الطبع و النشر و الحقوق المتعلقة بها .

ب/الشروط المتعلقة بالأشخاص المطلوب تسليمهم

عدم جواز تسليم الرعايا: حيث من المبادئ السائدة والمستقر عليها في المجتمع الدولي والتي نصت عليها معظم التشريعات الوطنية والاتفاقيات الدولية مبدأ عدم جواز تسليم الرعايا أيا كان نوع الجريمة المرتكبة من قبلهم في أي إقليم خارج دولهم.

-عدم جواز تسليم ممنوحي حق اللجوء السياسي.

-عدم جواز تسليم من تمت محاكمتهم عن ذات الجريمة المطلوب التسليم من اجلها وعلة هذا الشرط هو عدم ازدواجية العقاب .

ج/ إجراءات تسليم المجرمين : فهي القواعد والأسس التي تنتهجها الدول الأطراف فيما يتعلق بعملية التسليم وفقا لقوانينها الوطنية وتعهداتها الدولية وذلك بهدف إحداث نوع من التوازن بين حرية الأشخاص وحقوقهم من جانب وبين الحفاظ على آمنها واستقرارها من جانب آخر يتبين من خلال هذه الدراسة ان نظام تسليم المجرمين هو نظام حيوي تسعى الدول من خلاله الى تفعيل التعاون القضائي فيما بينها للحد من انتشار الجريمة الالكترونية في كل المجالات والتصدي للمجرمين بفعالية ، غير أنه يلاقي صعوبات من الناحية التطبيقية امام سيادة الدول ، كون هذه الاخيرة تعطي لقواعد الدستور قيمة أسمى من الاتفاقيات الدولية[1].

[1] جميل عبد الباقي الصغير ، المواجهة الجنائية لقرصنة البرامج التلفزيونية المدفوعة ، دار النهضة العربية ، القاهرة ،2001 ، ص 130 .

المطلب الثاني : دور الهيئات والمنظمات الدولية في مكافحة الجرائم الإلكترونية

إهتم المجتمع الدولي بموضوع التصدي للجريمة الإلكترونية نظرا لما تتميز به من خصوصية مقارنة بالجرائم الأخرى بحيث لجأ إلى تكثيف جهوده لمكافحتها ، من خلال دور الهيئات والمنظمات الدولية وإرسائها في قالب تعاوني لوضع حد لهذا النوع من الجرائم .

الفرع الأول : منظمة الأمم المتحدة

من المتعارف لدى القانونيين أن منظمة الأمم المتحدة هيئة إدارية مستقلة تقوم على مبادئ عالمية من مساواة بين الدول في السيادة ، حل النزاعات بالطرق السلمية ومنع استعمال القوة في العلاقات الدولية بهدف حفظ الأمن والسلام الدوليين وتنمية العلاقات الودية الدولية بين الدول، وتحقيق التعاون الأمني في مواجهة الجرائم ذات الطابع الدولي ومن بينها مكافحة الجريمة الإلكترونية.

لقد إهتمت هيئة الأمم المتحدة بموضوع مكافحة الجريمة الإلكترونية من خلال تعزيز العمل المشترك بين أعضاء المنظمة للحد من انتشارها وتعاظم آثارها[1] ، وهذا بلجوئها إلى إبرام اتفاقيات وإنشاء منظمات لهذا الغرض ، فمن الخطوات التي إعتمدتها كان المؤتمر السابع المنعقد في ميلانو بإيطاليا سنة 1985 أين لجأت إلى تكليف لجنة لدراسة موضوع حماية نظم المعالجة الآلية والاعتداء على الكمبيوتر، ثم عرضت هذه الدراسة لاحقا في تقرير بالمؤتمر الثامن المنعقد بهافاناسنة 1990والموافقة عليه من خلال إصدارها توصيات بشأن الجريمة الإلكترونية[2] ،ومن أبرز التوصيات التي خرجت بها المبادئ التالية :

- تحديث القوانين الجنائية الوطنية بما في ذلك التدابير المؤسسية وتحسين أمن الكمبيوتر والتدابير المنعية .
- تلقين آداب استعمال الكمبيوتر كجزء من مقررات الاتصالات والمعلومات.
- إعتماد سياسات تعالج المشكلات المتعلقة بمرتكبي الجرائم الإلكترونية.
- زيادة التعاون الدولي من أجل مكافحة الجرائم الإلكترونية.
- إعتماد إجراءات تدريب كافية للموظفين والوكالات المسئولة عن مكافحة جرائم الحاسوب والتحري والإدعاء فيها[3].

[1] محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، الأردن، ،2005ص 155.

[2] براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل شهادة الدكتوراه العلوم، تخصص: القانون ، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو ، 2018 ، ص26.

[3] محمود أحمد عبابنة، مرجع سابق، ص 1.

في سنة 1994 قامت بتوقيع اتفاقية تريبس في مجال حماية الملكية الفكرية من السطو عليها خصوصا بعد ظهور السرقة الإلكترونية على الأعمال الفنية ، لذا عالجت هذه الاتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية[1] ، والتي تضمنت حماية برامج الحاسب الآلي والبيانات المجمعة داخله[2] ، كما لجأت الأمم المتحدة لإبرام معاهدة دائما بخصوص حقوق المؤلف سنة 1996 عرفت باتفاقية الويبو وهي إتفاق خاص في إطار اتفاقية برن وعلى إثر هذا تطرقت هذه الاتفاقية إلى حماية المصنفات وحقوق مؤلفيها في البيئة الرقمية، وعلى كل طرف متعاقد فيهذه الاتفاقية الامتثال للأحكام الموضوعية الواردة في اتفاقية برن 1971 المعتمدة في1986[3].

ومن بين أهم المواضيع التي تناولتها إتفاقية الويبو تأكيدها على حماية برامج الحاسوب[4] ، وقواعد البيانات وفقا لما نصت عليه **م 05 من اتفاقية الويبو 1996** : «**تتمتع مجموعات البيانات أو المواد الأخرى بالحماية بصفتها هذه ، أيا كان شكلها ، إذا كانت تعتبر ابتكارات فكرية بسبب اختيار محتوياتها أو ترتيبها ، ولا تشمل هذه الحماية البيانات أو المواد في حد ذاتها ، ولا تخل بأي حق للمؤلف قائم في البيانات أو المواد الواردة في المجموعة**» .

فعلى هذا الأساس أن برامج الكمبيوتر والبيانات بكل أشكالها مَن المصنفات الرقمية التي تدخل ضمن حقوق الملكية الفكرية التي سعت الأمم المتحدة لحمايتها من خلال إتفاقيتي تريبس 1996 ، والويبو 1994 ، ومع تزايد جرائم تكنولوجيات الإعلام والاتصال قامت المنظمة بعقد مؤتمرها العاشر في بودابست سنة 2000 الذي توج بإبرام الاتفاقية الخاصة بمكافحة استعمال التكنولوجيا لأغراض إجرامية بهدف الحد من جرائم تقنية المعلومات ، كما عقدت في نفس السنة مؤتمر دولي بعنوان "تحديات الجريمة السيبرانية العابرة للحدود" ، وفي سنة 2005 وضعت أجندة لمكافحة جرائم تقنية المعلومات سميت بأجندة تونس بمناسبة القمة العالمية لمجتمع المعلومات ، بهدف ملاحقة مرتكبي جرائم الانترنت العابرة للحدود وتعزيز التعاون الدولي في مجال مكافحة الجرائم

---

[1] جعفر جاسم الطائي، جرائم تكنولوجيات المعلومات _رؤية جديدة للجريمة الحديثة _، الطبعة الأولى، دار البداية ناشرون موزعون، عمان، الأردن، 2007، ص 2 .

[2] جاءت المادة 10من اتفاقية تريبس كما يلي :

1- "تتمتع برامج الحاسب الآلي (الكمبيوتر،) سواء أكانت بلغة المصدر أو بلغة الآلة بالحماية باعتبارها أعمالا أدبية بموجب معاهدة برن (1971).

2-تتمتع بالحماية البيانات المجمعة أو المواد الأخرى، سواء أكانت في شكل مقروء آليا أو أي شكل آخر، إذا كانت تشكل خلقا فكريا نتيجة انتقاء أو ترتيب محتوياتها وهذه الحماية لا تشمل البيانات أو المواد في حد ذاتها ولا تخل بحقوق المؤلف المتعلقة بهذه البيانات أو المواد ذاتها".

[3] المنظمة العالمية للملكية الفكرية، ملخصات الاتفاقيات والمعاهدات والاتفاقات التي تديرها الويبو، 2013، ص 40 متوفر على الرابط التالي :https://www.wipo.int/edocs/pubdocs/ar/intproperty/442/wipo_pub_442.pdf

[4] جاءت المادة 04من اتفاقية الويبو كما يلي ":تتمتع برامج الحاسب الآلي بالحماية باعتبارها مصنفات أدبية بمعنى المادة 2من اتفاقية برن. وتطبق تلك الحماية على برامج الحاسوب أيا كانت طريقة التعبير عنها أو شكلها".

الإلكترونية، كما ساهمت اللجنة الاقتصادية والاجتماعية لغرب آسيا تحت إشراف من هيئة الأمم المتحدة في عقد ورشة عمل حول التشريعات الدولية الخاصة بالإجرام الإلكتروني سنة 2008 بهدف المواجهة الدولية للجريمة الإلكترونية[1].

رغبة في مواصلة هذه الجهود لجأت منظمة الأمم المتحدة إلى عقد المؤتمر الثاني عشر حول منع الجريمة والعدالة الجنائية بالبرازيل في أفريل 2010 بخصوص تطورات إستخدام العلم والتكنولوجيا بحيث أدرجت فيه موضوع مكافحة الجريمة الإلكترونية ، وقامت بتشكيل لجنة منع الجريمة والعدالة الجنائية التي كلفت بإعداد دراسة تحليلية شاملة حول الجريمة الإلكترونية والتدابير الممكنة للتصدي لها، كما قامت اللجنة السالفة الذكر بعقد اجتماع دولي لفريق من الخبراء الحكوميين وذلك من خلال تكليفهم بإعداد دراسة مفصلة لظاهرة الجريمة الإلكترونية في جانفي 2011[2].

الفرع الثاني : المجلس الأوروبي

حاولت أوروبا وضع الأدوات اللازمة للأمن الإلكتروني[3] لذلك فإن للمجلس الأوروبي دور في مكافحة الجرائم الإلكترونية بحيث أقّر توصيات ووقع على عدة إتفاقيات منذ أواخر منتصف القرن العشرين، إذ أنه في سنة 1971 تم توقيع إتفاقية برن بسويسرا والتي تعد حجر الأساس لحماية حقوق المؤلف ، والتي خضعت لتعديل في 1979 ودخلت حيز النفاذ سنة 1986 ووقعت عليها 120 دولة أوروبية ، وقد تضمنت **المادة 09 منها** على أن المؤلف يتمتع بحق استئثاري في التصريح على القيام بعمل نسخ للمصنف بأي طريقة ، بحيث جاءت المادة السالفة الذكر كما يلي : «**يتمتع مؤلفو المصنفات الأدبية والفنية الذين تحميهم هذه الاتفاقية بحق استئثاري في التصريح بعمل نسخ من هذه المصنفات بأية طريقة وبأي شكل كان** » وتهدف هذه الاتفاقية إلى حماية حقوق المؤلفين على مصنفاتهم الأدبية والفنية ، وبموجبها تتمتع برامج الحاسب الآلي سواء كانت بلغة المصدر أو بلغة الآلة بالحماية لكونها أعمالا أدبية وفقا لما جاء فيها من تقديم حلول للمشكلات القانونية الناتجة عن المصنفات المنشورة على شبكة الانترنت[4].

[1] براهيمي جمال، مرجع سابق، ص ص 271-274 .

[2] نفس المرجع ، ص ص 272-273 .

[3] جعفر حسن جاسم الطائي، مرجع سابق، ص ص 238-239 .

[4] بدري فيصل، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة لنيل شهادة دكتوراه علوم، تخصص: قانون عام، كلية الحقوق، جامعة الجزائر.20، ص ص 17-17 .

أقر لاحقا المجلس الأوروبي توصيات خاصة بالبيانات ذات الطابع الشخصي من سوء استخدامها وحماية تدفق المعلومات ، وعلى إثر هذا تم إبرام اتفاقية تتعلق بحماية الأشخاص من مواجهة المعالجة الإلكترونية للبيانات ذات الطابع الشخصي في 28جانفي1981[1] ، وفي سنة 1985 وضع المجلس قواعد إرشادية خاصة بتحديد أنماط جرائم الكمبيوتر، وطالب الدول الأعضاء في المجلس إلى ضرورة المواجهة التشريعية للاستعمال غير المشروع للكمبيوتر من خلال الحماية الجنائية ضدها وحماية الحق في المعلومات بالإضافة إلى حماية حقوق وحريات الأفراد المدنية[2].

واصل المجلس الأوروبي ما بدأه من جهود في مجال الحد من الجريمة الإلكترونية وهذا بلجوئه إلى نشر توصيات بشأن وضع قانون لمواجهة الأفعال غير المشروعة بواسطة الكمبيوتر سنة 1989 ثم في 1995 أصدر المجلس توصية لاحقة تضمنت الإجراءات الجنائية المتبعة في الجرائم الإلكترونية[3] بحث الدول الأعضاء إعادة النظر في الإجراءات الجنائية فيما يخص التحقيق في هذا النوع من الجرائم، ومن بين هذه الإجراءات نذكر ما يلي:

- تفتيش أجهزة الكمبيوتر وضبط المعلومات التي تحتويها، ومراقبتها خلال انتقالها.
- وضع إجراءات جنائية تسمح بتفتيش برامج الكمبيوتر وفقا للإجراءات العادية الخاصة بإجراء التفتيش مع إعلام صاحب الكمبيوتر بالتفتيش والمعلومات التي تم ضبطها.
- احترام ضمانات التفتيش أثناء تفتيش الأجهزة الملحقة بالكمبيوتر من منظومات معلوماتية وضبط المعلومات الموجودة بداخلها.
- تطبيق إجراءات المراقبة والتسجيل في إجراء التحقيقات مع الحفاظ على السرية في أداء هذه الإجراءات.
- إلزام الجهات الحكومية والخاصة المكلفة بتوفير خدمات الاتصال بالتعاون مع جهات التحقيق.
- تعديل القوانين الإجرائية بما يتماشى مع التفتيش لأجهزة الكمبيوتر.
- تكوين وحدات خاصة لمكافحة الجرائم الإلكترونية والوقاية منها.
- ضرورة التعاون بين الدول في مجال إجراءات التحقيق ومكافحة الجرائم الإلكترونية بإبرام اتفاقيات دولية[4].

---

[1] خالد ممدوح إبراهيم، الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، 2009، ص 401 .

[2] براهيمي جمال، مرجع سابق، ص 279 .

[3] سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة الماجستير، في العلوم القانونية، تخصص: علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2013، ص 85 .

[4] محمد أحمد سليمان عيسى، "التعاون الدولي لمواجهة الجرائم الإلكترونية، "المجلة الأكاديمية للبحث القانوني، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرة، بجاية، 2016، ص ص 58-59 .

الفرع الثالث : المنظمة الدولية للشرطة الجنائية (الانتربول)

تم إنشاء المنظمة الدولية للشرطة الجنائية سنة1993[1] من أهم أجهزة التعاون الدولي المكلفة بمكافحة الإجرام بصفة عامة والجرائم المرتبطة بالانترنت والتي يتواجد مقرها في باريس بفرنسا[2] ، والتي تهدف إلى تأكيد وتشجيع التعاون بين أجهزة الشرطة في الدول الأطراف من أجل مكافحة الجريمة ذات طابع دولي عابر للحدود من خلال تبادل المعلومات بخصوص الجرائم والمجرمين وتسليمهم لتحقيق الردع الخاص والعام من خلال توقيع العقوبة[3] ، وعليه فمن الجرائم التي تسعى إلى إعتراضها ومكافحتها الجريمة الإلكترونية بكل صورها التي باتت من الصعب التحكم في التصدي لها من طرف هيئات الشرطة الوطنية للدول لكون هذه الجرائم في بعض الأحيان عابرة للأقاليم الجغرافية للدولة .

من الأمثلة التي تبين جهود شرطة الإنتربول في مجال مكافحة الجريمة الإلكترونية جريمة وقعت في لبنان تعود حيثياتها لتوقيف أحد الطلبة من طرف القضاء اللبناني بتهمة إرسال صور إباحية عبر الانترنت لفتاة قاصر لم تبلغ عشر (10) سنوات ، إثر تلقي النيابة اللبنانية برقية من شرطة الإنتربول في ألمانيا بهذا الخصوص[4] ، وبذلك فإنها تباشر عملها من خلال عملية التحري والتحقيق عن طريق الاستعانة بالمكاتب المركزية الوطنية التابعة لها الموجودة في أقاليم الدول المنظمة إليها[5] كطوكيو، الأرجنتين ونيوزيلندا، ومن بين المهام التي تقوم بها تكوين مجموعة متخصصين من الدول الأعضاء لمباشرة التحري والتحقيق في مجال الجرائم الإلكترونية، تشكيل ورشات وفرق عمل متخصصة، كما تقوم بتزويد أجهزة الشرطة الوطنية للدول الأعضاء بإرشادات وتعليمات توجيهية[6] .

بالإضافة إلى الاستعانة بأحدث الوسائل لجمع وتخزين المعلومات المتعلقة بالجرائم الإلكترونية[7] ، أخيرا أنشأ الإنتربول خلية خاصة لمكافحة استغلال الأطفال على الانترنت بما في ذلك استخدام صور القصر لتشجيع

---

[1] Férale-Schuhl Christiane, CyberDroit le droit à l'épreuve de l'internet, 5em édition, Dalloz, Paris, 2009/ 2010, P 920.

[2] هروال نبيلة هبة، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الإسكندرية، ، 2006 ،مصر ، ص ص149-151 .

[3] محمد محمد محمد عنب ، استخدام التكنولوجيا الحديثة في الإثبات الجنائي، مطبعة السلام الحديثة، د.ب.ن، ،2007 ، ص ص317- 318.

[4] أمير فرج يوسف، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت ، مكتبة الوفاء القانونية، الإسكندرية، مصر، 2011 ، ص 428 .

[5] خالد ممدوح إبراهيم، الجرائم المعلوماتية، مرجع سابق، ص400.

[6] براهيمي جمال، مرجع سابق ، ص ص 299-300 .

[7] حسين ربيعي، مرجع سابق، ص 151

استغلالهم الجنسي[1] ،وفي إطار مكافحة مكافحة الجريمة العابرة للحدود انضمت الجزائر إلى منظمة الإنتربول سنة ، 1963 وكان هذا أثناء انعقاد الجمعية العامة في هلسنكي بفنلندا بتمثيل من المكتب المركزي الوطني الذي يعمل تحت الوصاية المباشرة للمديرية العامة للأمن الوطني.

2-الأوروجست:

تم إنشاء منظمة الأوروجست في 28 فيفري 2002 على مستوى أوروبا ، وتعد بمثابة جهاز يساعد على التعاون القضائي والشرطي في مكافحة الجرائم الخطيرة ، وهذا في حالة ما إذا كان الإجرام بين دولتين من الاتحاد الأوروبي أو دولة عضو فيها مع دولة من العالم الثالث أو دولة عضو مع الرابطة الأوروبية[2] ، وتعد بمثابة الدعامة الفعالة في مجال التحقيقات والمطاردات التي تقوم بها السلطات القضائية الوطنية وخصوصا فيما يتعلق بالإجرام الإلكتروني[3] .

3-شرطة الانترنت الدولية(IWP) :

هي منظمة دولية أنشئت سنة 1986 بالولايات المتحدة الأمريكية بهدف تلقي البلاغات والشكاوي من طرف مستخدمي الانترنت وملاحقة المجرمين إلكترونيا من خلال القيام بالتحري والتحقيق لجمع الأدلة ضدهم وتقديمهم للمحاكمة ، بالاعتماد على مجموعة متخصصين في القانون والمؤسسات الحكومية والشرطة وخبراء فنيين من 61 دولة حول العالم في مجال الجرائم الإلكترونية[4].

4-شرطة الأفريبول:

تعد بمثابة مؤسسة تقنية دائمة ذات طابع إقليمي تتمتع بالشخصية القانونية اللازمة للقيام بمهامها المنوط بها ، أنشئت بمبادرة من الجزائر في 13ديسمبر 2015 وبدأت مزاولة عملها بتاريخ 06 جويلية 2017 بمناسبة اجتماع مسئولي أجهزة الشرطة للدول الإفريقية الأعضاء في الإتحاد الإفريقي، ويبلغ عدد الأعضاء المؤسسة فيها 41 دولة إفريقية[5].

تهدف شرطة الأفريبول إلى تنسيق التعاون الشرطي بين الدول الإفريقية الأعضاء ، وكذا العمل على تشجيع وتكوين خبراء ومتخصصين بإنشاء مراكز إفريقية لتدريبهم وفقا لنص **م 03 من النظام الأساسي لآلية**

---

[1] Férale-Schuhl Christiane, Op, Cit, P 921.

[2] هروال نبيلة هبة، مرجع سابق، ص ص 159-160 .

[3] بدري فيصل، مرجع سابق، ص 90 .

[4] براهيمي جمال، مرجع سابق، ص 302 .

[5] خالدي خديجة، "آلية الإتحاد الإفريقي للتعاون الشرطي أفريبول، "مجلة العلوم الاجتماعية والإنسانية، ع ،01 جامعة العربي تبسي، تبسة ، 2018 ، ص 308

الإتحاد الإفريقي للتعاون الشرطي (أفريبول) وتقوم الشرطة الإفريقية بعدة مهام من بينها مكافحة الجريمة الإلكترونية من خلال تبادل المعلومات والاستخبارات وفقا لما ورد في نص **م 04 الفقرة "د" من النظام الأساسي لآلية الإتحاد الإفريقي للتعاون الشرطي "أفريبول** «"**تيسير تبادل أو تقاسم المعلومات أو الاستخبارات لمنع ومكافحة الجرائم المنظمة عبر الوطنية والإرهاب والجريمة الإلكترونية**» .

الفرع الرابع : مجلس وزراء الداخلية العرب

حيث يهدف هذا المجلس إلى تنمية وتوثيق التعاون بين الدول العربية في مجالات الأمن الداخلية ومكافحة الجريمة وذلك من خلال:

- دعم الأجهزة الأمنية ذات الإمكانات المحدودة.
- تطوير العمل العربي المشترك وإقرار الخطط الأمنية العربية المشتركة.
- إنشاء الهيئات والأجهزة اللازمة لتحقيق أهدافه ومنها تعزيز وسائل تعاون مع الهيئات الدولية المعنية باختصاصاته[1].

الفرع الخامس : مجلس وزارء العدل العرب:

بموجب القرار رقم (229) سنة 1996 وباستعراض الباب التاسع الخاص ضد الأشخاص نجد القانون قد إحتوى على فصل خاص بالاعتداء على حقوق الأشخاص الناتج عن المعالجات المعلوماتية وذلك في المواد (461-464) حيث أشارت المواد (463-461) على وجوب حماية الحياة الخاصة وأسرار الأفراد من خطر المعالجة الآلية وكيفية جمع المعلومات الاسمية وكيفية الإطلاع عليها والمادة (464) نصت على عقاب من يقوم بفعل الدخول الغش إلى كامل أو جزء من نظام المعالجة الآلية للمعلومات ، وعرقلة أو إفساد نظام التشغيل عن أداء وظيفته المعتادة تغيير المعلومات داخل النظام ، وتزوير وثائق المعالجة الآلية وسرقة المعلومات[2] .

[1] محمود احمد عبابنة ، مرجع سابق، ص ص 164-165 .

[2] نفس المرجع ، ص ص 180-181 .

خلاصة الفصل الأول :

إن الجريمة الالكترونية باعتبارها من الجرائم المعلوماتية المعاصرة التي واكبت عصر التقدم التكنولوجي خصوصا بعد ظهور شبكة المعلومات الدولية " انترنت "بسبب التقدم العلمي الحاصل ساعد على انتشار و تنوع هذا السلوك الإجرامي و الذي أصبح يهدد الإنسان في مختلف المجالات لا سيما الاقتصادية و الاجتماعية و الثقافية، و الأخلاقية وحتى المعتقدات الدينية لذلك و أمام الانتشار الواسع لهذا النمط الإجرامي الجد متطور والذي تستخدم فيه أحدث التقنيات التكنولوجية العالية و المتطورة و سرعة و حيلة و بداهة مرتكبيه و التي تجعلهم دائما يفلتون من العقاب في ظل غياب الدليل المادي للجريمة إضافة إلى غياب منظومة تشريعية وطنية تحدد الفعل، تجرمه، ثم تحدد العقوبة المناسبة لمرتكبه انعكس ذلك سلبا على المستوى الدولي، فعلى الرغم من وجود العديد من الاتفاقيات الدولية المتعلقة بالجريمة الالكترونية التي سبق التطرق إليها إلا أنها تبقى غير كافية في غياب تظافر للجهود الدولية و التي تسعى في مجملها إلى اتخاذ التدابير اللازمة للحد من هذه الجرائم بالنظر إلى الطبيعة الخاصة لها كونها من الجرائم الدولية العابرة للحدود لذلك يجب على جميع الدول أن تسعى إلى تعديل قوانينها الداخلية و جعلها تواكب التطور العلمي والتكنولوجي، و العمل على إبرام اتفاقيات دولية ثنائية و متعددة الأطراف لاحتواء الجريمة والتخفيف منها.

الفصل الثاني :

مكافحة الجريمة الإلكترونية في ظل القانون الوطني (الجزائر أنموذجا)

تمهيد :

شكل الانفجار المعلوماتي الذي تشهده الجزائر ، والتطور المتسارع والمتلاحق لهذه التكنولوجيا تنوعا في الأنشطة الإجرامية تفرغ في جنباتها أجراس الخطر لتنبه حجم المخاطر وهول الخسائر الناجمة عنها ، فعدم كفاية التشريعات الخاصة بها وصعوبة التكييف القانوني لها وإجراءات متابعتها من أهم الصعوبات التي تعتري بالنسبة لمكافحة هذه الجريمة.

من خلال هذا الموقف إرتأينا أن تكون نقطة الانطلاق من عنوان هذا الفصل ، فنتعرض في المبحث الأول إلى المكافحة التشريعية وهذا في ضل القانون العام (قانون العقوبات وقانون الإجراءات الجزائية) والقانون الخاص (قانون الملكية الفكرية وقانون التأمين وقانون البريد ...إلخ) لننتقل إلى المكافحة المؤسساتية في المبحث الثاني .

المبحث الأول : المكافحة التشريعية (القوانين والنصوص) للجريمة الإلكترونية

بما أن المعلومة تمثل قيمة أو ثروة إقتصادية كبرى ، إستوجب ذلك توفير حماية جنائية خاصة ، فالمعلومة أصبحت تقوم ماليا ، وبالتالي تدخل في عتاد الأموال الإقتصادية ، وقد تكون المعلومة شخصية وإفشائها يهدد الحياة الخاصة من جوانب متعددة ، ونظرا للتطور السريع في التكنولوجيا وتقنيات المعلومات (شبكة الأنترنت) ، أظهرت الدراسات الجنائية عدم كفاية النصوص التقليدية في تطبيقها على الجرائم المستحدثة في ظل التطور الهائل في أنظمة معالجة المعلومات ونقلها عبر الشبكات ، وباتت الحاجة ضرورية لاستحداث قواعد قانونية جديدة لمواجهة هذه الجرائم المستحدثة .

المطلب الأول : مكافحة الجريمة الإلكترونية في ظل قانون العقوبات وقانون الإجراءات الجزائية

إن القانون الجنائي التقليدي لا يتطور دائما بنفس السرعة التي تتطور التكنولوجيا الجديدة ، لاسيما أن نصوصه وضعت في عصر لم يكن إستخدام الحاسوب والأنترنت قد ظهر فيه ولم تظهر المشاكل القانونية الناتجة عن إستخدامه ، لكن نجد أن المشرع الجزائري تدارك الفراغ القانوني في مجال الإجرام المعلوماتي وهذا من خلال النصوص المستحدثة سواءا في قانون العقوبات أو الإجراءت المستحدثة في قانون الإجراءات الجزائية .

الفرع الأول : مكافحة الجريمة الإلكترونية في ظل قانون العقوبات

لما كانت الحاجة ملحة و ضرورية لحماية أنظمة المعالجة الآلية إستقر الفكر القانوني على ضرورة وجود نصوص خاصة لهذا الغرض ، و لهذا نجد المشرع الجزائري قدتدارك مؤخرا ولو نسبيا الفراغ القانوني في مجال الاجرام الالكتروني و ذلك باستحداث نصوص تجريمية لقمع الاعتداءات الواردة على المعلوماتية بموجب القانون 15/04[1] المتضمن تعديل قانون العقوبات، لكن تجدر الإشارة إلى أن المشروع الجزائري قد ركز على الاعتداءات الماسة بالأنظمة المعلوماتية ، وأغفل الاعتداءات الماسة بمنتوجات الإعلام الآلي والمتمثلة في التزوير الالكتروني ، وهنا نذكر بعض الجرائم المتعلقة بالجرائم الإلكترونية :

أولا : جريمة المساس بأنظمة المعالجة الآلية للمعطيات

جريمة المساس بأنظمة المعالجة الآلية للمعطيات أو جريمة الغش المعلوماتي وهوالفعل المنصوص و المعاقب عليه في المواد 394 مكرر إلى المادة 394 مكرر07 ، ونجد أّن المشرع الجزائري لم يعرف لنا نظام المعالجة الآلية

[1] القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004 ، المتضمن قانون العقوبات ، الجريدة الرسمية عدد 71صادر في 2004/11/10.

للمعطيات، بالرجوع إلى لاتفاقية الدولية الخاصة بالإجرام الالكتروني قدمت تعريفا للنظام المعلوماتي في مادتها الثانية وكذلك عرفها الفقه الفرنسي[1].

وبالعودة إلى قانون العقوبات الجزائري نجد أن الغش المعلوماتي يأخذ صورتانأساسيتان:

- الدخول في منظومة معلوماتية.
- المساس بالمنظومة المعلوماتية.

1-الدخول في منظومة معلوماتية: و يشمل فعلين هما: الدخول و البقاء.

- **جريمة الدخول غير المشروع:**

تنص المادة 394 مكرر من قانون العقوبات الجزائري ، والتي تقابلها المادة 23 فقرة 01 قانون عقوبات فرنسي على معاقبة كل من يدخل عن طريق الغش في كل جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك ، وتضاعف العقوبة إذا ترتّب على الدخول أو البقاء أو الحذف أو تغيير معطيات المنظومة أو تخريب النظام[2].

- **جريمة البقاء الغير مشروع:**

نص المشرع الجزائري على هذه الجريمة في المادة 394 مكرر من قانون العقوبات الجزائري المقابلة لنص المادة 1/323من قانون العقوبات الفرنسي ، ويقصد بالبقاء الدخول الشرعي أكثر من الوقت المحدّد و ذلك بغية عدم أتاء إتاوة ، وتقوم الجريمة مباشرة على الحاسوب أو سواء حصل الدخول مباشرة على الحاسوب أو حصل بعد كما يجرم ، اللقاء حتى ولو تم بصفة عرضية[3].

2المساس بمنظومة معلوماتية:

تنص المادة 394 مكرر 1من قانون عقوبات جزائري والتي يقابلها في النص الفرنسي المادة 3/323 من قانون العقوبات الفرنسي : على أن "كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدّل بطريق الغش المعطيات التي يتضمنها"[4].

---

[1] الاتفاقية الدولية حول الإجرام المعلوماتي التي أبرمت بتاريخ 2001/11/08 من طرف المجلس الأوربي ، و تم وضعها للتوقيع منذ تاريخ 2001/11/23.

[2] دردور نسيم ، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن ، مذكرة لنيل شهادة الماجستير شعبة القانون الجنائي ، جامعة منتوري قسنطينة ، 2012-2013 ، ص 95 .

[3] د.أحسن بوسقيعة ، الوجيز في القانون الجزئي، الطبعة السادسة ، دار هومة ، الجزائر، 2007 ،ص445.

[4] مرزوق نسيمة ، جرائم الانترنيت، مذكرة تخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر، 2006-2009 ،ص10 .

ثانيا : جريمة التزوير المعلوماتي

إن قانون العقوبات الجزائري لم يستحدث نصا خاصا بالتزوير المعلوماتي الذي يعتبر من أخطر صور الغش المعلوماتي نظرا للدور الهام و الخطير الذي أصبح يقوم به الحاسوب الآن ، و نجد أن المشرع الجزائري نص على التزوير الخاص بالمحررات في القسم الثالث والرابع والخامس من الفصل السابع من الباب الأّول من الكتاب الثالث من قانون العقوبات في المواد من 214 إلى 229 التي تشترط المحرر لتطبيق جريمة التزوير ، ولم يتخذ أي موقف لتوسيع مفهوم المحرر من أجل إدماج المستندات المعلوماتية ضمن المحررات محل جريمة التزوير[1].

كما لم يغفل المشرع عن العقوبات الخاصة بالجرائم الإلكترونية فقد ميزنا بين نوعين من العقوبات وهي عقوبات أصلية وأخرى تكميلية وعقوبات للشخص المعنوي وعقوبة الإشتراك والشروع في هذه الجرائم .

1/العقوبات الأصلية :

نص المشرع الجزائري في القانون رقم 15/04 على عقوبات أصلية لجريمتي الدخول والبقاء غير المشروعان للنظام المعلوماتي، وكذا جريمة المساس بمنظومة معلوماتية وفق الآتي :

-**عقوبة الدخول أو البقاء غير المشروعان للنظام** : في حالة الدخول غير المشروع من طرف المجرم الإلكتروني للنظام كله أو جزء منه أو متى كان مسموح له بالدخول إلى جزء معين من النظام وتجاوزه ، ومتى كان الدخول أو التواجد داخل النظام مخالف لإرادة صاحب النظام ، تكون العقوبة بالحبس من ثلاثة أشهر إلى سنة وغرامة من 50.000دج إلى 100.000 دج طبقا للمادة 394 مكرر من قانون العقوبات رقم 15/04 .

أما في حالة الدخول أو البقاء ونتج عنه حذف أو تغيير لمعطيات المنظومة ، أو انجر عن هذا الدخول أو البقاء تخريب لنظام اشتعال المنظومة ، فإن العقوبة تضاعف إلى الحبس من ستة أشهر إلى سنتين وغرامة من 50.000دج إلى 150.000 دج ، وذلك وفقا للمادة 394 مكرر من قانون العقوبات السابق الذكر.

-**عقوبة المساس بمنظومة معلوماتية** : نص المشرع الجزائري في المادة 394 مكرر 01 من نفس القانون السابق الذكر على عقوبة الإعتداء العمدي على المعطيات الموجودة داخل النظام ، وذلك بالحبس من 06 أشهر إلى 03 سنوات وغرامة من 500.000 دج إلى 2.000.000 دج ، وذلك في حالة ارتكاب الجرائم الماسة بالأنظمة المعلوماتية، وفي حالة حيازة أو إفشاء أو نشر أو استعمال المعطيات المتحصل عليها من إحدى الجرائم الماسة بالأنظمة المعلوماتية تكون العقوبة، الحبس من شهرين إلى 03 سنوات وغرامة من 1.000.000 دج إلى 5.000.000 دج .2

[1] قارة أمال، الجريمة المعلوماتية، رسالة لنيل درجة الماجستير في القانون الجنائي والعلوم الجنائية، جامعة الجزائر، كلية الحقوق، الجزائر، 2002 ، ص 42 .

[2] ختير مسعود، الحماية الجنائية لبرامج الكمبيوتر، أساليب وثغرات ، دار الهدى للنشر والتوزيع، الجزائر ، طبعة ، 2010 ، ص ص 99-100.

2/ العقوبات المقررة للشخص المعنوي

نص المشرع الجزائري في المادة 51 مكرر من القانون رقم 15/04 على مسآلة الشخص المعنوي وذلك وفق شروط :

- أن ترتكب إحدى الجرائم المنصوص عليها قانونا
- أن تكون بواسطة أحد أعضاء أو ممثلي الشخص المعنوي
-أن ترتكب الجريمة لحساب الشخص المعنوي كما نصت المادة 394 مكرر 04 من نفس القانون على العقوبات الواجبة التطبيق على الشخص المعنوي في حالة ارتكابه لأي جريمة اعتداء على نظام المعالجة الألية للمعطيات بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي[1] .

3/ عقوبة الإشتراك والشروع في الجريمة

عقوبة الإشتراك : نصت عليها المادة 394 مكرر 05 من القانون رقم 15/04 بقولها "كل من شارك في مجموعة أو إتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم ، وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية ، يعاقب بالعقوبات المقررة للجريمة ذاتها" .

عقوبة الشروع : نصت عليها المادة 394 مكرر 07 من نفس القانون بقولها "يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها" .

4/العقوبات التكميلية

نصت المادة 394 مكرر 06 من نفس القانون على مجموعة من العقوبات التكميلية ، يحكم بها إلى جانب العقوبات الأصلية وهي كالتالي :

المصادرة : وتعني مصادرة الأجهزة والبرامج والوسائل المستخدمة لارتكاب الجرائم الماسة بالنظام وذلك ببيعها ، أو حجزها مع مراعاة حقوق الغير حسن النية.

إغلاق المواقع : إغلاق مواقع الأنترنت أو المواقع الإلكترونية بصفة عامة ، والتي كانت وسيلة لارتكاب هذه الجرائم أو ساهمت في ارتكابها .

إغلاق المحل (المقهى الإلكتروني) : يكون في الحالة التي يكون صاحب المحل مشاركا في الجريمة ، وذلك إذا تمت الجريمة وهو عالم بها ولم يتصدى لها بالإخبار عنها ، أو بمنع مرتكبيها من ارتياد محله لارتكاب مثل هذه الجرائم[2] .

[1] ختير مسعود ، المرجع السابق ، ص ص 100 – 101 .
[2] نفس المرجع ، ص ص 102 – 103 .

ومن الملاحظ أن هذه العقوبات جاءت رادعة حيث تضاعف عند الضرورة ، كما اشتملت على عقوبات تكميلية ، وحتى عقوبات الشخص المعنوي .

الفرع الثاني : مكافحة الجريمة الإلكترونية في ضل قانون الإجراءات الجزائية

سارع المشرع الجزائري بتعديل قانون الإجراءات الجزائية تماشيا مع التطور لمعلوماتي الذي لحق بالجريمة ، محاولة منه تطويقها والقضاء عليها ، أو على الأقل الحد من إنتشارها ، وذلك في إطار المكافحة الإجرائية لهذا النوع من الإجرام ، حيث أنه بتعديلي 09/01 و 14/04 وضع قواعد وأحكام خاصة لسلطة المتابعة والاختصاص ، الغرض منها هو مواجهتها ، و هذه الأحكام هي[1]:

1.جواز تمديد الاختصاص المحلي للمحكمة :حيث نصت المادة 329 من ق إ ج في فقرتها الأخيرة على جواز تمديد الاختصاص المحلي للمحكمة ليشمل اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

2.توسيع مجال اختصاص النيابة العامة : حيث انه وبموجب المادة 37 من ق إ ج تم توسيع مجال إختصاص النيابة العامة ليشمل نطاقات أخرى لم يكن مرخصا لها بها من قبل حيث نصت هذه المادة على تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة إختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، و جرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف.

3.العمل بنظام المشروعية في تحريك الدعوى العمومية : حيث سحب نظام الملائمة من النيابة العامة في مجال متابعة بعض الجرائم ، حيث يلتزم وكيل الجمهورية بتحريك الدعوى العمومية بقوة القانون بحيث لا يتمتع بشأنها بسلطة الملائمة بين تحريك الدعوى العمومية وعدم تحريكها مثلما فعل في الجرائم المنصوص عليها في المواد 144 مكرر ، 144 مكرر 1 و 144 مكرر 2 من قانون العقوبات المعدل والمتمم بالقانون 09/01 المؤرخ في26 يونيو 2001 .

4.إضافة لما سبق و دائما في إطار المكافحة الاجرائية للجرائم المعلوماتية تم توسيع مجال إختصاص النيابة العامة في مجال البحث والتحري عن هذه الجرائم بمنح الإذن بالتفتيش والقيام باعتراض المراسلات وتسجيل الأصوات والتقاط الصور حسب نص المادة 65 مكرر 5 في إطار تعديل ق إ ج ج بالقانون 22/06 المؤرخ في 2006/12/20 التي تنص "إذا إقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم

[1] معتق عبد اللطيف ، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن ، مذكرة ماجستير ، جامعة الحاج لخضر باتنة ، 2015-2016 ، ص 48 .

المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالصرف وكذا جرائم الفساد ، يجوز لوكيل الجمهورية أن يأذن بما يأتي :

*اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية.

*وضع الترتيبات التقنية ، دون موافقة المعنيين ، من اجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص يتواجدون في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص.

يسمح الإذن المسلم بغرض وضع الترتيبات التقنية بالدخول إلى المحلات السكنية أو غيرها ولو خارج المواعيد المحددة في المادة 47 من هذا القانون وبغير علم أو رضا الأشخاص الذين لهم حق على تلك الاماكن تنفذ العمليات المأذون بها على هذا الاساس تحت المراقبة المباشرة لوكيل الجمهورية المختص" .

5/التسرب : إضافة لما سبق تجدر الإشارة إلى الإجراء الجديد الخاص بمكافحة الجرائم المعلوماتية والمنصوص عليه في المادة 65 مكرر 11من ق إ ج ج ، وهو إجراء التسرب فتنص المادة 65 مكرر 11 على أنه "عندما تقتضي ضرورات التحري أو التحقيق في إحدى الجرائم المذكورة في المادة 65 مكرر 5 أعلاه ، يجوز لوكيل الجمهورية أو لقاضي التحقيق ، بعد إخطار وكيل الجمهورية ، أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب ضمن الشروط المبينة في المواد أدناه " ، وهي المواد 65 مكرر 12 إلى 65 مكرر18 من قانون الإجراءات الجزائية.

وقد عرفت المادة 65 مكرر 12 التسرب على انه "قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في إرتكابهم جناية أو جنحة ، بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف ".

كما سمحت الفقرة الثانية من المادة 65 مكرر 12 أن يستعمل لغرض إجراء التسرب هوية مستعارة أو أن يرتكب عند الضرورة الأفعال المنصوص عليها في المادة 65 مكرر 14 وهذه الافعال هي:

•اقتناء أو نقل أو حيازة أو تسليم أو إعطاء مواد أو أموال أو منتجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها.

•وإستعمال أو وضع تحت تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل أو التخزين أو الإيواء أو الحفظ أو الاتصال.

ويمكن للمتسرب بإتيان هذه الأفعال دون أن تترتب عليه المسؤولية الجزائية لأنه مرخص له بهذه الأفعال بهدف الوصول إلى مرتكبي الجريمة.

وقد بينت المادة 65 مكرر 15 الشروط الواجب توفرها في الإذن بالتسرب ، وهي أن يكون مكتوبا ومسببا و أن يذكر فيه الجريمة التي تبرر اللجوء إلى هذا الإجراء ، وهوية ضابط الشرطة القضائية الذي تتم عملية التسرب تحت مسؤوليته .

كما يجب أن يحدد فيه (أي الإذن) مدة عملية التسرب التي لا يمكن أن تتجاوز أربعة أشهر كما أجازت المادة 65 مكرر 15 إجراء جديد في مكافحة الجريمة الإلكترونية إعتبار ضابط الشرطة القضائية الذي جرت عملية التسرب تحت مسؤوليته كشاهد عن العملية في إجراءات التحقيق فيها.

6/ الإجراءات المادية (المعاينة، التفتيش، الضبط)

* **المعاينة** :هي إجراء بمقتضاه ينتقل المحقق إلى مكان وقوع الجريمة ليشاهد آثارها بنفسه وتقتضي المعاينة إثبات حالة الأشخاص والأشياء[1] ، وكل ما يعتبر في كشف الحقيقة ، وبهذا المعنى تستلزم المعاينة الإنتقال إلى محل الواقعة أو أي محل توجد به أشياء ، أو آثار يرى المحقق أن لها صلة بالجريمة ، كما أن المعاينة في الجريمة التقليدية تكون ذات أهمية متمثلة في تصور كيفية وقوع الجريمة وظروف ملابساتها وتوفير أدلة مادية ، لكن هذه المعاينة لا تؤدي ذات الدور في كشف غموض الجريمة الإلكترونية، وضبط الأشياء التي قد تفيد في إثباتها ونسبتها إلى مرتكبيها، لأن الجريمة التقليدية غالبا لها مسرح تجرى عليه الأحداث التي تخلف آثار مادية ، على خلاف الجريمة الإلكترونية يتضاءل دورها في الإفصاح عن الحقيقة المؤدية للأدلة المطلوبة ، لأن الجريمة الإلكترونية قلما تخلف آثار مادية، وأن كثير من الأشخاص يردون إلى مسرح الجريمة خلال فترة من زمان وقوع الجريمة، وحتى اكتشافها أو التحقيق فيها وهي طويلة نسبيا، الأمر الذي يجعل الجاني يغير أو يتلف أو يعبث بالأثار المادية للجريمة إن وجدت، وهذا ما يورث الشك في دلالة الأدلة المستقاة من المعاينة[2] ، ومن الإجراءات الواجب اتباعها عند إجراء المعاينة ما يلي :

– تصوير جهاز الحاسوب وما قد يتصل به من أجهزة طرفيه ومحتوياته –عدم التسرع في نقل أي مادة معلوماتية للتيقن من عدم وجود أي مجالات مغنطيسية في العالم الخارجي .

– حذف المستندات الخاصة بالإدخال وكذلك مخرجات الحاسوب الورقية.

– ربط الأقراص التي تحمل أدلة مع جهاز يمنع الكتابة عليها ، مما يتيح لجهات التحقيق قراءة بياناتها من دون تغييرها.

[1] عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية، دراسة مقارنة، رسالة مكملة للحصول على درجة الماجستير في القانون العام ، جامعة الشرق الأوسط، 2014 ، ص 77 .

[2] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، مصر، 2002 ، ص ص 20-21 .

* **التفتيش** :التفتيش هو إجراء من إجراءات التحقيق ، يستهدف البحث عن الحقيقة في مستودع السر، لذلك يعتبر من أهم الإجراءات لأنه غالبا ما يسفر عن أدلة مادية تؤدي إلى نسبة الجريمة للمتهم ، والمستهدف من التفتيش هو جهاز الحاسوب بمكوناته المادية (وحدات لكل منها وظيفة معينة متصلة ببعضها البعض في شكل نظام متكامل) ، والمكونات المعنوية (الكيانات المنطقية) ، فعندما يستهدف التفتيش الكيانات المادية لايشكل عائق، وإنما الإشكال يثور عندما ينصب على المكونات المعنوية (البرامج، قواعد البيانات...) ، لأنه هنا يتطلب الكشف عن الرقم السري للمرور إلى الملفات أو الشفرات أو ترميز البيانات[1] .

تفتيش مكونات الحاسوب المادية :لا يوجد مانع قانوني من أن ينصب التفتيش على المكونات المادية للحاسوب وملحقاته ، وذلك تبعا لطبيعة المكان الذي يتواجد فيه الحاسوب ، إذ أن لصفة المكان أهمية خاصة في مجال التفتيش ، فإذا كانت خاصة كمسكن المتهم أو أحد ملحقاته كانت لها حكمه ، فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه ، وحسب المادة رقم 45 ف 3 تنص على "لاتطبق هذه الأحكام إذا تعلق الأمر بجرائم ... والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات " ، والمادة 47 ف 3 تنص على " عندما يتعلق الأمرب ... الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ... فإنه يجوز إجراء التفتيش ... في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل ..." ، والمادة 64 ف 2 وتطبق فضلا عن ذلك أحكام المواد 44-47 من هذا القانون" ، بمعنى عدم تطبيق الضمانات الواردة بهذه المادة بخصوص التفتيش المتعلق بالجريمة الإلكترونية ، حيث لا يشترط حضور الشخص المشتبه في أنه ساهم في ارتكاب الجريمة عند تفتيش مسكنه ، وأنه يجوز القيام بإجراء التفتيش في كل ساعة من ساعات النهار أو الليل ودون حاجة إلى رضائه عند القيام بهذا الإجراء[2] .

مدى خضوع مكونات الحاسوب المعنوية للتفتيش : عرف الفقه اختلاف حول مدى خضوع المكونات المعنوية للحاسوب لإجراءات التفتيش ، وانقسم إلى اتجاهين ، إتجاه يرى عدم جواز تفتيش المكونات المعنوية للحاسوب ، وقد عملت الدول التي تبنت هذا الإتجاه إلى حماية هذه الكيانات المنطقية عبر قانون الملكية الفكرية ، واتجاه آخر يرى إمكانية تفتيش المكونات المعنوية للحاسوب لأن كل ما يشغل حيزا ماديا في فراغ معين، هذا الحيز يمكن قياسه والتحكم فيه ، وبناءا عليه فإن الكيان المنطقي للحاسوب أو البرنامج يشغل حيزا ماديا في ذاكرة الحاسوب ، ويمكن قياسه بمقياس معين هو "البايت " و "الكيلوبايت"و"الميغابايت"، وهكذا تقاس سعة أو حجم

[1] زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى للطباعة والنشر، الجزائر، 2011 ، ص ص131-132 .

[2] سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذ كرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، جامعة الحاج لخضر، باتنة ، 2012-2013 ، ص 145 .

الذاكرة الداخلية للحاسوب بعدد الحروف التي يمكن تخزينها فيها ، غير أن النصوص القانونية التي تنص على أحكام التفتيش تم سنها قبل أن يعرف القانون الأشياء غير المادية ، لذا فإن طبيعة البيانات والمعطيات المعالجة تتطلب قواعد خاصة تحكمها، فالنصوص التقليدية الخاصة بالتفتيش لا يمكن إعمالها على النظم المعلوماتية ، لأن قياسها على الأشياء المادية سيكون منافيا للشرعية الإجرائية[1] .

مدى خضوع شبكات الحاسوب للتفتيش عن بعد : نفرق هنا بين فرضين.

الفرض الأول :إتصال حاسوب المتهم بحاسب موجود في مكان آخر داخل الدولة : لقد أجاز المشرع في المادة 05 من القانون رقم 09-04 إذا كانت هناك أسباب تدعو للإعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية آخرى ، فيجوز تمديد التفتيش بعد إعلام السلطة القضائية المختصة مسبقا بذلك[2] ، حيث تنص المادة 05 منه على " .... في الحالة المنصو ص عليها في الفقرة "أ" من هذه المادة إذا كانت هناك أسباب تدعو للإعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى ، وأن هذه المعطيات يمكن الدخول إليها إنطلاقا من المنظومة الأولى يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك .... ".

الفرض الثاني :إتصال حاسب المتهم بحاسب موجود في مكان آخر خارج الدولة.

ويكون بالدخول إلى منظومة معلوماتية أو جزء منها، وكذا المعطيات المخزنة فيها ولو عن بعد ، وذلك في حالة ما إذا كانت المعطيات القائم البحث عنها يمكن الدخول إليها انطلاقا من منظومة معلوماتية تقع خارج الإقليم الوطني ، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للإتفاقيات الدولية ذات الصلة ، ووفقا لمبدأ المعاملة بالمثل ، تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث، أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها[3] ، حيث تنص المادة 05 من القانون رقم 09-04 على أنه " ... إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى ، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للإتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل ".

* **ضبط الأشياء** : يختلف ضبط الأشياء في الجريمة الإلكترونية عن الضبط في الجريمة التقليدية من حيث المحل ، ففي هذه الأخيرة يكون المحل أشياء مادية، أما في الجريمة الإلكترونية تكن الأشياء ذات طبيعة معنوية كالبيانات ،

[1] سعيداني نعيم ، مرجع سابق ، ص 147 .

[2] المرجع السابق ، ص 148 .

[3] بن دعاس فيصل، إجراءات التحري في الجرائم المعلوماتية، محاضرة في إطار التكوين المحلي المستمر للقضاة، مجلس قضاء قسنطينة ، ص3 .

المراسلات الإلكترونية ، وتجدر الإشارة إلى أن ضبط الأشياء قد يرد على عناصر معلوماتية منفصلة مثل الإسطوانات الممغنطة ، وهنا لا يثور أي إشكال عند القيام بالضبط ، لكن الصعوبة تكون عندما يلزم ضبط النظام كله، أو الشبكة كلها تحتوي على عناصر لا يمكن فصلها ، أما بالنسبة للمكونات المادية للحاسوب فيمكن ضبط الوحدات المعلوماتية الآتية :

- وحدات الإدخال : لوحة المفاتيح، الفأرة، نظام القلم الضوئي.
- ضبط وحدة الإخراج : الشاشة ، الطابعة، الرسم والمصغرات الفيلمية

وكل ما يتم ضبطه من بيانات إلكترونية يتعين تحريزها وتأمينها فنيا ، تنص المادة 06 من القانون رقم 09-04 على أنه":عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم ، أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة ، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية ....".

المطلب الثاني : الحماية والمكافحة في ظل القوانين الخاصة

بالرغم من وجود نصوص وإجراءات قانونية تكفل لنا متابعة المجرم الإلكتروني وهذا في قانون العقوبات وقانون الإجراءات الجزائية ، إلا أن المشرع الجزائري ومن باب الحرص والحد من الجرائم الإلكترونية فقد قام بإستحداث قوانين خاصة من شأنها الحد من هذه الجرائم كقوانين حماية الملكية الفكرية وقانون البريد والمواصلات وقانون التأمينات .

الفرع الأول : مكافحة الجريمة الالكترونية في قوانين الملكية الفكرية

نظرا للاعتداءات التي تتعرض لها مختلف المقترحات الفكرية عبر الانترنيت تطرقنا في بحثنا هذا إلى مدى إمكانية الحماية من خلال نصوص قانون الملكية الفكرية ، سنتوصل في ذلك من خلال نقطتين أساسيتين:

1.الحماية في إطار قانون الملكية الصناعية.

2.الحماية في إطار قانون الملكية الأدبية و الفنية.

أولا : مكافحة الجريمة الالكترونية في اطار الملكية الصناعية

1- في الأمر 03-06 المتعلق بالعلامات التجارية :

تطرق المشرع الجزائري إلى تنظيم أحكام العلامات التجارية من خلال عدة قوانين ، آخرها الأمر رقم 03-06 المؤرخ في 2003/07/19[1] ، والمتعلق بالعلامات وتعرف العلامات التجارية على أنها كل ما يتخذ من تسميات أو رموز أو أشكال توضع على البضائع التي يبيعها التاجر أو يضعها المنتج أو يقدم بإصلاحها أو تجهيزها، أو ختمها لتمييزها عن بقية المبيعات أو المصنوعات[2] ، أو الخدمات ، ومن شروط العلامة التجارية : أن تكون مميّزة ، أن تكون جديدة ، أن تكون غير مخالفة للنظام العام .

2- في الأمر رقم 03-07 المتعلق ببراءات الاختراع :عرفت المادة 02 من الأمر 03-07 الاختراع بأنه فكرة لمخترع تسمح عمليا بإيجاد حل لمشكل محدد في مجال للتقنية ، وبشأن الشروط التي يجب توافرها في الاختراع فتتمثل فيما يلي : (شرط الابتكار ، شرط الجدة ، القابلية للتطبيق الصناعي ، المشروعية)

تجدر الاشارة الى ان المشرع الجزائري قد استبعد البرامج المعلوماتية صراحة منمجال الحماية بواسطة براءات الاختراع وذلك طبقا للمادة 07 من الأمر 03-07 المتضمن براءة الاختراع التي نصت على أنه "لا تعد من قبيل الاختراعات في مفهوم هذا الأمر برامج الحاسوب"

[1] الأمر رقم 03-06 المؤرخ في 19جويلية2003 المتعلق بالعلامات التجارية،ج ر عدد ،44 صادر في 23جويلية2003

[2] الأمر رقم 03-07المؤرخ في ،2003/07/19المتعلق ببراءات الاختراع،ج ر عدد 44صادر في23جويلية 2003

ثانيا : مكافحة الجريمة الالكترونية من خلال القوانين الأدبية و الفنية

نظرا للتطور الذي واكب مجال الاتصال ، و الذي رافقه تطور في وسائل نقل الإنتاج الفكري ، على إختلاف صوره من علوم وفنون وآداب ، مما أوجد مصنفات جديدة جديرة بحماية حق المؤلف ، و قد كان من أهم هذه المصنفات التي حضها بالاهتمام من قبل المختصين في مجال الملكية الفكرية نجد المصنفات الخاصة ببرامج الحاسبات الالكترونية ، وقواعد البيانات التي كانت طبيعتها التقنية تختلف عن المصنفات التقليدية الامر الذي تطلب متابعتها باستمرار ووضع قواعد قانونية محددة وثابتة لحمايتها .

-اتجه المشرع الجزائري إلى الاعتراف صراحة بوصف المصنف المحمي لمصنفات الإعلام الآلي ، و ذلك من خلال تعديله للأمر 73-14 بموجب الأمر 97-10[1] والذي يتبين من خلال إستقراءها ما يلي:

1-أن المشرع وسع قائمة المؤلفات المحمية حيث أدمج تطبيقات الاعلام الآلي ضمنالمصنفات الأصلية و التي عبّر عنها بمصنفات قواعد البيانات وبرامج الإعلام الآلي ، التي تمكن من القيام بنشاط علمي أو أي نشاط من نوع آخر أو الحصول على نتيجة خاصة من المعلومات التي تقرأ بآلة و تترجم بإنتفاعات الكترونية بالحاسوب ، أما قواعد البيانات فهي مجموعة المصنفات والأساليب والقواعد ، ويمكن أن تشمل أيضا الوثائق المتعلقة بسير المعطيات.

2-أن الحماية تحدّد من 25 إلى 50 سنة بعد وفاة المبدع تماشيا مع اتفاقية برن التي حدّدت كمدة دنيا للحماية 50 سنة ، وبالتالي هذه المدة تشمل حتى مصنفات الاعلام الآلي .

3-تشديد العقوبات الناجمة عن المساس بحقوق المؤلفين لا سيما مؤلفي المصنفات المعلوماتية .

الفرع الثاني : مكافحة الجريمة الالكترونية في القانون 2000-03 المتعلق بالبريد والمواصلات السلكية واللاسلكية

قانون رقم 2000-03 المؤرخ في 2000/08/05 والذي يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية :

تسارع هذا القانون الى مواكبة التطور الذي شهدته التشريعات العالمية مسايرة التطور التكنولوجي لذلك بات من السهولة بمكان إجراء التحويلات المالية عن الطريق الالكتروني ذلك ما نصت عليه المادة 87 من هذا

[1] أمر رقم 97-10 مؤرخ في 06-03-1997المتعلق بحق المؤلف و الحقوق المجاورة، الجريدة الرسمية عدد 13 الصادر في 1997/03/12معدّل و متم بأمر 05-03مؤرخ في 2003/07/19 المتعلق بحقوق المؤلف ، والحقوق المجاورة ، الجريدة الرسمية عدد 44 الصادر في 2003/07/23 .

القانون بالقول " يمكن أن ترسل الأموال ضمن النظام الداخلي بواسطة الحوالات الصادرة عن المتعامل والمحولة بالبريد أو البرق أو عن الطريق الإلكتروني"[1] .

نصت المادة 2/84 منه بقولها " تطبق أحكام المادة 89 من هذا القانون عن استعمال حوالات دفع عادية أو الكترونية أو برقية"[2].

نصت المادة 105 الفقرة الأخيرة على أنه " لا يمكن بأي حال من الأحوال انتهاك حرمة المراسلات".

رتبت المادة 127 منه جزاء كل من تسول له نفسه وبحكم مهنته أن يفتح أو يحول أو يخرب البريد أو ينتهك حرمة المراسلات بنصها : " كل موظف أو عون من أعوان الدولة أو مستخدم أو مندوب عن مصلحة البريد يقوم اختلاس أو إتلاف رسائل مسلمة إلى البريد أو يسهل فضها أو اختلاسها أو إتلافها يعاقب بالحبس من ثلاثة أشهر إلى خمس سنوات وبغرامة من 30.000 دج إلى 500.000 دج ، ويعاقب بالعقوبة نفسها كل مستخدم أو مندوب في مصلحة البرق أو يختلس أن يتلف برقية أو يذيع محتواها .

ويعاقب الجاني فضلا عن ذلك بالحرمان من كافة الوظائف أو الخدمات العمومية من خمس إلى عشر سنوات[3] .

الفرع الثالث : مكافحة الجريمة الالكترونية في القانون 08-01 المتعلق بالتأمينات

قانون رقم 08-01 المؤرخ في 2008/01/23 والمتمم لقانون رقم 01-83 متعلق بالتأمينات :

المادة 6 مكرر 1 نصت على أنه البطاقة الالكترونية تسلم للمؤمن له إجتماعيا مجانا من طرف هيئات الضمان الاجتماعي وهي صالحة في كل التراب الوطني وهي تقدم لكل مقدم علاج أو مقدم خدمات مرتبطة بالعلاج وهذا الأخير يزود إلكترونيا ويسمى " المفتاح الالكتروني لهيكل العلاج " حسب نص المادة 65 مكرر[4].

نصت المادة 93 مكرر 2 منه على معاقبة كل من يسلم أو يستلم البطاقة الالكترونية بغرض إستعمالها بطريقة غير مشروعة وجاءت كما يلي : "دون الإخلال بالعقوبات المنصوص عليها في التشريع المعمول به ، يعاقب بالحبس من سنتين إلى خمس سنوات وبغرامة من 200.000دج إلى100.000دجكل من يسلم أو يستلم بهدف الاستعمال غير المشروع البطاقة الالكترونية للمؤمن له إجتماعيا أو المفتاح الالكتروني لهيكل العلاج أو المفتاح الالكتروني لمهن الصحة"[5].

---

[1] المادة 87 من القانون رقم 2000-03المؤرخ في 2000/08/05 والذي يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية ، الجريدة الرسمية رقم 48 بتاريخ 2000/08/05 .

[2] المادة ، 2/84 نفس القانون.

[3] المادة 127نفس القانون.

[4] زبيخة زيدان ، الجريمة المعلوماتية في التشريع الجزائري و الدولي ، دار الهدى ، عين مليلة ، الجزائر ،2011 ، ص 77-78.

[5] المادة 93مكرر2 ، قانون رقم 01.08 المؤرخ في 2008/01/23والمتم لقانون رقم : 83-01متعلق بالتأمينات.

نصت المادة 93 مكرر 3 على أنه من يقوم عن طريق الغش بتعديل أو حذف كلي أو جزئي للمعطيات التقنية أو الإدارية المدرجة في البطاقة الالكترونية للمؤمن له اجتماعيا أو في المفتاح الالكتروني لهيكل العلاج أو في المفتاح الالكتروني لمهن الصحة وهي نفس العقوبة التي تطلق كذلك على كل من قام بتعديل أو نسخ وبطريقة غير مشروعة البرمجيات التي تسمح بالوصول أو باستعمال المعطيات المدرجة في البطاقة الالكترونية للمؤمن له اجتماعيا أو في المفتاح الالكتروني لهيكل العلاج أو مهن الصحة[1] .

الفرع الرابع : مكافحة الجريمة الالكترونية في القانون 09-04 المتعلق بالجرائم المتصلة بتكنولوجيا الإعلام والإتصال

صدر القانون 09-04 مؤرخ في 14شعبان 1430 الموافق 2009/08/05 للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها ، ويتضمن 19 مادة موزعة على ستة فصول ، وهو ثمرة عامين من التحضير والدراسة والتحليل والمقارنة مع أحدث القوانين ،

وقامت بإعداده نخبة من رجال القانون بمشاركة خبراء ومهنيين مختصين في مجال الإعلام الإلكتروني من كافة القطاعات المهنية ، كما يتضمن القانون أحكام خاصة بالمراقبة الإلكترونية التي لا يجوز إجراؤها إلا بإذن من السلطة القضائية المختصة وفي حالات تم تحديدها وهي الأفعال الموصوفة بجرائم الإرهاب والتخريب، والجرائم الماسة بأمن الدولة أوحالة توفير معلومات عن اعتداء محتمل يهدد منظومة من المنظومات المعلوماتية لمؤسسات الدولة أو الدفاع الوطني أو

النظام العام .وينص القانون على إنشاء هيئة وطنية للوقاية من الإجرام المتصل بتكنولوجيات الإعلام والإتصال ومكافحته ، تتولى تنشيط وتنسيق عمليات الوقاية من الجرائم الإلكترونية ومساعدة مصالح الشرطة القضائية في التحريات التي تجريها بشأن هذه الجرائم ، كما تتكفل اللجنة أيضا بتبادل المعلومات مع نظيراتها في الخارج ، علما بأن القانون أكد على مبدأ التعاون الدولي من منطلق المعاملة بالمثل .

يعتبر القانون رقم 09-04 ذو نطاق شامل في مجال مكافحة الجريمة الإلكترونية ، حيث جاء تجريمه للأفعال المخالفة للقانون و التي ترتكب عبر وسائل الاتصال عامة ، وبالتالي فهو يطبق على كل التكنولوجيات الجديدة والقديمة بما فيها شبكة الأنترنت وعلى كل تقنية تظهر مستقبلا [2].

ومنه نستعرض بعض المواد :

[1] المادة 93مكرر3 ، نفس المرجع .

[2] طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، الإسكندرية ، 2009 ، ص ص 342-343

نصت المادة 2 منه على مفهوم كل من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال منظومة المعلوماتية ، معطيات معلوماتية ، مقدمو الخدمات ، المعطيات المتعلقة بحركة السير ، الإتصالات الإلكترونية .

نصت المادة 4 منه على مراقبة الإتصالات الإلكترونية الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية.

نصت المادة 5منه على القواعد الإجرائية تفتيش المنظومات المعلوماتية.

نصت المادة 6منه على حجز المعطيات المعلوماتية.

نصت المادة 7على الحجز عن طريق منع الوصول إلى المعطيات .

نصت المادة 8 على المعطيات المحجوزة ذات المحتوى الإجرام.

نصت المادة 9 على حدود إستعمال المعطيات المتحصل عليها.

نصت المادة 10على إلتزامات مقدمي الخدمات مساعدة السلطات.

نصت المادة 11 على حفظ المعطيات المتعلقة بحركة السير.

نصت المادة 12 على الإلتزامات الخاصة بمقدمي خدمة الإنترنت.

نصت المادة 13 و 14 على إنشاء مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها[1] .

كما نستعرض بعض الإجراءات في عمليات التحري في هذا المجال :

أولا :مراقبة الإتصالات الإلكترونية

نصت المادة الرابعة من هذا القانون على الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية و هي على النحو التالي:

1-الرقابة على الأفعال الموصوفة بجرائم الإرهاب أو التخريب و الجرائم الماسة بأمن الدولة.

2-حالة توفر معلومات عن إحتمال إعتداء على منظومة معلوماتية على نحو يهدد النظام أو الدفاع الوطني أو مؤسسات الدولة أو الإقتصاد الوطني.

3-لمقتضيات التحريات والتحقيقات القضائية ، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.

4-في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

لا يتم هذا الإجراء إلا بإذن مكتوب من السلطة القضائية المختصة.

[1] قانون ، 09-04المرجع السابق .

عندما يتعلق الأمر بالحالة الأولى من المادة الرابعة يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية التابعين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ، إذنا لمدة 6 أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها.

ثانيا : تفتيش المنظومة المعلوماتية

لقد أجاز هذا القانون من خلال مادته الخامسة للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في الحالات الضرورية المنصوص عليها سابقا ، الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها ومنظومة تخزين معلوماتية.

كما بين القانون بأنه يجوز تمديد التفتيش بسرعة إلى المنظومة المعلوماتية أو جزء منها إذا كانت هناك أسباب تدعو للإعتقاد بأنه يمكن الدخول إليها ، و هذا بعد إعلام السلطة القضائية المختصة مسبقا بذلك.

وأضاف القانون بأنه في حالة ما إذا كانت المعطيات المبحوث عنها يمكن الدخول إليها إنطلاقا من منظومة معلوماتية تقع خارج الإقليم الوطني ، يكون الحصول عليها بمساعدة السلطات الأجنبية المختصة طبقا للإتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل.

كما أجاز القانون لسلطات التفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها ، قصد مساعدتها و تزويدها بكل المعلومات الضرورية لعملها[1].

ثالثا :حجز المعطيات المعلوماتية

حسب هذا القانون إنطلاقا من مادته رقم 06 يتم نسخ المعطيات محل البحث و كذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية ، تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية .

ويجوز إستعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات قصد جعلها قابلة للإستغلال لأغراض التحقيق شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات.

كما نص القانون من خلال مادته رقم 08 على إمكانية الحجز عن طريق منع الوصول إلى المعطيات و ذلك بأمر من السلطة التي تباشر التفتيش عن طريق تكليف أي شخص مؤهل مع إستعمال وسائل تقنية مناسبة لذلك .

[1] د. خلدون عيشة ، المرجع السابق ، ص 53 .

ربعا :حفظ المعطيات المتعلقة بحركة السير

ألزم ذات القانون من خلال مواده رقم 10 و 11 مقدمي الخدمات بتقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع و تسجيل المعطيات المتعلقة بمحتوى الإتصالات في حينها.

وهذا بوضع المعطيات التي يتعين عليها حفظها تحت تصرف السلطات المذكورة مع كتمان سرية هذه العمليات ، إذ يقوم مقدموا الخدمات بحفظ مايلي :

1-لمعطيات التي تسمح بالتعرف على مستعملي الخدمة.

2-المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للإتصال.

3-الخصائص التقنية و كذا تاريخ و وقت و مدة كل إتصال.

4-المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة و مقدميها.

5-المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الإتصال ، و كذا عناوين المواقع المطلع عليها.

تحدد مدة هذه المعطيات بسنة واحدة إبتداء من تاريخ التسجيل ، مع الإشارة إلى قيام المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عند عدم إحترامهم للإلتزامات المنصوص عليها قانونا مما يؤدي إلى عرقلة حسن سير التحريات القضائية ، إذ يعاقب الشخص الطبيعي بالحبس من ستة أشهر إلى خمس سنوات و بغرامة من 50.000دج إلى 500.000 دج ، أما الشخص المعنوي فيعاقب بالغرامة المحددة وفقا للقواعد المقررة في قانون العقوبات.

كما ألزم القانون إنطلاقا من المادة رقم 12 مقدمي خدمات الإنترنت بالقيام بما يلي:

1-التدخل الفوري لسحب المحتويات التي يسمح الإطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين و تخزينها أو جعل الدخول إليها غير ممكن.

2-وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها[1].

[1] د. خلدون عيشة ، المرجع السابق ، ص 55 .

المبحث الثاني : المكافحة المؤسساتية للجريمة الإلكترونية

يمكن القول أن المحقق هو من يتولى التحقيق من رجال الضبطية القضائية ، أو من أعضاء النيابة العامة ، أو قضاة التحقيق ويلحق بالمحقق الجنائي الباحث الجنائي الذي يكون غالبا من الشرطية القضائية ، الذين خول لهم القانون مهمة جمع الاستدلالات عن المشتبه بهم .

وسنحاول من خلال هذا المبحث استعراض أبرز الهيئات المختصة في مجال مكافحة الجرائم الإلكترونية ، وسنتناول الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بالمطلب الأول ، إضافة لتلك الوحدات التابعة لسلك الامن ، وكذلك تلك التابعة لقيادة الدرك الوطني بما يسمى الضبطية القضائية في مطلب ثاني .

المطلب الأول : الهيئة الوطنية للوقاية من الجرائم المتصلة بتيكنولوجيا الإعلام والإتصال

تتمثل جرائم الإعلام والاتصال في جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وكل الجرائم التي يتم ارتكابها أو يسهل ارتكابها عن طريق منظومة معلوماتيةأو باستعمال نظام الاتصالات الإلكترونية وفقا لما ورد في نص **الفقرة أ من المادة 2 من قانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها**.

لذلك تم إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بموجب نص **المادة 13من القانون المشار إليه أعلاه** والتي يتم تحديد تشكيلتها وتنظيمها وسيرها عن طريق التنظيم ، وكان ذلك بهدف مساعدة السلطات القضائية ومصالح الأمن الوطني في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وانجاز الخبرات القضائية[1] ، وتعد الهيئة بمثابة سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي توضع لدى وزير العدل بمدينة الجزائر وفقا لنص **المادتين 03 و 04 من المرسوم الرئاسي رقم 15-261 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها**[2].

---

[1] حابت أمال، "الطابع الخصوصي للإجراءات الجزائية في شأن الجرائم الإلكترونية في القانون الجزائري،" مداخلة ألقيت في الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، يومي 16و 17نوفمبر 2015 ، ص11.

[2] المرسوم الرئاسي رقم 15-261المؤرخ في 08 أكتوبر 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة تكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر.ج.ج عدد 53 الصادرة في 08أكتوبر 2015جاء نص المادة 01 منه كما يلي «تطبيقا لأحكام المادة 13من القانون رقم 09-04المؤرخ في 14شعبان عام 1430الموافق 5غشت سنة 2009 والمذكور أعلاه، يهدف المرسوم إلى تحديد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها التي تدعى في صلب النص الهيئة» .

وقد نظم كل من ق.ر **09-04 السابق الذكر والمرسوم الرئاسي 15-261** تنظيم عمل الهيئة ، أما بالنسبة لتشكيلتها وكيفية سيرها فقد تم إدراجهما في المرسوم السالف الذكر.

الفرع الأول : تشكيلة الهيئة وتنظيمها

حدد الفصل الثاني من المرسوم الرئاسي المشار إليه أعلاه تشكيلة الهيئة بحيث أنها تضم هياكل تقنية وإدارية.

أولا : الهياكل الإدارية

تشمل الهياكل الإدارية للهيئة على اللجنة المديرة والمديرية العامة تكلفان بإدارتها بحيث يرأس اللجنة المديرة وزير العدل وتتشكل من أعضاء حكوميين يتمثلون في الوزير المكلف بالداخلية، وزير البريد وتكنولوجيات الإعلام والاتصال وممثل عن رئاسة الجمهورية بالإضافة إلى مسئولين من مصالح الأمن الوطني وقاضيان من المحكمة العليا يعينهما المجلس الأعلى للقضاء وفقا لما نصت عليه **م 07 من المرسوم المشار إليه أعلاه** ، وتكلف بكل ما يتعلق بتنظيم سير عمل الهيئة بصفة عامة وتقييم حالة الخطر بخصوص الجرائم الواقعة على أمن الدولة لتحديد عمليات المراقبة الإلكترونية وأهدافها.

أّما بالنسبة للمديرية العامة فيديرها مدير عام يتم تعيينه وانهاء مهامه بموجب مرسوم رئاسي طبقا لنص **م 09 من المرسوم الرئاسي 15-261** ويكلف بمجموعة من المهام التي تدخل ضمن صلاحياته والمتمثلة أساسا في التسيير الإداري والمالي للهيئة وتنفيذ عملها مع تنسيق ومتابعة أعمال هياكلها ومراقبتها وتمثيلها على المستوى الوطني والدولي ، وكذا القيام بإجراءات التأهيل وأداء اليمين بالنسبة للمستخدمين وممارسة السلطة السلمية عليهم، بالإضافة إلى سهره على احترام قواعد السر المهني للهيئة، زيادة على ذلك يقوم بإعداد تقرير سنوي لنشاطها وعرضه على اللجنة المديرة لتصادق عليه مع قيامه بتحضير اجتماعات هذه اللجنة[1].

ثانيا : الهياكل التقنية

تضم الهيئة هيكلين تقنيين يتمثلان في مديرية المراقبة الوقائية لليقظة الإلكترونية ومديرية التنسيق التقني يكلفان بمهام الوقاية من الجرائم الإلكترونية ومكافحتها.

تشمل مديرية المراقبة الوقائية واليقظة الإلكترونية كل من ملحقات جهوية تقوم بتشغيلها[2] ، ومركز للعمليات التقنية الذي تشغله المديرية، والذي يتم تزويده بمجموعة من المنشآت والتجهيزات والوسائل للقيام

[1] المادة 10من المرسوم الرئاسي 15-261 مرجع سابق ، ص17 .

[2] المادة 14 مرجع نفسه، ص18.

بالمراقبة التقنية للاتصالات الإلكترونية وفقا لنص **م 13 من المرسوم المذكور أعلاه** ، وتكلف المديرية بعدة اختصاصات والتي يمكن تلخيصها فيما يلي:

_ تنفيذ عمليات المراقبة الوقائية للاتصالات الإلكترونية للكشف عن الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال بموجب رخصة مكتوبة من السلطة القضائية وتحت مراقبتها طبقا للتشريع الساري المفعول وارسالها إلى كل من هذه السلطة والشرطة القضائية.

_ جمع كل المعلومات والبيانات المتعلقة بالكشف عن الجرائم الإلكترونية بهدف استغلالها وتقديمها تلقائيا أو بناءا على طلب لكل من السلطات القضائية ومصالح الأمن الوطني .

_ تنفيذ توجيهات اللجنة المديرة وطلبات المساعدة القضائية الدولية بخصوص جمع المعلومات، المعطيات المتعلقة بالمجرمين وتحديد أماكن تواجدهم.

_ القيام بعمليات التوعية حول استعمالات تكنولوجيات الإعلام والاتصال والمخاطر التي تنجر عنها بهدف الحد من الجريمة الإلكترونية.

_ السهر على حسن سير عمل مركز العمليات التقنية وملحقاتها الجهوية مع الحفاظ على منشآتها وتجهيزاتها وما تحتويه من وسائل تقنية ، وكذا الحفاظ على السر المهني في تأدية أعمالها[1].

أما فيما يخص مديرية التنسيق التقني فوفقا لنص **م 12 من الرسوم المرسوم الرئاسي رقم 15-261** تكلف باختصاصات تتمثل أساسا في مجموعة من المهام تتلخص في تسيير منظومة الإعلام للهيئة وادارتها ، مع إنجاز الخبرات التي تدخل في مجال اختصاصاتها ، بالإضافة إلى إنشائها لقاعدة معلومات لحفظ المعطيات والبيانات التحليلية الجنائية المتعلقة بالجرائم الإلكترونية واعداد إحصائيات وطنية لهذه الجرائم ، كما تقوم بكل دراسة أو تحليل أو تقييم لصلاحياتها إمّا من تلقاء نفسها أو بطلب من طرف اللجنة المختصة .

الفرع الثاني : سير الهيئة

تضمن الفصل الثالث من **المرسوم الرئاسي رقم 15-261** على كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، حيث تقوم بعقد إجتماعات والمصادقة على النظام الداخلي لها ، بالإضافة إلى تزويد مختلف هياكلها بالتشكيلة البشرية لضمان سير عمل الهيئة ، لها صلاحية طلب أي معلومات أو وثائق تفيدها من مؤسسة أو مصلحة معينة بغرض تأدية مهامها وطلب المساعدة من موظفين تقنيين في مجال تكنولوجيات الإعلام والاتصال العاملين في وزارات أخرى وفقا للشروط الواردة في التنظيم الساري المفعول ، كما

[1] المادة 11 من المرسوم الرئاسي رقم 15-261 ، مرجع سابق، ص18

خّول لها القيام بإجراءات التحقيق ومراقبة الاتصالات الإلكترونية مع تجميعها وحفظها من طرف التقنيين الموكل إليهم ذلك ، وكذلك ضمان سرية هذه العملية، والحفاظ على السر المهني ومعاقبة كل موظف يستغل المعلومات والمعطيات المتحصل عليها في أغراض أخرى غير الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال .

الفرع الثالث : مهام الهيئة

تتجلى عموما مهام الهيئة في مجال الوقاية ومكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، حيث حددت **م 14ق.ر09-04** مهام الهيئة التي تتمثل في تنشيط وتنسيق عمليات الوقاية ومكافحة الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال بمساعدة السلطات القضائية وأجهزة الأمن الوطني، جمع المعلومات والخبرات القضائية وتبادل المعلومات مع نظيراتها في الخارج بغرض جمع كل البيانات ذات الصلة بأماكن تواجد مرتكبي الجرائم الإلكترونية .

بالإضافة إلى ذلك نجد **المرسوم الرئاسي رقم 15-261 في م 04** منه تضمنت مزيدا من التفاصيل بشأن مهام الهيئة ، بحيث يمكنها أن تجري جميع عمليات التحري والتحقيق في إطار الوقاية من الجرائم الإلكترونية ، مساعدة السلطات القضائية وأجهزة الأمن الوطني في مجال مكافحة هذه الجرائم وتضمن تنفيذ طلبات المساعدة للدول الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي ، والمساهمة في تكوين وتدريب المحققين في مجال التحقيقات التقنية في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

المطلب الثاني : الضبطية القضائية

نظرا لخصوصية الجريمة الإلكترونية كان محتما توفير كوادر ، وأجهزة متخصصة تعنى بعملية البحث والتحري عن الجريمة الإلكترونية ، وكان ذلك إما على مستوى جهاز الشرطة أو الدرك الوطني .

الفرع الأول : الوحدات التابعة لسلك الأمن الوطني

تعد الجريمة الإلكترونية وجه جديد للجرائم يستلزم استحداث هياكل جديدة وتدعيم الهياكل القديمة المختصة في مكافحة الجرائم على مستوى المديرية العامة للأمن الوطني ، وعلى هذا الأساس قررت القيادة العليا للأمن الوطني إستحداث مخابر وفصائل وخلايا مختصة في مكافحة الجرائم الإلكترونية، والقيام بعمليات التحسس والتوعية من خلال المشاركة في الملتقيات الوطنية والدولية وجميع التظاهرات التي من شأنها توعية المواطن ، بالإضافة إلى تنظيم دروس توعوية في مختلف الأطوار الدراسية[1].

أولا: النيابة المديرية للشرطة العلمية على المستوى المركزي

قامت المديرية العامة للأمن الوطني بتحديث بنيتها الهيكلية من خلال إنشاء وحدات متخصصة تعمل عل مكافحة نوع معين من الجرائم دون سواها، وهذا باستحداث أربعة (04) وحدات نيابية متخصصة تتمثل في:

- نيابة الشرطة العلمية والتقنية.
- نيابة مديرية الاقتصادية والمالية.
- نيابة القضايا الجنائية.
- مصلحة البحث والتحليل[2].

وما يهم في دراستنا هي مديرية النيابة للشرطة العلمية والتقنية التي تتألف من مخبر مركزي على مستوى الجزائر العاصمة وثلاثة (03) مخابر جهوية، ويتكون كل مخبر من دائرتين دائرة للشرطة العلمية وأخرى تقنية ، وتتمثل المهمة الرئيسية للمخبر المركزي بالمساهمة إلى جانب أجهزة العدالة في إظهار الحقيقة عن طريق تقديم المساعدات التي تطلبها الهيئات القضائية فيما يتعلق بتفسير وتحليل الآثار المادية التي يعثر عليها في مسرح الجريمة أثناء عملية التحري والتحقيق[3].

---

[1] حملاوي عبد الرحمان، دور المديرية العامة للأمن الوطني في مكافحة الجرائم الإلكترونية ، مداخلة ألقيت في الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة ،كلية الحقوق والعلوم السياسية ، جامعة محمد خيضر، بسكرة ، يومي 16-17نوفمبر ، 2015 ص ص 08-09 .

[2] ربيعي حسين ، آليات البحث والتحقيق في الجرائم المعلوماتية ، أطروحة لنيل شهادة الدكتوراه في الحقوق ، فرع: قانون العقوبات والعلوم الجنائية ،كلية الحقوق والعلوم السياسية ، جامعة باتنة ،2016 ، ص 177 .

[3] بهلول مليكة ، دور الشرطة العلمية والتقنية في الكشف عن الجريمة ، أطروحة لنيل شهادة الدكتوراه علوم، فرع: الحقوق ،كلية الحقوق ، جامعة الجزائر ،2013 ، ص140 .

1 –دائرة الشرطة العلمية:

تتكون مصلحة الشرطة العلمية من ستة (06) فروع[1] ، تتولى تحليل وفحص الأدلة[2] ، المتصلة بالمجال البيولوجي، الطب الشرعي ، الكيمياء ، المخدرات وكذلك تلك المتعلقة بمجال التسميم والحرائق والمتفجرات.

2–دائرة الشرطة التقنية:

تتولى دائرة الشرطة العلمية مهام البحث والتحقيق وتحليل الأدلة الجنائية الناتجة عن الجرائم التي تستعمل فيها القذائف بمختلف أنواعها ، وكذلك جرائم التزوير ، إضافة إلى الجرائم الإلكترونيةحيث تقوم الشرطة التقنية بمباشرة الإجراءات الخاصة بكل جريمة على مستوى الفروع الخاصةبكل نوع من الجرائم .

ثانيا: دائرة الأدلة الرقمية والآثار التكنولوجية على المستوى الجهوي

بالإضافة إلى المخبر المركزي الذي يتواجد بالجزائر العاصمة يوجد أيضا مخبرين جهويين على مستوى كل من قسنطينة ووهران يتوليان أعمال البحث والتحري في الجرائم، بما فيها الجريمة الإلكترونية وهذا تحت تسمية دائرة الأدلة الرقمية والآثار التكنولوجية والتي لم تكن سوى قسم عند إستحداثها سنة 2004 وبسبب الارتفاع المتزايد لقضايا الجرائم الإلكترونية باستعمال تقنية المعلومات تم ترقيتها إلى دائرة تضم ثلاثة (03) أقسام :

- قسم استغلال الأدلة الرقمية الناتجة عن الحاسوب والشبكات.
- قسم استغلال الأدلة الناتجة عن الهواتف النقالة.
- قسم تحليل الأصوات (يتواجد على مستوى المخبر المركزي بالجزائر العاصمة).

في سنة 2010 تم خلق ما يقارب 23 خلية لمكافحة الجرائم الإلكترونية موزعة على كل ربوع الوطن شرق، وسط، غرب وجنوب[3] ، وتكلف الدائرة بعدة مهام ، من بينها البحث والتحري بحيث أّن أعضاء الدائرة عادة ما يستجيبون للطلبات التي يقدمها لهم أعوان الشرطة التابعون لخلايا مكافحة الجرائم الإلكترونية الموزعة على كل مديريات الأمن الوطني أو لطلبات وكيل الجمهورية ، أو قاضي التحقيق التي تردهم في شكل إنابة قضائية من أجل دعمهم ومساعدتهم أثناء إجراء المعاينة لمسرح الجريمة لحجز الأدلة المتواجدة عليها ، وكذلك ضمان الدعم التقني لمختلف مصالح الشرطة والأجهزة القضائية من طرف خبراء مؤهلين إذ أنه في مرحلة التحقيق لا يتعدى

[1] تتكون دائرة الشرطة العلمية من ستة (6)فروع تتمثل في: فرع البيولوجية والبصمة الوراثية، فرع الكيمياء الشرعية،فرع المتفجرات والحرائق، فرع التسمم الشرعي، فرع مراقبة النوعية الغذائية وفرع الطب الشرعي.

[2] بهلول مليكة، مرجع سابق، ص 147.

[3] حملاوي عبد الرحمان، مرجع سابق، ص 08 .

دورهم إعداد تقارير الخبرة التي يطلبها كل من قاضي التحقيق ووكيل الجمهورية على الأدلة التي تم ضبطها كتحليل محتوى الأقراص الصلبة أو المواقع التي تم اختراقها[1].

من الأمثلة الواقعة بالجزائر في هذا الصدد ، جريمة تعود حيثياتها إلى جويلية 2013 إثر تلقي مصالح الأمن الوطني بالجزائر العاصمة شكوى من وزارتي التعليم العالي والبحث العلمي وبريد الجزائر ، مفادها اختراق لمواقعها الإلكترونية والمعلوماتية من طرف هاكر جزائري ينتحل هوية الرئيس الراحل صدام حسين باسم مستعار "صدام 2013" وعلى إثرها باشرت الجهات المختصة في مكافحة الجرائم الإلكترونية لتحرياتها عن هذا الهاكر، وتم تحديد هويته الحقيقية وتنقلت الضبطية القضائية إلى مسكنه في أولاد ميمون بتلمسان وهو شاب يبلغ 22 سنة[2].

الفرع الثاني : الوحدات التابعة للدرك الوطني

اهتمت قيادة الدرك الوطني بمكافحة الجريمة الإلكترونية بمختلف أشكالها وأنواعها ، وهذا من خلال استحداث هياكل تابعة لها من أجل التصدي للإجرام المعلوماتي الذي بات يشكل تهديدا خطيرا على أمن الدولة وسلامة المجتمع ، وعليه تم إنشاء أربعة (04) وحدات تنشط في مجال الوقاية من الجريمة الإلكترونية ومكافحتها والتي سنعرضها في هذا الفرع لنبّين أهم ما تقوم به في هذا المجال.

أولا: المعهد الوطني للأدلة الجنائية وعلم الإجرام

تم إنشاء المعهد الوطني للأدلة الجنائية وعلم الإجرام بموجب **المرسوم الرئاسي رقم 04-183 المتضمن إحداث المعهد الوطني للأدلة الجناية وعلم الإجرام للدرك الوطني وتحديد قانونها الأساسي[3]**، وفقا لنص **م 02 من هذا المرسوم** يعتبر المعهد مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلال المالي ، ويوضع تحت وصاية وزارة الدفاع الوطني في بوشاوي بالجزائر العاصمة ، فهو يخضع لجميع الأحكام التشريعية والتنظيمية العسكرية ، وقد صنف من بين المعاهد الكبرى في العالم[4].

[1] ربيعي حسين، مرجع سابق، ص 180

[2] الموقع الرسمي لمديرية الأمن الوطني ، www.dgsn.dz

[3] المرسوم الرئاسي رقم 04-183المؤرخ في 26يونيو2004 ،المتضمن إحداث المعهد الوطني للأدلة الجنائية وعلمةالإجرام للدرك الوطني وتحديد قانونه الأساسي ، ج.ر.ج.ج عدد 41، الصادرة في 27يونيو 2004 ، ص ص 21-22 .

[4] بهلول مليكة، مرجع سابق، ص 144

يشمل المعهد على إحدى عشر (11) دائرة متخصصة في مجالات مختلفة جميعها تضمن إنجاز الخبرة، التكوين والتعليم بالإضافة إلى تقديم المساعدات التقنية والقيام ببحوث ودراسات وتحاليل في علم الجريمة[1] ، نظرا لاحتوائه على تجهيزات ووسائل تكنولوجية جد متطورة ، بالإضافة إلى بنك المعلومات ومخابر للأدلة الرقمية والخبرة الصوتية للوقاية من جرائم الإعلام الآلي والهاتف المحمول[2] ، ومن بين دوائره نجد دائرة الإعلام الآلي والإلكترونيك المكلفة بتحليل البيانات الرقمية وتقديم المساعدة للمحققين في مجال التحري والتحقيق في الجرائم الإلكترونية.

تتكون دائرة الإعلام الآلي والإلكترونيك من ثلاثة (03) مخابر تتمثل في مخبر الإعلام ، مخبر الفيديو ومخبر الصوت ، وتكلف هذه الدائرة بمهمة رصد ومراقبة وتتبع عمليات الاختراق والقرصنة وكذلك اكتشاف المعلومات المسروقة وتفكيك البرامج المعلوماتية[3].

1-مخبر الإعلام الآلي:

يحتوي مخبر الإعلام الآلي على سبعة (07) قاعات تتمثل في مكتب التوجيه ، فصيلة الأنظمة المشحونة ، فصيلة تحليل المعطيات ، فصيلة الهواتف ، فصيلة اقتناء المعطيات ، قاعة موزع وقاعة تخزين ، وتم تزويده بأحدث التجهيزات والوسائل لإنجاز المهام المخولة له لاكتشاف الجرائم المتعلقة بالمجال المعلوماتي والإلكتروني وهذا بالاعتماد على:

- محطة ثابتة ومحمولة لإجراء خبرات الإعلام الآلي.
- جهاز اقتناء معلومات الهواتف والحواسيب.
- محطة ترميم وتصليح الأجهزة والحوامل المعطلة.
- الحبكات الإعلامية (خبرات الإعلام والتجهيزات البيانية)[4].

من أهم المهام التي تعهد للمخبر تحليل ومعالجة حوامل المعطيات الرقمية (الهاتف ، الشريحة ، القرص الصلب وذاكرة الفلاش) وتحديد التزوير الرقمي للبطاقات البنكية[5] ، وبلا شك فإنه يقوم بتقديم المساعدة

[1] هواري عياش ،المعهد الوطني للأدلة الجنائية وعلم الإجرام، مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية، مداخلة ألقيت في الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، يومي 16و 17 نوفمبر ، 2015 ، ص 03

[2] بهلول مليكة، مرجع سابق، ص 144

[3] بارة سمير، الدفاع الوطني والسياسات الوطنية للأمن السيبرانيcyper security في الجزائر: الدور والتحديات، المجلة الجزائرية للأمن الوطني الإنساني، عدد 20 ، مخبر الأمن الإنساني: الواقع، الرهانات والآفاق، جامعة باتنة 1 ، 2017، ص 436

[4] هواري عياش ، مرجع سابق، ص 06

[5] المرجع نفسه ، ص 06.

للمحققين في المجال التقني عن طريق إصلاح كل تلف في الأجهزة الإلكترونية التي يتم العثور عليها في مسرح الجريمة .

2-مخبر الفيديو:

يضم مخبر الفيديو أربعة (04) قاعات تتمثل في قاعتان للتحليل ، قاعة التخزين وقاعة موزع ، ولكي تباشر هذه القاعات مهامها تتوفر على أحدث الأجهزة من بينها :

- مجموعة أجهزة لقراءة مختلف حوامل الفيديو الرقمية والممغنطة.
- جهاز فيديو بوكس.
- حبكات إعلامية (كونيتك ستوديو ، ماكس ثلاثة أبعاد)
- موزع لحفظ شرائح الفيديو.

من المهام التي تباشرها هذه القاعات إعادة بناء مسرح الجريمة بتشكيل ثلاثي الأبعاد ، بالإضافة إلى تحسين نوعية الصورة (فيديو أو صورة) بمختلف التقنيات ، ومقارنة الأوجه وشرعية الصور والفيديو[1].

3-مخبر الصوت:

يتشكل مخبر الصوت من خمسة (05) قاعات ثلاثة منها تختص في التحليل وقاعة موزع وأخرى للتخزين ، ومن بين التجهيزات التي يتوفر عليها المخبر :

- أجهزة الازدواجية والسماع.
- حبكات إعلامية (معالجة وتحسين التسجيلات الصوتية ، نسخ الأقراص المضغوطة)
- أجهزة التصليح والتغيير.

يكلف المخبر بمهام تدخل في إطار اختصاصه من تحسين نوعية إشارة الصوت بنزع التشويش وتعديل السرعة ، معرفة وتحديد المتكلم وكذلك تحديد شرعية التسجيلات الصوتية[2].

ثانيا: مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية

تم إنشاء مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية سنة 2008 ويعتبر الجهاز الوحيد المختص بهذا الصدد في الجزائر ، يعمل على تأمين منظومة المعلومات لخدمة الأمن العمومي ، وأعتبر بمثابة مركز

[1] هواري عياش، مرجع سابق، ص07

[2] مرجع نفسه ، ص 08

توثيق ، ويتواجد مقره ببئر مراد رايس[1] ، ويتجلى هدف المركز في اكتشاف الجرائم والمخالفات المرتكبة في حق الأفراد والمؤسسات وممتلكاتهم التي تنتشر بواسطة التكنولوجيا الحديثة للإعلام والاتصال عبر الانترنت، ومحاربة كل أنواع الجريمة الإلكترونية[2].

يعهَد لمركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية القيام بمجموعة من المهامالتي تدخل في مجال اختصاصه لمكافحة الجريمة الإلكترونية بصفة عامة بحيث يكلف بما يلي:

- التعاون بشكل وثيق مع الهيئات الأجنبية على مكافحة الجريمة الإلكترونية.
- إجراء التحقيقات بالتعاون والتنسيق بين مخابر المركز والمعهد الوطني للأدلة الجنائية وعلم الإجرام.
- جمع وحفظ الأدلة الرقمية على المستوى المركزي أو على المخابر التقنية.
- البحث عن أسباب حذف وثيقة أو ملف ما أو رسالة معينة وكيفية استخراجها واسترجاعها.
- القيام بإعادة تحليل وتتبع أرشيف الإبحار عبر الانترنت.
- تتبع مسار البريد الإلكتروني وتحديد مصدر الهجمات بالفيروسات أو الاختراق غير القانوني للوثائق الشخصية.
- توفير الأدلة حول سرقة المعطيات والمعلومات وتزوير الوثائق واستعمالها .
- البحث عن أدلة في وثيقة معينة أو رسالة إلكترونية باستخدام برمجيات خاصة ومفاتيح الكلمات[3] .

لقد تمكنت قيادة الدرك الوطني من خلال التكوين المستمر لأفرادها والمشاركة في الملتقيات الوطنية والدولية وتبادل الخبرات مع الدول الأخرى من أن توفر القوى المؤهلة ذات كفاءة عالية من مهندسي الإعلام الآلي ورجال القانون من أجل الفهم الصحيح للجريمة الإلكترونية والتصدي لها[4] ، كما قامت قيادة الدرك الوطني بإطلاق برنامج لوقاية القصر من هذه الجريمة وهذا بفتح مكتب على مستوى المركز لحماية القصر من خلال ترصد كل محاولات الإيقاع بهم عبر الانترنت.

فعلى هذا الأساس تكمن المهمة الأساسية للمركز في محاربة كل أنواع الجريمة الإلكترونية التي تتخذ من الانترنت وسيلة ، فمن القرصنة المعلوماتية إلى الذم والتحقير أو الشتم إلى التهديد أو الابتزاز ، مرورا بالتحرش

[1] بارة سمير، مرجع سابق، ص 335

[2] د. إدريس عطية ، مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها ، مكانة الأمن السيبراني في منظومة الأمن الأوني الجزائري ، مجلة الجيش، العدد 599 ،مؤسسة المنشورات العسكرية، الجزائر ،2013 ، ص ص15-16

[3] د. إدريس عطية ، مرجع سابق، ص ص 12-16

[4] بارة سمير، مرجع سابق، ص ص 345-346

بكل أنواعه وسرقة الهوية وانتحال الشخصية[1] ، وغيرها من الجرائم الإلكترونية الأخرى التي تهدد سلامة المجتمع وأمن الدولة باستعمال شتى الأجهزة الإلكترونية لتنفيذ هذا النوع من الجرائم.

ثالثا: المصلحة المركزية للتحريات الجنائية

تعد المصلحة المركزية للتحريات الجنائية هيئة ذات اختصاص وطني من بين مهامها مكافحة الجريمة الإلكترونية[2] ، وعليه يمكن القول بأنها جهاز تابع لقيادة الدرك الوطني له مهام عديدة في ميدان التحريات الجنائية والمساهمة في إجراء التحقيقات لمكافحة الجرائم بكافة أنواعها ومن بينها الجريمة الإلكترونية بكل أشكالها التي أضحت من جرائم العصر الفتاكة بالمجتمع في العالم الافتراضي.

رابعا: مديرية الأمن العمومي والاستغلال

تعتبر بمثابة هيئة تعمل على التنسيق بين مختلف الوحدات الإقليمية والمركز التقني العلمي في مجال أعمال البحث والتحري في الجرائم الإلكترونية[3] ، وقد بلغ عدد القضايا التي عالجتها قيادة الدرك الوطني لسنة 2018 وهذا بداية من شهر جانفي إلى غاية شهر نوفمبر 1140 قضية متعلقة بالجريمة الإلكترونية منها 136قضية خاصة بالأطفال دون18سنة و 30% من مجموع القضايا تتعلق بالابتزاز والتشهير.

وعلى ضوء ما سبق عرضه حول الأجهزة المكلفة بالوقاية من الجريمة الإلكترونية نجد بأن الجزائر من بين الدول التي سعت جاهدة إلى التصدي لهذه الجريمة بكل أشكالها، من خلال مراقبة كل التحركات التي تتم عبر الانترنت من إبحار وتصفح للمواقع الإلكترونية، والحد منها بمكافحتها وذلك بالاعتماد على مختلف الوسائل والتقنيات الحديثة في مجال المعلوماتية التي تم تسخيرها للكشف عن هذا النوع من الجرائم.

[1] د إدريس عطية ، مرجع سابق، ص13

[2] ربيعي حسين، مرجع سابق، ص 183

[3] نفس المرجع ، ص 183

خلاصة الفصل الثاني :

نستخلص من خلال هذه الدراسة أن الجريمة الإلكترونية متميزة عن باقي الجرائم ليس فقط في تعريفها وخصوصيتها ، بل تعدى الأمر ذلك حتى في إجراءات التحقيق فيها وحجية إثباتها بالنظر إلى صعوبة إثباتها كما سبق التطرق إليه .

ولم يغفل المشرع الجزائري إلى خطورة هذه الجريمة وخطورة مرتكبها ، فبادر بسن مختلف النصوص القانونية التي جاء في أحكامها عقوبات مشددة لمرتكبي الجرائم الإلكترونية بغض النظر عن كون الفاعل شخصا طبيعيا أو معنويا وذلك بهدف تحقيق الردع والحد من هذه الجرائم التي دخلت إلى مجتمعاتنا كفيروس خبيث إنتقلت عدواه إلى بقاع العالم وتفشت فيه وأضحى من الصعب اليوم التخلص منها.

خاتمـــــــــة

الخاتمة :

لقد تعرضنا في مذكرتنا دراسة مكافحة الجريمة الإلكترونية من ناحيتين ، ناحية أولى تناولت الجهود الدولية في إطار تعاون المجتمع الدولي لمكافحة هذه الجريمة بالتعرض لأهم الاتفاقيات الدولية كاتفاقية المجلس الأوروبي وإتفاقية بودابست واتفاقية القانون النموذجي العربي لمكافحة الجريمة المعلوماتية ، ومن ناحية ثانية تناولنا الجهود الوطنية والتجربة الجزائرية في مكافحة هذا النوع من الجرائم وذلك من خلال القوانين العامة كقانون العقوبات وقانون الإجراءات الجزائية أو القوانين الخاصة كقانون التأمينات وقانون البريد وقانون حماية الملكية الفكرية ... إلخ.

إن تحديد أنواع الجرائم المعلوماتية يمكن استخلاصه من الأفعال التي تجرمها الدول أو الاتفاقيات الدولية باعتبارها جرائم معلوماتية أم لا ؟ فلحد الآن هناك جرائم معلوماتية مباحة في بلدان و مجرمة في بلدان أخرى، لذلك تظهر صعوبة تحديد أنواع هذه الجريمة وأقسامها ، غير أن النتيجة المتفق عليها بين غالبية الدول و المنظمات العالمية والاتفاقيات هي أنه توجد تقسيمات متفق عليها وهي تلك الجرائم المعلوماتية التي يكون الحاسب الآلي محلا لها، كجرائم الدخول و البقاء والاستعمال غير المصرح به للحاسب الآلي و جرائم الاعتداءات الواقعة على المعلومات كجرائم النسخ غير المشروع و القرصنة والإتلاف المعلوماتي والغش و التزوير المعلوماتيين.

وجرائم يكون الحاسب الآلي وسيلة أو آداة لارتكابها ، ومثالها جرائم التجسس المعلوماتي والجرائم الخاصة بالمواد الإباحية والمواد الإباحية الطفولية وحتى بعض الجرائم التقليدية المرتكبة بواسطة الحاسب الآلي كالقتل والابتزاز و التهديد .... إلخ.

إن تحديد الطبيعة القانونية للمعلومات كانت محل إشكال بين اتجاهين ، اتجاه تقليدي ينفي عن هذه الأخيرة امكانية الاعتداء عليها كونها شيء معنوي، و أنها تمتلك طبيعة قانونية من نوع خاص و إتجاه حديث يرى أن للمعلومات كيان مادي يمكن الاعتداء عليها كغيره من القيم المالية الأخرى ، و قد ظهر هذا الإشكال بصفة خاصة في جريمة السرقة المعلوماتية ، حيث إختلفت الدول والتشريعات فيما بينها من حيث تطبيق النصوص الخاصة بجريمة السرقة التقليدية في حالة سرقة المعلومات و مدى اعتبارها محلا لهذه الجريمة أم لا لكونها ذات طبيعة معنوية ، وهذا الإشكال قد صعب من عملية مكافحة هذه الجرائم .

إن للجريمة المعلوماتية خصائص منفردة و مميزة عن غيرها من الجرائم التقليدية لذلك وجدت معظم الدول نفسها مضطرة لإيجاد حلول لمواجهتها ، وهذه الحلول كانت بتعديل النصوص التقليدية وتطويرها وتشريع نصوص جديدة حتى لا تترك سلوكات مستهجنة ومجرمة دون عقاب ، وفي نفس الوقت حتى لا تخرج عن مبدأ الشرعية الذي هو مبدأ مكرس عالميا و في كل التشريعات العقابية .

أما من الناحية الإجرائية ، فإنه نظرا لطبيعة الجريمة المعلوماتية الخاصة وكيان بيئتها غير المحسوس تظهر صعوبة مهام السلطات شبه القضائية والسلطات القضائية في أداء دورها للكشف عن الجريمة و البحث عن أدلتها فحتى و إن نجحت الدول نسبيا في تطبيق الأساليب الإجرائية التقليدية كالمعاينة والتفتيش والضبط وإضفاء بعض الخصوصيات والشروط عليها، لتتلاءم وطبيعة الجريمة المعلوماتية، تبقى بعض الصعوبات دائما للكشف عن هذه الجريمة والمتمثلة في قلة الآثار المادية التي تتركها وكثرة الأشخاص الذين يترددون على مسرحها بين فترة ارتكابها و فترة اكتشافها مما يصعب عملية الكشف عنها.

كما انه من خلال هذه الدراسة يستنتج أنه لنجاح المكافحة الإجرائية لابد من تكوين السلطات القضائية المختصة في هذا المجال من الناحية الفنية و العلمية في مجال تكنولوجيات المعلومات و الاتصالات.

كما يستنتج ضرورة إيجاد الوسائل المناسبة للتعاون الدولي لمكافحة هذه الجريمة من الناحية الإجرائية بهدف التوفيق بين التشريعات الخاصة بهذه الجرائم كالتعاون الدولي على تبادل المعلومات و تسليم المجرمين و قبول أي دولة للأدلة المجموعة في دول أخرى.

إن المشرع الجزائري رغم مواكبته للدول السباقة في مكافحة الجريمة المعلوماتية من الناحية الموضوعية والإجرائية إلا أنه لم يتناول الجرائم المعلوماتية بشكل واسع حيث نجده قد أغفل النص على تجريم بعض الجرائم المعلوماتية الحساسة و التي انتشرت بشكل خطير في كل المجتمعات وحتى في المجتمع الجزائري وهي جرائم الاستغلال الجنسي للأطفال وتحريضهم على الدعارة والمخدرات عن طريق الشبكات المعلوماتية.

فالتجريم الوارد بنص المادة 342 من قانون العقوبات الجزائري وما يليها، لا يعد في نظرنا كافيا لتطويق هذا النوع الخطير من الجرائم إذا ما ارتكبت بالحاسبات الالية والشبكات المعلوماتية التي سهلت ومازالت تسهل التدفق الاباحي عبر العلم الافتراضي، والذي بات يهدد كيان الاطفال و الاحداث في كل مكان ومن اي مكان، لذلك كان على المشرع الجزائري تحديد هذه الجرائم والنص على تجريمها باستعمال عبارة "بواسطة الحاسبات أو أي تقنية معلوماتية " وإعتبار إستعمال الحاسب في إرتكابها ظرفا مشددا، و تحديد المسؤولين عن هذه الجرائم بوضع ضوابط قانونية حازمة تحد من انتشارها منعا لاستغلال الاطفال وتعريضهم لتجارب مؤذية، و ذلك عن طريق وضع قواعد للسلوك من قبل مزودي خدمة الانترنيت، و تشجيع انشاء خطوط ساخنة أو خضراء للمواطنين للإبلاغ عن المواقع الاباحية للأطفال عبر الانترنيت، وتدعيم التعاون الدولي في مجال مكافحة جرائم الاستغلال الجنسي للأطفال مثلما هو معمول به في الدول السباقة في مكافحة الجريمة المعلوماتية.

و أخيرا و لنجاح فعالية المكافحة للجريمة الإلكترونية لا يسعنا سوى التنويه والإشارة إلى ضرورة تبني كافة الدول في العالم للفكرة التي مازال أعضاء دول المجلس الأوروبي ينادون و يعملون على نشرها وترسيخها في المجتمع

المعلوماتي ككل، وهي فكرة العمل بالأخلاقيات المعلوماتية La cyber éthique وهذه الفكرة أي فكرة الأخلاقيات موجودة من قبل في كل مجتمع في الشرائع المهنية خاصة كأخلاقيات مهنة الطب و أخلاقيات مهنة المحاماة و الأخلاقيات البيولوجية ....إلخ، والتي هدفها العمل بمجموعة من المبادئ التي حتى ولو لم ترقى إلى مستوى القانون فهي ملزمة لأصحابها، و ذلك بالضمير المهني والأخلاقي للإنسان وعلى هذا ففكرة الأخلاقيات المعلوماتية تقوم على مبدأ معرفة المستعمل للحاسوب ولشبكات المعلوماتية utilisateur للحقوق التي له والواجبات التي عليه في مجال المعلوماتية، وبتكريس هذه الفكرة و العمل بها يؤدي على الأقل إلى التقليل من نتائج و آثار الجريمة المعلوماتية على الأفراد والمجتمعات و يساهم في مكافحتها والقضاء عليه.

وللخروج بنتيجة للبحث ، نقترح مجموعة من الإقتراحات والتوصيات نذكر منها :

– إعداد أنظمة ضبطية وقضائية مؤهلة في التعامل مع الجرائم الإلكترونية ، وتأهيل وتدريب خبراء مختصين في جمع وتحليل وفحص الأدلة الإلكترونية لمساعدة المخططين في بحثهم عن أدلة رقمية تثبت الجرم في القضايا المتعلقة بالجرائم الإلكترونية .

– صياغة بروتوكول أمني موحد يراعي متطلبات أمن المعلومات في مرحلة تصميم شبكات المعلومات كإجراء وقائي قبل وقوع الجريمة .

– تطبيق أنظمة حماية المعلومات ومراجعتها بصفة دورية لتطويرها لما يتناسب مع سرعة التطور التكنولوجي الحاصل.

– إصدار نظام شامل للمعلومات يحدد درجات السرية لما يحقق أعلى درجات الأمن المعلوماتي .

– إيجاد آلية للتنسيق بين القانونيين ومهندسي وتقني الحاسوب والشبكات للحد من عمليات القرصنة الإلكترونية أو الحد منها وإكتشافها إذا وقعت .

– إن محاربة الجريمة الإلكترونية على المستوى الدولي أو الوطني لا تتم إلا بإيجاد أساس تشريعي موحد وتصور شامل لمفهوم هذا النوع من الجرائم من أجل تحديد الأفعال التي تشكل هذه الجرائم ، إضافة إلى عقد إتفاقيات بين الدول يكون هدفها التنسيق وتوحيد الجهود لمكافحة هذه الجرائم ، وتشكيل لجان مختصة في البحث والتحري والتحقيق يكون أعضاؤها من ذوي الكفاءات في المجال المعلوماتي .

– زيادة التعاون الدولي لمواجهة الجرائم الإلكترونية عن طريق الإتفاقيات والمعاهدات الدولية سواءا الثنائية أو الجماعية متعددة الأطر .

– سد الفراغ التشريعي في مجال مكافحة الجريمة الإلكترونية ، على أن يكون شاملا للقواعد الموضوعية والإجرائية ، وعلى وجه الخصوص النص صراحة على الدخول غير المشروع للحاسب الآلي وشبكات الإتصال والبريد

الإلكتروني وكذلك إعتبار البرامج والمعلومات من الأمور ذات القيمة أي تحديد الطبيعة القانونية للأنشطة الإجرامية التي تمارس على الحاسوب والأنترنيت ، وايضا الإعتراف بحجية الأدلة الرقمية وإعطاؤها حكم المحررات التي يقبل بها القانون كدليل إثبات .

– منح سلطات الضبط والتحقيق الحق في إجراء تفتيش وضبط أي تقنية خاصة بالجريمة الإلكترونية تفيد في إثباتها ، على أن تمتد هذه الإجراءات إلى أية نظم حاسب آلي آخر له صلة بمحل الجريمة .

– نشر الوعي بين المواطنين خاصة الشباب بمخاطر التعامل مع المواقع السيئة والمشبوهة على الشبكات الإلكترونية ، وذلك بتفعيل دور المجتمع المدني والمؤسسات للقيام بدوره التوعوي والوقائي من الوقوع في براثن الرذيلة والممارسات الخاطئة .

قائمة المراجع والمصادر

قائمة المصادر والمراجع

أولا : القوانين

1/ القانون 04-15 المؤرخ في 2015/02/01 المتضمن تعديل قانون العقوبات ، الجريدة الرسمية رقم 06 الصادر بتاريخ 2015/02/01 .

2/ الأمر رقم 03-06 المؤرخ في 19 جويلية 2003 المتعلق بالعلامات التجارية ، ج ر عدد 44 صادر في 23 جويلية 2003.

3/ الأمر رقم 03-07المؤرخ في 2003/07/19 المتعلق ببراءات الاختراع ،ج ر عدد 44 صادر في 23 جويلية 2003 .

4/ أمر رقم 97-10 مؤرخ في 06-03-1997المتعلق بحق المؤلف والحقوق المجاورة ، الجريدة الرسمية عدد 13 الصادر في 1997/03/12 معدّل ومتم بأمر 05-03 مؤرخ في 2003/07/19 المتعلق بحقوق المؤلف ، والحقوق المجاورة ، الجريدة الرسمية عدد 44 الصادر في 2003/07/23 .

5/ القانون رقم 2000-03 المؤرخ في 2000/08/05 والذي يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية ، الجريدة الرسمية رقم 48 بتاريخ 2000/08/05 .

6/ القانون رقم 2000-03 المؤرخ في 2000/08/05 والذي يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية ، الجريدة الرسمية رقم 48 بتاريخ 2000/08/05 .

7/ قانون رقم 01-08 المؤرخ في 2008/01/23 والمتم لقانون رقم : 83-01 متعلق بالتأمينات.

8/ القانون 09-04 مؤرخ في 14شعبان 1430 الموافق 2009/08/05 للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها.

9/ المرسوم الرئاسي رقم 15-261المؤرخ في 08 أكتوبر 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة تكنولوجيات الإعلام والاتصال ومكافحتها.

ثانيا : الكتب

01- إدريس عطية ، مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها ، مكانة الأمن السيبراني في منظومة الأمن الأوني الجزائري ، مجلة الجيش، العدد 599 ،مؤسسة المنشورات العسكرية، الجزائر 2013،

02- أحسن بوسقيعة ، الوجيز في القانون الجزئي، الطبعة السادسة ، دار هومة ، الجزائر، 2007 .

03- أمير فرج يوسف ، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت ، مكتبة الوفاء القانونية ، الإسكندرية، مصر ، 2011 .

04- أمير فرج يوسف، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت، مكتبة الوفاء القانونية، الإسكندرية، مصر،2011 .

05- جعفر جاسم الطائي، جرائم تكنولوجيات المعلومات _ رؤية جديدة للجريمة الحديثة_، الطبعة الأولى، دار البداية ناشرون موزعون، عمان، الأردن، ،2007 .

06- جميل عبد الباقي الصغير ، المواجهة الجنائية لقرصنة البرامج التلفزيونية المدفوعة ، دار النهضة العربية ، القاهرة ،2001.

07- حسف جميعي ، مدخل إلى حق المؤلف و الحقوق المجاورة ، حمقة عمل الويبو التمهيدية ، المنظمة العالمية للمكية الفكرية ، القاهرة ، 2004 .

08- خالد ممدوح إبراهيم، الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر ،2009 .

09- ختير مسعود، الحماية الجنائية لبرامج الكمبيوتر، أساليب وثغرات ، دار الهدى للنشر والتوزيع، الجزائر ، طبعة ، 2010 .

10- زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى للطباعة والنشر، الجزائر، 2011 .

11- زبيخة زيدان ، الجريمة المعلوماتية في التشريع الجزائري و الدولي ، دار الهدى ، عين مليلة ، الجزائر ،2011 .

12- صورية بوربابة ، مجلة "القانون الدولي للدراسات البحثية" بعنوان : التعاون الدولي في مكافحة الجرائم المعلوماتية.

13- طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، الإسكندرية ، 2009.

14- عادل عبد العال إبراهيم خراشي ، اشكالية التعاون الدولي في مكافحة الجرائم الالكترونية وسبل التغلب عليها،، كلية الشريعة والقانون ، القاهرة .

15- عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، مصر، 2002.

16- عبد الله سيف الكيتوب ، الاحكام الاجرائية لجريمة الاحتيال المعلوماتي ، دار النهضة العربية ، القاهرة ، 2013.

17- عبد الله عبد الكريم عبد الله ، جرائم الكمبيوتر والمعلوماتية ، الجرائم الإلكترونية دراسة مقارنة في النظام

القانوني لمكافحة جرائم المعلوماتية والانترنت مع الإشارة إلى جهود مكافحتها محليا ودوليا ، منشورات الحلبي الحقوقية، بيروت، لبنان، 2007.

18- علي جبار الحسناوي ، جرائم الحاسوب و الانترنت ، دار اليازوري ، الاردن ، 2009.

19- عماد الدين محمود سويدات ، الحماية المدنية للعلامات التجارية، الطبعة الأولى، دار الحامد للنشر والتوزيع، الأردن، 2012.

20- فاتن حسين حوى ، المواقع الإلكترونية وحقوق الملكية الفكرية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن ، 2010.

21- محمد عد الله أبو بكر سلامة ، موسوعة جرائم المعلوماتية "جرائم الكمبيوتر والانترنت" ، المكتب العربي الحديث ، الإسكندرية ، 2014 .

22- محمد محمد عنب، استخدام التكنولوجيا الحديثة في الإثبات الجنائي، مطبعة السلام الحديثة، د.ب.ن، 2007، .

23- محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، الأردن 2005، .

24- محمود فياض ، المعاصر في قوانين التجارة الدولية، د ط، مؤسسة الوراق للنشر والتوزيع، الأردن ، 2012.

25- منير محمد الجهيني، ممدوح محمد الجهيني، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر العربي، الإسكندرية، ط ،2004 .

26- هروال نبيلة هبة، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الإسكندرية مصر ، 2006 .

27- يتوجي سامية ، معاهدة الويبو بشأن حق المؤلف ، مذكرة تخرج لنيل شهادة الماستر ، جامعة محمد خيضر ، بسكرة ، الجزائر ، 2008-2009 .

30-Férale-Schuhl Christiane , CyberDroit le droit à l'épreuve de l'internet , 5em édition , Dalloz , Paris, 2009/ 2010

ثالثا : المذكرات والرسائل

01- اسامة مهمل ، الاجرام السيبيراني ، مذكرة لنيل شهادة الماستر ، جامعة محمد بوضياف ، المسيلة ، 2017-2018.

02- بدري فيصل، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة لنيل شهادة دكتوراه

علوم، تخصص: قانون عام، كلية الحقوق، جامعة الجزائر2018 .
03- براهيمي جمال ، التحقيق الجنائي في الجرائم الإلكترونية ، أطروحة لنيل شهادة الدكتوراه في العلوم ، تخصص: القانون ، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو، 2018 .
04- بهلول مليكة ، دور الشرطة العلمية والتقنية في الكشف عن الجريمة ، أطروحة لنيل شهادة الدكتوراه علوم، فرع: الحقوق ، كلية الحقوق ، جامعة الجزائر ،2013 .
05- دردور نسيم ، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن ، مذكرة لنيل شهادة الماجستير شعبة القانون الجنائي ، جامعة منتوري قسنطينة ، 2012-2013 .
06- ربيعي حسين ، آليات البحث والتحقيق في الجرائم المعلوماتية ، أطروحة لنيل شهادة الدكتوراه في الحقوق ، فرع: قانون العقوبات والعلوم الجنائية ، كلية الحقوق والعلوم السياسية ، جامعة باتنة ،2016 .
07- سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة الماجستير، في العلوم القانونية، تخصص: علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة ، 2013 .
08- قارة أمال، الجريمة المعلوماتية، رسالة لنيل درجة الماجستير في القانون الجنائي والعلوم الجنائية، جامعة الجزائر، كلية الحقوق، الجزائر، 2002 .
09- عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية، دراسة مقارنة، رسالة مكملة للحصول على درجة الماجستير في القاون العام ، جامعة الشرق الأوسط، 2014
10- محمد أحمد سليمان عيسى، "التعاون الدولي لمواجهة الجرائم الإلكترونية،" المجلة الأكاديمية للبحث القانوني، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرة، بجاية ،2016 .
11- مرزوق نسيمة ، جرائم الانترنيت، مذكرة تخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر، 2009-2006 .
12- معتق عبد اللطيف ، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن ، مذكرة ماجستير ، جامعة الحاج لخضر باتنة ، 2015-2016 .

رابعا : المقالات والمحاضرات

01- بارة سمير، الدفاع الوطني والسياسات الوطنية للأمن السيبراني security cyperفي الجزائر: الدور والتحديات، المجلة الجزائرية للأمن الوطني الإنساني، عدد 20 ، مخبر الأمن الإنساني: الواقع، الرهانات والآفاق، جامعة باتنة 1 ، 2017 .
02- بن دعاس فيصل، إجراءات التحري في الجرائم المعلوماتية، محاضرة في إطار التكوين المحلي المستمر للقضاة، مجلس قضاء قسنطينة.
03- حابت أمال، "الطابع الخصوصي للإجراءات الجزائية في شأن الجرائم الإلكترونية في القانون الجزائري،"

مداخلة ألقيت في الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، يومي 16و 17نوفمبر 2015 .

04- حملاوي عبد الرحمان، دور المديرية العامة للأمن الوطني في مكافحة الجرائم الإلكترونية ، مداخلة ألقيت في الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة ، كلية الحقوق والعلوم السياسية ، جامعة محمد خيضر، بسكرة ، يومي 17-16 نوفمبر ، 2015 .

05- خالدي خديجة، "آلية الإتحاد الإفريقي للتعاون الشرطي أفريبول،" مجلة العلوم الاجتماعية والإنسانية، ع 01،جامعة العربي تبسي، تبسة ، 2018 .

06- خلدون عيشة ، محاضرات في الجريمة المعلوماتية ، ملقات على طلبة سنة أولى ماستر قانون جنائي ، كلية الحقوق جامعة الجلفة ، 2021-2022.

خامسا : المواقع الإلكترونية

1/الموقع الرسمي لمديرية الأمن الوطني ، www.dgsn.dz

2/https://www.wipo.int/edocs/pubdocs/ar/intproperty/442/wipo_pub_442.pdf

فهـــرس المحتويـــات

فـهـرس الـمحتويـات

الملخص باللغة العربية :

إن تطور وسائل الإعلام والاتصال ، والاعتماد المتزايد عليها أدى إلى ظهور العديد من الجرائم الإلكترونية التي تأثرت كغيرها من الجرائم بهذا التطور ، حيث أصبحت من بين التحدّيات التي تواجهنا يوميا خصوصا في الآونة الأخيرة ، الأمر الذي إستلزم على الأجهزة الأمنية إستحداث وحدات خاصة لرصد كل التحركات المشبوهة في هذا المجال وفرض قوانين تعاقب على كل فعل يشكل جريمة إلكترونية .

كما أنّ للجهود الدولية دور فعال في دعم سبل مكافحة الجرائم الإلكترونية ، ونظرا للطبيعة التي تتسم بها هذه الجرائم ، فإنها تواجه عدة صعوبات تؤثر خاصة على عملية التحري والتحقيق لجمع الأدلة الإلكترونية بالطرق التقليدية ، مما إستوجب على المشرع الجزائري القيام بإستحداث قواعد خاصة ملائمة لهذه الطبيعة ، وقبول الدليل الإلكتروني مثل قبول أيّ دليل جنائي آخر ، وللقاضي الجنائي السلطة التقديرية في الأخذ به أو استبعاده ، أو رفضه .

Le résumé en langue française :

L’évolution des moyens d'information et de communication, et la dépendance croissante sur aux a provoqué l'apparition beaucoup de cybercriminalités qu'ont été affectée comme les autres crimes par ce progresse, où sont devenant parmi les défis qu’il nous rencontre quotidiennement surtout ces derniers temps, ce qui obligé les services de sécurité a crée des unités spéciales pour moniteur tous les mouvementes suspectes dans ce domaine et imposer des lois punir sur les actes constituant un crime électronique.

Ainsi que les efforts internationaux a un rôle actif a soutenir les moyens de lutter contre la cybercriminalité, et compte tenu de la nature qui caractérisé a ces crimes. Elle rencontre plusieurs difficultés qu'il affecté surtout l'opération d'enquête pour collecter les preuve électronique par les méthodes traditionnel, ce qui nécessité au législateur algérien à crée les règles spéciales convenable à cette nature. Et l'acceptation de preuve électronique est comme l'acceptation toutes autres preuves criminel, et le juge pénal a le pouvoir discrétionnaire de prendre le, de l’exclure ou de le rejeter.