جـــامعـــة علي لونيسي البليدة2
مخبر الجريمة والانحراف بين الثقافة والتمثلات الاجتماعية
مجلة سوسيولوجيا الجريمة
للبحوث والدراسات العلمية في الظواهر الاجرامية
رقم الإيداع القانوني ر د م د: 2716-7976

# الإطار المفاهيمي والقانوني لمواجهة الجرائم السيبرانية

## Conceptual and legal framework for confronting cyber crimes

فاطمة خرشف

korchofdoctora@gmail.com

لزار سميرة

Lazare.samira2020@gmail.com

**ملخص**

باتت الحاجة الى مساحات الكترونية آمنة و فعالة أكثر إلحاحا من أي وقت مضى ، نتيجتا لما سببته الهجمات السيبرانية من تهديد للسلم و الأمن الدوليين ،ان سهولة ارتكاب هذه الجرائم نتيجة تطور وسائط تكنولوجيا المعلومات ،و صعوبة اثباتها ،ادى بالدول الى سن قوانين وقائية و أخرى ردعية لمكافحة الجرائم السيبرانية ،حيث شددت العقوبة من خلالها على المجرمين و حملتهم مسؤولية سلوكهم.

**الكلمات المفتاحية** :جريمة ،سيبرانية ،عقوبة ،امن دولي ،مسؤولية.

**Summary**

The need for safe and effective electronic spaces has become more urgent than ever, as a result of the threat caused by cyber attacks to international peace and security. The ease of committing these crimes as a result of the development of information technology media, and the difficulty of proving them, led countries to enact preventive and other laws A deterrent to combat cybercrime, whereby the punishment has been tightened on criminals and held responsible for their behavior.

Keywords: crime, cyber, punishment, international security, responsibility.

جـــامعـــة علي لونيسي البليدة2
مخبر الجريمة والانحراف بين الثقافة والتمثلات الاجتماعية
مجلة سوسيولوجيا الجريمة
للبحوث والدراسات العلمية في الظواهر الاجرامية
رقم الإيداع القانوني ر د م د: 2716-7976

**مقدمة**

في أواخر 1990، اشارت الاحصاءات الى ان الحركة على شبكة الانترنت العامة تتضاعف كل عام ،و يعود ذلك الى النمو المتزايد لعدد مستخدمي الشبكة و لعدم وجود ادارة مركزية تتحكم باستخدام الشبكة ، الامر الذي يسمح بالتوسع الطبيعي لاستخدامها من دون قيود او موانع فأي استخدام جديد يستطيع الانضمام الى الشبكة من دون قيود تذكر ،و قد قدر عدد مستخدمي الانترنت بحوالي المليارين عام 2001.

أصبحنا في عصر انتشار تكنولوجيا المعلومات أكثر عرضة للوقوع كضحايا للجرائم الالكترونية ، حيث يعتبر الانتشار السريع لوسائط الاتصال الحديثة سلاح ذو حدين ، يمكن استخدامه من أجل تسهيل و تسريع الاتصالات حول العالم و تبادل المعلومات و انتشار المعرفة ،كما قربت المسافات بين الدول و الاشخاص ،وقللت من الجهد و المال و قلصت الزمن خلال هذه الوسائط الجديدة ومن ضمنها خدمات الاعلام الالي و شبكة الانترنت ،كما يمكن ان يتم استخدامها من جهة اخرى في افعال تم تسميتها بالجرائم السبيرانية، أو الالكترونية او المعلوماتية.

فالجريمة الإلكترونية هي فعل يتسبب بضرر جسيم للأفراد أو الجماعات والمؤسسات و الدول، بهدف ابتزاز الضحية وتشويه سمعتها من أجل تحقيق مكاسب مادية أو خدمة أهداف سياسية باستخدام الحاسوب ووسائل الاتصال الحديثة مثل الإنترنت و تطبيقاتها. تكون الجرائم المعلوماتية بهدف سرقة معلومات واستخدامها من أجل التسبب بأذى نفسي ومادي جسيم للضحية، أو إفشاء أسرار أمنية هامة تخص مؤسسات هامة بالدولة أو بيانات وحسابات خاصة بالبنوك والأشخاص، تتشابه الجريمة الإلكترونية مع الجريمة العادية في عناصرها من حيث وجود الجاني والضحية وفعل الجريمة، ولكن تختلف عن الجريمة العادية باختلاف البيئات والوسائل المستخدمة، فالجريمة الإلكترونية يمكن أن تتم دون وجود الشخص مرتكب الجريمة في مكان الحدث، كما أن الوسيلة المستخدمة هي التكنولوجيا الحديثة ووسائل الاتصال الحديثة والشبكات المعلوماتية.

التأثير الأساسي للجرائم الإلكترونية هو التأثير المالي ؛ يمكن أن تشمل الجرائم الإلكترونية أنواعًا مختلفة من الأنشطة الإجرامية التي يحركها الربح ، بما في ذلك هجمات برامج الفدية والاحتيال عبر البريد الإلكتروني والإنترنت والاحتيال في الهوية ، فضلاً عن محاولات سرقة الحساب المالي أو بطاقة الائتمان أو معلومات بطاقة الدفع الأخرى. قد يستهدف مجرمو الإنترنت أيضًا المعلومات الشخصية للفرد ، بالإضافة إلى بيانات الشركة الخاصة بالسرقة وإعادة

البيع. نظرًا لأن العديد من العمال يستقرون في إجراءات العمل عن بُعد بسبب الوباء (كوفيد 19)، فمن المتوقع أن تزداد جرائم الإنترنت وتكرارها في الاعوام القادمة ، مما يجعل حماية البيانات الاحتياطية مهمة بشكل خاص.

لدراسة هذا البحث قمنا بصياغة الاشكالية التالية :

**ماهي الجرائم السيبرانية ؟ و ماهي الاليات التشريعية المرصدة لمكافحتها في الجزائر ؟**

## 1.مفهوم الجريمة السيبرانية

### 1.1 تعريف الجريمة الإلكترونية

1.1.1تُعرِّف اتفاقية مجلس أوروبا بشأن الجرائم الإلكترونية ، التي وقعت عليها الولايات المتحدة ، الجريمة الإلكترونية على أنها مجموعة واسعة من الأنشطة الضارة ، بما في ذلك الاعتراض غير القانوني للبيانات ، وتداخلات النظام التي تعرض سلامة الشبكة وتوافرها ، وانتهاكات حقوق النشر.) بواسطة (kut brush)

–هي "نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه".

– و يعرفها مكتب تقييم التقنية في الولايات المتحدة الأمريكية بأنها: "الجريمة التي تلعب فيها البيانات الحاسوبية و البرامج المعلوماتية دورا رئيسيا".

– كما عرفتها منظمة التعاون الاقتصادي والتنمية "OECD" بأنها:"كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية". ((Organisations Economique de commerce et développement

كما يمكن تعريفها بأنها استخدام الأجهزة التقنية الحديثة مثل الحاسب الآلي و الهاتف النقال ، أو احد ملحقاتها أو برامجها في تنفيذ أغراض مشبوهة و أمور غير أخلاقية لا يرتضيها المجتمع.(زيدان زليخة،2011،ص42)

### 2.1.1تعريف وزارة العدل الأمريكية للجريمة الالكترونية

الجريمة الإلكترونية هي أي نشاط إجرامي يشمل جهاز كمبيوتر أو جهاز متصل بشبكة أو شبكة. بينما يتم تنفيذ معظم الجرائم الإلكترونية من أجل تحقيق ربح لمجرمي الإنترنت ، يتم تنفيذ بعض الجرائم الإلكترونية ضد أجهزة الكمبيوتر أو الأجهزة مباشرة لإتلافها أو تعطيلها ، بينما يستخدم البعض الآخر أجهزة الكمبيوتر أو الشبكات لنشر برامج ضارة أو معلومات غير قانونية أو صور أو مواد أخرى. تقوم بعض الجرائم الإلكترونية بالأمرين معًا –

على سبيل المثال ، استهداف أجهزة الكمبيوتر لإصابتها بفيروس كمبيوتر ، والذ ينتشر بعد ذلك إلى أجهزة أخرى ، وأحيانًا إلى شبكات كاملة.

### 3.1.1 تعريف الجريمة كظاهرة اجتماعية

يقصد بالجريمة كظاهرة اجتماعية بأنها كل فعل يتنافى مع القيم السائدة في المجتمع و هي خطيئة اجتماعية تعارض قيم و اخلاق المجتمع ،و الجريمة هي كل فعل او امتناع يصدر عن إرادة مدركة تخرق أمن و مصالح و حقوق الأفراد و المجتمع و يعاقب مرتكبها بعقوبة او بتدابير احترازية ،و تكون الجريمة قانونية إذا وقعت بالمخالفة لقواعد القانون .(نجم محمد صبحي ،2006 ،ص17)

### 4.1.1 تعريف النظام المعلوماتي

عرفت معاهدة بودابست( THE BUDABEST CONVENTION ON CYBER CRIME ) النظام المعلوماتي في المادة الأولى الفقرة أ بأنه جهاز مكون من SOFTWARE و HARDWARE تم تطويره لتحقيق المعالجة الآلية للبيانات فهو يعني وجود مجموعة من التعليمات التي يمكن أن تنفذ بواسطة كمبيوتر توصلا إلى نتائج محددة.(شحادة زينات طلعت ،ص 29)

### 2.1تعريف الجريمة السيبرانية

الجريمة السيبرانية هي فعل أو امتناع عدي ينشأ عن الاستخدام غير المشروع لتقنية المعلومات ،يهدف الى الاعتداء على الأموال المادية و المعنوية أو الاعتداء على خصوصية الأفراد ،أو هي عمل او امتناع يأتيه الانسان إضرارا بمكونات الحاسب او شبكات الاتصال الخاصة به ،من جهة أخرى هي الجريمة التي يكون النظام المعلوماتي فيها وسيلة لارتكاب جريمة تقليدية. إما ضد الأموال كالتحويل الالكتروني غير المشروع للأموال ،او ضد الأشخاص كجريمة السب أو القذف عبر الانترنت.(نبيل دريس ،الجريمة السيبرانية بين المفهوم و التشريع في الجزائر.

إن مصطلح الجرائم السيبرانية هو إحدى المصطلحات الحديثة والمستخدمة عن جرائم الإنترنت الذي تعددت مصطلحاته وذلك لنشأة وتطور ظاهرة الإجرام المرتبط والمتصل بتقنية المعلومات . وفي الحقيقة لو تأملنا نجد بأن مصطلح الجرائم السيبر انية ) crime cyber ) هو مصطلح غير عربي ، لكنه هو المتداول والمستخدم حديثا في وقتنا الحالي في هيئة الاتصالات وتقنية المعلومات وكذلك في المؤتمرات والندوات ) كملتقى الجرائم السيبرانية والأدلة

الرقمية ( الذي نظمته جامعة الأمير نايف العربية للعلوم الأمنية في مدينة الرياض عام 2112 م . وكذلك نجد كلمة سيبراني )cyber( قد ارتبط بالأمن الإلكتروني فأصبحنا نعتمد مصطلح الأمن السيبراني.

### 1.2.1 تعريف السيبرانية في اللغة :

السيبيرانية كلمة انجليزية مشتقة من كلمة (cyber) و تعني مرتبط بالحاسوب او شبكات الحاسوب ،و قيل تعني فضاء الانترنت ،و قيل كلمة يونانية مشتقة من كلمة (kybernetes) و تعني الشخص الذي يدير دفة السفينة ،مجازا للمتحكم.

### 2.2.1 تعريف قانون السيبرانية

عرف قانون السيبيرانية بأنه "مجموعة القواعد و الاحكام الواردة في شتى فروع القانون ،و التي يمكن تطبيقها على مسألة معلوماتية بحس بنوع المشكلة المثارة ،و التي قد تخضع لأحكام قانونية متعددة 1 تثير فكرة المعلوماتية قلقا بالغا إذا استخدمت أنظمة المعلومات في انتهاك حقوق الأفراد و حرياتهم العامة (العلجوني احمد خالد ،2002،ص9.)

### 3.2.1 تعريف النظام السيبراني

نعني بالنظام المعلوماتي كل مكونات الحاسب الالي الماديةHardWare و المعنوية Software و شبكات الاتصال الخاصة به NetWorrks ،او هي مجموعة عناصر مادية و غير مادية يمكن باجتماعها العمل الفوري مع المعلومة .( أبو الغيط رشا مصطفى ،2003،ص5)

### 4.2.1 عناصر النظام السيبراني

يقوم النظام السيبراني على عنصرين أحدهما مادي و الأخر معنوي .

- العنصر المادي (HardWare) يتمثل في جهاز الحاسب الآلي بالإضافة الى مجموعة من ملحقاته و الوسائط التي توصل به كي يتلقى من خلالها المعطيات و المعلومات ،و الحاسب الآلي عبارة عن آلة يمكن برمجتها لتقبل بيانات (مدخلات ) وتجري تشغيلا عليها لتحواها الى معلومات مفيدة (مخرجات) و تخزينها والاحتفاظ بها لاستخدامها في المستقبل 1 .تتكون هذه الآلة من عدة وحدات منها ،وحدات الادخال ،و حدات الإخراج ،وحدة المعالجة المركزية ،و وحدات التخزين .

-العنصر المعنوي (Software) و هو ما يعرف بالكيان المنطقي للنظام المعلوماتي ،و الذي يشمل جميع العناصر غير المادية اللازمة لتشغيل الكيان المادي ،عرفه المنشور الفرنسي الصادر في 22 نوفمبر 1981 بأنه مجموعة البرامج و الأساليب و القواعد ،و عند الاقتضاء الوثائق المتعلقة بتشغيل وحدة معالجة البيانات .تقوم برامج الحاسب software بأداء ثلاث وظائف أساسية هي تشغيل النظام ،و تنفيذ البرامج الجاهزة ،و كتابة برامج جديدة بلغة الحاسب.(مكاوي حسن عماد ،1997،ص75).

يختلف الكيان المنطقي عن البرنامج ،فالكيان المنطقي مصطلح اعم و اشمل من البرنامج ،حيث يضم بالإضافة الى البرنامج وصف البرنامج و المستندات الملحقة بالبرنامج و هكذا فإن البرنامج في مفهومه الواسع يضم الى جانب التعليمات و الأوامر التعليمات الموجهة الى العميل ،مثل بيانات استعمال البرنامج و كيفية المعالجة الالكترونية للمعلومات .(دريس نبيل ، السيبرانية بين المفاهيم و التشريعات الوطنية 27)

تعتبر المعلومات بما لها من اهمية سواء بطبيعتها او لترجمتها الى اموال الهدف الرئيسي لمرتكبي الجرائم يمكن تصنيف فيئات المجني عليهم من مرتكبي الجرائم الى الفئات التالية : المؤسسات المالية و القطاعات الحكومية ،المؤسسات العسكرية،الاشخاص الطبيعية .

تعتبر المؤسسات المالية كالبنوك و الشركات المالية من اكثر الاماكن المستهدفة من قبل مرتكبي جرائم السرقة و النصب و الاحتيال .(ايمن عبد الحفيظ ،2005،ص39)

المؤسسات العسكرية :

لم تقتصر حدود ثورة المعلومات على القطاع المدني بل كان لها اكبر اهمية في تطوير انظمة الحرب الحديثة و ادت الى ظهور ما يسمى بحرب المعلومات، حيث أصبحت الدولة التي تمتلك المعلومات هي الدولة الأقوى ،و لذلك بدأ الاهتمام ينصب على الجاسوسية العسكرية ،و أصبح اطلاق الاقمار الصناعية من الجهات العسكرية هو المحور الذي يقوم عليه الاتجاه في تطوير الاجهزة و المعدات العسكرية مما استتبع ظهور حروب جديدة تسمى حروب المعلومات بين الدول .

و اصبحت المعلومات هي السلاح الرئيسي في هذه الحرب، و بالتالي أدى ذلك الى تطوير في صياغة التنظيمات الهجومية و الدفاعية لحرب المعلومات مما يجعل منظومة القوات المسلحة في الحروب المستقبلية تخوذ حروب

معلوماتية تعتمد على شبكات الحاسبات الآلية في نقل المعلومات عن طريق الشبكات من خلال الاقمار الصناعية .(ايمن هبد الحفيظ، ص42)

### 3.1 خصائص الجريمة السيبرانية

إن الجريمة السيبرانية تتميز بعدة خصائص منها:

- جرائم ترتكب بواسطة الأجهزة الإلكترونية كالحاسب الالي والهواتف الخلوية : وهما الأداتان التي تمكن المجرم من دخول الإنترنت لتنفيذ جريمته .
- جرائم خفية : فليس من السهولة اكتشافها لضعف القدرة الفنية للضحية وذلك مقارنة بالمجرم ، ولربما أيضا لمهارات المجرم الفنية والعلمية المتقدمة لقدرته على إخفائها ، أو لخوف الضحية من الإبلاغ عن الجريمة تجنبا للإساءة إلى السمعة .(القرعان محمود أحمد ، ص 31.)
- جرائم سريعة التنفيذ : فسرعة ارتكاب الجريمة قد تكون خلال جزء من الثانية ، وقد لا تتطلب الإعداد قبل التنفيذ .
- جرائم عن بعد : (القرعان ،ص31) فيمكن للجاني تنفيذ جريمته وهو في دولة بعيدة كل البعد عن المجني عليه .
- جرائم عابرة للحدود : فهي لا تعرف الحدود الجغرافية للدول ، الارتباط العالم بشبكة واحدة ، وهذا قد يسبب إشكاليات لدى الاختصاص القضائي من حيث التحقيق والمحاكمة ، وذلك تبعا لتعقيد الإجراءات التي تحكمها الاتفاقيات والمعاهدات والعالقات الدولية ، والتنازع فيما بينهما على أي القانون الواجب التطبيق .

– جرائم صعبة الإثبات : وتكمن صعوبة إثباتها إلى أن متابعتها واكتشافها عن طريق الصدفة ، ومن الصعوبة حصرها في مكان معين ، حيث أنها ال تترك أثرا واضحا للعيان ، أو تشاهد بالعين المجردة ، فما هي الا أرقام تدور في السجلات والمواقع الإلكترونية ، كما أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف عنها ، وتعود الصعوبة لعدة أسباب (بنت عطية روان،2020):

– إنها كجريمة لا تترك أثرا بعد ارتكابها .

– صعوبة الاحتفاظ الفني بآثارها إن وجدت .

- تحتاج لخبرة فنية يصعب على المحقق التقليدي التعامل معها .
- تعتمد على الخداع في ارتكابها ، والتضبيب في التعريف على مرتكبيها .
- تعتمد على مستوى من الذكاء المرتفع في ارتكابها " ( محمود أحمد القرعان ، مرجع سابق ،ص4)

### 4.1 اقسام الجريمة السيبرانية

قسم دليل إرشادات الاسكوا للتشريعات السيبرانية الجرائم السيبرانية الى اقسام سمتها رئيسية و هي اثنا عشر جريمة و هي:

- جرائم التعدي على البيانات المعلوماتية :شملت الجرائم التي يكون موضوعها البيانات للمعلوماتية أي التي يتم من خلالها التعرض للبيانات المعلوماتية و جرم اعتراض المعلوماتية (الباب الأول من تشرع الاسكوا).
- جرائم التعدي على الأنظمة المعلوماتية :و تتناول جرائم الولوج غير المشروع الى نظام معلوماتي او المكوث فيه مع التعرض للبيانات المعلوماتية و جرائم إعاقة عمل نظام معلوماتي.(اباب الثاني من نفس المرجع)
- إساءة استعمال الأجهزة او البرامج المعلوماتية :تتناول كذلك هذه الجرائم جرائم كل من قدم او انتج او زرع او حاز بغرض الاستخدام جهازا او برنامجا معلوماتيا او اية بيانات معلوماتية معدة او كلمات سر ،و ذلك بغرض اختراق أي من الجرائم المنصوص عليها سابقا .(نفس المرجع ،الباب الثالث )
- جرائم الأموال : تشمل جرائم الاحتيال و الغش بوسيلة معلوماتية و جرم التزوير المعلوماتي و جرم الاختلاس او سرقة أموال بوسيلة معلوماتية ،و جرم اعمال التسويق و الترويج غير المرغوب فيها و جرم الاستيلاء على أدوات التعريف و الهوية المستخدمة في نظام المعلومات و الاستخدام غير المشروع لها و جرم الاطلاع على معلومات سرية او حساسة او افشائها.( الباب الرابع )
- جرائم الاستغلال الجنسي للقاصرين : هي الأفعال التي تتعلق باستغلال الأطفال القصر في اعمال جنسية ،و تتشمل الرسوم او الصور أو الكتابات او الأفلام او الارشادات او اية اعمال اباحية يشارك فيها القصر ، او تتعلق باستغلال القاصرين في المواد الإباحية و تشمل أيضا انتاج مواد اباحية للقاصرين بقصد بثها بواسطة نظام معلوماتي.( الباب الخامس)
- جرائم التعدي على الملكية الفكرية للأعمال الرقمية : و تشمل الجرائم التالية :جرم وضع اسم مختلس على عمل و جرم تقليد امضاء المؤلف او ختمه ،جرم تقليد عمل رقمي او قرصنة البرمجيات ،جرم بيع أو عرض

عمل مقلد او وضعه في التداول ،و جرم الاعتداء على أي حق من حقوق المؤلف او الحقوق المجاورة .( الباب السادس)

- جرائم البطاقات المصرفية و النقود الالكترونية :تشمل أعمال تقليد بطاقة مصرفية عن قصد بصورة غير مشروعة و استعمالها عن قصد و تزوير نقود الكترونية بصورة غير مشروعة و عن قصد لما لذلك من اخلال بالاقتصاد الوطني و تأثير سلبي على العمليات المصرفية .( الباب السابع)
- جرائم تمس المعلومات الشخصية :تشمل الأفعال التي تتعلق بمعالجة البيانات ذات الطابع الشخصي دون حيازة تصريح او ترخيص مسبق يسمح القيام بالمعالجة ،و افشاء معلومات ذات طابع شخصي لأشخاص لا يحق لهم الاطلاع عليها.(الباب الثامن)
- جرائم العنصرية و الجرائم ضد الإنسانية بوسائل معلوماتية :و تشمل جرم نشر و توزيع المعلومات العنصرية بوسائل معلوماتية ،و جرم تهديد أشخاص او التعدي عليهم بسبب انتمائهم العرقي او المذهبي او لونهم ،و ذلك بوسائل معلوماتية ،و جرم توزيع معلومات بوسيلة الكترونية بشأنها انكار او تشويه او تبرير أعمال إبادة جماعية أو جرائم ضد الإنسانية ،و جرم المساعدة او التحريض بوسيلة الكترونية على ارتكاب جرائم ضد الإنسانية .( الباب التاسع)
- جرائم المقامرة و ترويج المواد المخدرة بوسائل معلوماتية :تشمل جرم تملك و إدارة مشروع مقامرة على الانترنت و جرم تسهيل ،و جرم تسهيل و تشجيع مشروع مقامرة على الانترنت ، و جرم ترويج الكحول للقاصرين على الانترنت ، و جرم تروم مواد مخدرة على الانترنت.(الباب العاشر )
- جرائم المعلوماتية ضد الدولة و السلامة العامة: تشمل الأفعال الجرمية الناشئة عن المعلوماتية التي تطال الدولة و سلامتها و أمنها و استقرارها و نظامها القانوني ،و هي جرائم تعطيل الاعمال الحكومية او اعمال السلطة العامة باستعمال وسيلة معلوماتية ،كما تشمل جرائم الإخفاق في الإبلاغ او الإبلاغ عن قصد بشكل خاطئ عن جرائم معلوماتية ،بالإضافة الى فعل العبث بالأدلة القضائية المعلوماتية او اتلافها او اخفائها ،و الاعمال الإرهابية التي ترتكب باستعمال شبكة الانترنت او اية وسيلة معلوماتية ،و جرائم التحريض على القتل باستعمال شبكة الانترنت او أية وسيلة معلوماتية.( الباب الحادي عشر)

- جرائم تشفير المعلومات :تشمل أفعال تسويق أو توزيع او تصدير او استيراد وسائل تشفير دون حيازة ترخيص او تصريح من قبل المراجع الرسمية المختصة في الدولة بالإضافة الى بيع او تسويق او تأجير وسائل تشفير ممنوعة .( الباب الثاني عشر)

### 1.4.1 تقسيمات اخرى للجريمة الالكترونية

يمكن تقسيم للجرائم السيبرانية بالنظر الى القصد الجنائي : الى جرائم عمدية و غير عمدية ،و بالنظر الى وقت الجريمة :جرائم متلبس بها و غير متلبس بها ،و بالنسبة الى جسامتها :جرائم جسيمة و غير جسيمة ،كما يمكن تقسيمها حسب مصدرها :جرائم وطنية في حال ان كانت منصات الهجوم او القائمين عليها داخل البلاد المستهدف ،و عالمية في حال منصات الهجوم او القائمين عليها خارج البلد المستهدف.

### 2.4.1 أدوات الجريمة الالكترونية :

- برامج نسخ المعلومات المخزنة في أجهزة الحاسب الآلي.
- الانترنت كوسيط لتنفيذ الجريمة .
- خطوط الاتصال الهاتفي التي تستخدم لربط الكمرات ووسائل التجسس.
- أدوات مسح الترميز الرقمي (الباركود).
- الطابعات .
- أجهزة الهاتف النقال و الهواتف الرقمية الثابتة.

## 2. الآليات التشريعية الوطنية الخاصة بمكافحة الجريمة السيبرانية

يتفاقم يوما بعد يوم وضع جريمة الفضاء السيبراني حيث بالإضافة الى الجرائم التي ترتكب فرديا ،أصبحت الجريمة السيبرانية منظمة الى درجة انها باتت تعتبر أحد أساليب الحرب الجديدة و إحدى وسائل الهجوم الإرهابي بناء على الوضع التشريعي القائم كان من الازم إيجاد حلول للثغرات في التشريعات السيبرانية لملاحقة الجريمة السيبرانية العابرة للحدود الوطنية بغية تفعيل مكافحتها.

و لتأمين انسجام التشريعات الوطنية معها حتى لا يفلت المجرم من العقاب بعد ارتكاب فعله و ينتقل الى بلد اخر ،و بغية اتباع سياسة جنائية مشتركة و تعزيز مبدأ التعاون بين الدول و المنصوص عليه في ميثاق الأمم

المتحدة ،حاولت الدول الجهات الدولية وضع تشريعات نموذجية في هذا المجال ،تطبق احكام اتفاقية بودابست و تأخذها كدليل ( بوداباست المتعلقة بالجريمة الالكترونية بتاريخ 2001/11/23.

## 1.2اليات تشريعية عامة

في بداية الامر لم تكن الجرائم الالكترونية منتشرة كثيرا في الجزائر ،و ذلك يعود لعدم انتشار وسائل ارتكابها و عدم امكانية امتلاكها من طرف كل شرائح المجتمع خاصة الطبقة ذات الدخل الضعيف ،و لهذا كانت جرائمها خاضعة للقوانين العامة في البلاد .

### 1.1.2 الدستور

عمدت الدولة الجزائرية و تطبيقا للمواثيق الدولية بحماة حقوق الانسان و حرياته الاساسية ،حيث ادرجت باب كامل في دستورها للحقوق و الحريات الاساسية اين تم دسترة الكثير منها و كفل الدستور حمايتها ،من بين هذه الحقوق، الحق في المعلومة و الحق في الحياة الخاصة التي يحميها القانون ،و كلما تطورت الحياة و ظهرت حقوق جديدة عدل الدستور و ادرجت نصوص فيه تضمن حمايتها كحق الابتكار الفكري و الفني و حق المؤلف الذي تم دسترته أيضا بعد ما كثر التعدي على هذا الحق و ظهر كثير من النزاعات بشأنه .

كفل الدستور سرية الحياة الخاصة و قرر حماية للحقوق اللصيقة بالشخصية، و حرم الاعتداء على هذه الحقوق كانتهاك حرمة الاشخاص، و النيل من سمعتهم ،او اعتراض مراسلاتهم او تصويرهم او تسجيل مكالماته ،او السب و القذف ،من بين المواد التي ضمنت هذه الحقوق المادة 38 و المادة 44 من الدستور.(الدستور ،باب الحقوق و الحريات )

### 2.1.2القانون المدني

اما القانون المدني فقد اعطى اولوية للحقوق و حرم التعدي على حقوق الغير ،اين اقر في المادة 124 منه حق التعويض عن كل عمل يسبب ضررا للغير ،فالقانون المدني أُقر بالمسؤولية المدنية التي توجب التعويض و التي تقوم على اساس الفعل الضار ،و بالتالي كل نوع من انواع الجريمة الالكترونية سواء كانت جرائم مادية او معنوية كالنيل من سمعت الافراد و التشهير بهم او جرائم الاموال التي تتم عن طريق شبكة الانترنت و تحويل الارصدة ،فمرتكبها يكون مسؤول مسؤولية مدنية و هو ملزم بالتعويض للمجني عليه ،و الذي له حق رفع دعوى قضائية

كصاحب صفة و مصلحة امام القاضي المدني ،و طلب التعويض عن ضرر أصابه جراء اعتداء الكتروني مس بحياته الخاصة على شبكة الانترنت.(القانون المدني الجزائري )

حتى الحكومة و أجهزتها ليس لها الحق في انتهاك الحياة الخاصة للمواطن كالتصوير و اعتراض مراسلاته او تسجيلها و غيرها من الافعال الماسة بحرمته كمواطن ،الا في حالات خاصة قيدها القانوني ،و لا تتم الا بالحصول على امر يسمح بذلك تصدره الجهات المعنية و المختصة في الدولة .

**3.1.2 قانون العقوبات**(القانون رقم 04 - 15 المؤرخ في 10 نوفمبر 2004 )

جرم المشرع الجزائري الأفعال الماسة بأنظمة الحاسب الالي و ذلك نتيجة تأثره بالثورة المعلوماتية العالمية و التي تشكل نوع جديد من الاجرام الذي لم تشهده البشرية من قبل، هذا الامر دفع بالمشرع الجزائري لتعديل قانون العقوبات بموجب القانون 15/04 المؤرخ في العاشر من نوفمبر 2004 المعدل و المتمم للأمر رقم 156/66المتضمن قانون العقوبات ،و الذي خصص له القسم 7مكرر منه تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات "و الذي تضمن 8 مواد ،من المادة 394مكرر الى غاية 394 مكرر 7 .(قانون رقم 15-04)

عرف المشرع الجزائري من خلال هذه المواد نظام المعالجة الآلية للمعطيات حيث اشترط ضرورة الترابط بين مكونات أو أجهزة النظام أو بين الأنظمة فيما بينها ،و ركز على وظيفة المعالجة الآلية للمعطيات موسعا بذلك المجال ليشمل بذلك كلا من المعالجة الآلية للمعطيات .

كتعريفها بدلالة موضوع الجريمة أو السلوك محل التجريم أو الوسيلة المستخدمة، وغير ذلك من المعايير.

أقر المشرع الجزائري تدابير ردعية في القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 إذ تناولت المواد من 394 مكرر إلى 394 مكرر7 أحكام قمع الجرائم المرتكبة في أنظمة المعالجة الآلية للمعطيات ويأخذ الغش المعلوماتي صورتين:

1. الدخول في منظومة معلوماتية ويشمل فعلين هما:
   أ. الدخول تأخذ العبارة على إطلاقها .
   ب. البقاء أكثر من الوقت المحدد.

وعقوبتها بنص المادة 394 مكرر قاع بالحبس من ثلاثة أشهر إلى سنة وبغرامة من50.000 دج إلى 200.000 دج وتضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة وإذا ترتب تخريب نظام اشتغال المنظومة تكون العقوبة من ستة أشهر إلى سنتين والغرامة من 50.000 دج إلى 300.000 دج .

2. المساس بمنظومة معلوماتية ما 394 مكرر 1 ق ع ويشمل فعلين :

أ. إدخال معطيات في نظام المعالجة الآلية غريبة عنه.

ب. تخريب المعطيات التي يتضمنها نظام المعالجة الآلية.

وعقوبتها بنص المادة 394 مكرر 1 قاع بالحبس من ستة أشهر إلى ثلاثة سنوات وبغرامة من500.000 دج إلى 4.000.000 دج.

كما أورد المشرع عقوبات تتراوح من شهرين إلى ثلاث سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج لكل من يقوم بتصميم أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة وحيازة أو إفشاء أو نشر أو استعمال لأي كان المعطيات المتحصل عليها من إحدى الجرائم المذكورة وتضاعف العقوبات إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام.

وأورد المشرع أحكام مشددة على الشخص المعنوي إذ ضاعف العقوبة وجعلها خمس مرات عقوبة الشخص العادي وأحكام خاصة بالمصادرة مع عدم المساس بالغير حسن النية[2].

### 4.1.2 قانون الإجراءات الجزائية (القانون 17- 07 )

نص المشرع الجزائري على تمديد الاختصاص المحلي لوكيل الجمهورية في الجرائم الإلكترونية في المادة 37 قانون إجراءات جزائية ،كما نص على التفتيش في المادة 7/45 ،كما امر في المادة 6/51 على التوقيف للنظر في جريمة المساس بأنظمة المعالجة ،كما نص على اعتراض المراسلات و تسجيل الأصوات و التقاط الصور في المواد من 65 مكرر 5 الى غاية المادة 65 مكرر 10 ،اما بالنسبة لإجراءات التحقيق و المحاكمة فتطبق عليها نفس إجراءات الجريمة التقليدية .(المواد 37 ،7/45، 6/51 ن56مكرر5 الى 65مكرر10)

## 2.2 التشريعات الخاصة بمكافحة الجريمة السيبرانية في الجزائر

### 1.2.2 الحماية في ظل قانون الملكية الفنية و الأدبية (القانون رقم 03-05)

تم تقنين حقوق الملكية الفكرية كونه حق من حقوق الانسان و حريته في التفكير و الإبداع و الابتكار ،و تعتبر هذه العناصر الركيزة الأساسية لقياس تطور الدول و المجتمعات ،اين يقاس تطور الدول بعدد و مكانة المفكرين و المبدعين فيها ،و كون مكونات الحاسب الآلي الأساسية من برامج و و بيانات عبارة عن جهد فكري خاص ،كان لازما على المشرع أن يحمي هذه الحقوق و التي سماها بحقوق الملكية الفكرية او بالأحرى حقوق الملكية الفنية و الأدبية ،و ذلك بتجريم الأفعال التي تشكل اعتداء عليها و أقر عقوبات جزائية على مرتكبيها.

اعترف المشرع بوصف المصنف الفكري لمعطيات الحاسب الآلي أين أقر حماية قانونية لبرامج الحاسب الآلي و ذلك من خلال إخضاعها لحقوق المؤلف حسب ما جاء في الامر 03-05 المؤرخ في 19-07-2003 ،المتعلق بحقوق المؤلف و الحقوق المجاورة بوصفه المصنف المحمي لمصنفات الاعلام الآلي .

ان تصنيف برامج و بيانات الحاسب الآلي مصنفا فكريا و ادماجها ضمن المصنفات الأصلية ،يعني ان أي اعتداء على الحق المالي أو الادبي لمؤلف البرنامج و البيانات يشكل فعل من أفعال التقليد المنصوص عليه في المادة 151 من الامر 03-05 يترتب عليه العقوبات الجزائية المقررة في المواد 153- 156-157-158 من نفس الامر .صنف المشرع الجرائم التي تمس مصنف برامج و بيانات الحاسب الآلي الى ثلاث أنواع هي :

أ. الجنح المرتبطة بالحق المعنوي للمؤلف (1/151)الامر 03-05.

ب. الجنح المرتبطة بالحق الادبي للمؤلف (1/151-152) من نفس الامر .

ت. الجنح المرتبطة بالمصنف المقلد.

ان تجريم المشرع للأفعال الماسة بحقوق المصنف أدى بيه الى فرض عقوبات و جزاءات تطبق على مرتكبي هذه الأفعال .اين فرض عقوبات على جنح تقليد معطيات الحاسب الالي ،اين قسمها الى عقوبات أصلية من خلال المادة 153 من الامر 03-05 و التي تكون عقوبتها الحبس من 6 اشهر الى 3 سنوات ،ويمكن ان تضاف لها عقوبات مالية ،و عقوبات تكميلية ،كمصادرة العتاد او الوثائق و غيرها من الإجراءات و العقوبات التكميلية.

### 2.2.2 قانون التأمين

قد تطرق هذا القانون كذلك إلى تنظيم الجريمة الإلكترونية من خلال هيئات الضمان الاجتماعي، في نصوص قانونية عديدة تخص البطاقة الإلكترونية التي تسلم للمؤمن له اجتماعيا مجانا بسبب العلاج وهي صالحة في كل التراب الوطني، وكذا الجزاءات المقررة في حالة الاستعمال غير المشروع أو من يقوم عن طريق الغش بتعديل أو نسخ أو

حذف كلي أو جزئي للمعطيات التقنية أو الإدارية المدرجة في البطاقة الإلكترونية للمؤمن له اجتماعيا أو في المفتاح الإلكتروني لهيكل العلاج أو في المفتاح الإلكتروني لمهن الصحة للبطاقة الإلكترونية حسب المادة 93 مكرر 247.(بوضياف اسمهان، 2018)

### 3.2.2 الحماية في قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال (القانون رقم 09-04)

صدر القانون رقم 09-04 الصادر في 05 أوت 2009 ،والمتضمن 19 مادة موزعة على ستة فصول، وهو ثمرة عامين من التحضير والدراسة والتحليل والمقارنة مع أحدث القوانين، قامت بإعداده نخبة من رجال القانون بمشاركة خبراء ومهنيين مختصين في مجال الإعلام الإلكتروني من كافة القطاعات المهنية ، 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 أو حالة توفير معلومات عن اعتداء محتمل يهدد منظومة من المنظومات المعلوماتية لمؤسسات الدولة أو الدفاع الوطني أو النظام العام.

وأهم ما نتج عن هذا القانون و تماشيا مع دليل الارشاد الدولي العالمي و الاتفاقيات العالمية الخاصة بمكافحة الجريمة الالكترونية ،هو إنشاء هيئة وطنية للوقاية من الإجرام المتصل بتكنولوجيات الإعلام و الاتصال 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 الذي نص عليه ميثاق الامم المتحدة سواء في اطار تبادل المعلومات و الخبرات في مجال وسائل التكنولوجيا الحديثة ، او في اطار متابعة مرتكبي الجريمة كون الجريمة السيبرانية اليوم أصبحت جريمة منضمة عابرة للحدود الوطنية ،تخضع في محاربتها لتكاتف الجهود الدولية ،سواء في تمديد الاختصاص، او في الامر بالقبض الدولي ،او مشاركة الانتربول في القضايا الخاصة بهذه الجريمة ،أو تطبيق اتفاقيات التعاون في مجال تسليم المجرمين ،و غيرها من الاحكام المتعلقة بالجريمة المنضمة.

يعتبر القانون رقم 09 -04 ذو نطاق شامل في مجال مكافحة الجريمة الإلكترونية، حيث جاء تجريمه للأفعال المخالفة للقانون و التي ترتكب عبر 1 ختير مسعود، المرجع السابق الذكر، ص 102 – مستقبلا.( ختير مسعود، الحماية الجنائية لبرامج الكومبيوتر، أساليب وثغرات، دار الهدى للنشر والتوزيع، الجزائر طبعة 2010

،ص102)تضمن القانون تعريف الجريمة المعلوماتية والذي لم يختلف كثيرا عما ورد في قانون العقوبات، كما نص على بعض الأحكام المتعلقة بمراقبة الاتصالات الالكترونية و الإجرائية لتفتيش المنظومات المعلوماتية، إضافة إلى إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال و مكافحتها .

ولعل أهم ما يثيره هذا القانون بالرغم من أنه جاء ليكمل سلسلة الترسانة القانونية لمواجهة الإشكالات القانونية التي ترتبط بتنوع الجريمة الإلكترونية وتطورها المستمر، بالرغم من ذلك يبقى الفصل الثاني من هذا القانون يثير قلق الحقوقيين بدعوى أن القانون اجاز مراقبة الاتصالات الفردية من دون علمهم ومن دون ارتكاب أي نوع من الإجرام المادي أو المعنوي و هو ما يشكل خرقا للحق في الخصوصية و انتهاكا لحقوق الإنسان وقرينة البراءة المكفولة في الدستور.

إن الظاهر من النص يوحى بأن القانون تضمن انتهاك صارخ للحق في الخصوصية، ولكن الواضح أن هناك ما يبرره في الغالب وهذا ما جاء في مضمون المادة 4 من القانون 90-04 والتي نصت على أربع حالات فقط يجوز اللجوء فيها إلى هذا الإجراء وذلك بالنظر إلى خطورة التهديدات المحتملة و أهمية المصلحة المحمية، تتمثل هذه الحالات في :

- جرائم الإرهاب و التخريب وجرائم ضد امن الدولة .
- عندما تتوفر معلومات عن احتمال وقوع اعتداء على منظومة معلوماتية تهدد مؤسسات الدولة أو الدفاع الوطني.
- ضرورات التحقيق والمعلومات القضائية.
- في إطار تنفيذ طلبات المساعدات القضائية بين الدول .

**خاتمة**

ان الانتشار السريع للجرائم السيرانية و تنوع اشكالها و سهولة ارتكابه التي دمرت أفراد ومؤسسات و دول بأكملها ،أدت بالمجتمع الدولي على مختلف اطيافه بالتصدي لها و الوقوف في وجهها و محاربتها ،كون الجرائم السيبرانية اليوم أصبحت تشكل نوع من الحروب الجديدة تنفذ هجومات قادرة على تدمير العالم بأكمله من خلال فيروس بسيط يتم تسليطه على الافراد او أنظمة الحواسيب لتشل بذلك حركة كل الإدارات و أكبرها في العالم ،خاصة الإدارات العسكرية .

لخطورة هذه الجرائم قامت الدول بسن تشريعات خاصة لمكافحة الجريمة ،منها ما هي وقائية ،و منها ردعية أين تم تشديد عقوبة مرتكبي هذه الجرائم ،قامت الجزائر بإدخال تعديلات على قانون العقوبات بالقانون رقم 04-15 حتى يتماشى مع هذه الجرائم الجديدة كما أدخلت كذلك تعديلات على قانون الإجراءات الجزائية اين تم تعديل الامر رقم 66-156 بالقانون رقم 06-22،هذا من جهة.

و من جهة أخرى و لعدم إلمام القوانين السابقة بكل جوانب الجريمة الإلكترونية، أصدرت الحكومة قوانين خاصة منها القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها و قانون الملكية الفكرية المتعلق بحماية حق المؤلف والحقوق المجاورة رقم 03-05.

و لمواجهة الظاهرة قامت الدول بوضع سياسات و افاق للحد من الجريمة الالكترونية نذكر منها على سبيل المثال لا الحصر مايلي :

- ضرورة تنمية التعاون الدولي لتعزيز الامن المعلوماتي من خلال انشاء مؤسسات مشتركة و سن تشريعات دولية واضحة لتنظيم و ضبط الامن السيبراني و معاقبة مرتكبي هذه الجرائم حتى لا تكون مصدر قلق للمجتمع .
- ان الجريمة السيبرانية جريمة عابرة للحدود فيجب تفعيل مبدأ التعاون الدولي في مجال تسليم المجرمين ،كون الجريمة المعلوماتية لا تقع في مسرح الجريمة دائما و كثيرا ما تقع عن بعد.
- ضرورة استجابة الشركات الخاصة التي تمتلك الأدلة الرقمية الموجودة في البيانات ومنحها للجهات القضائية المختصة التي تطلبها من أجل حل مشكل صعوبة الوصول الى الأدلة الرقمية.
- العمل على تحديث الإطار التنظيمي فيما يتعلق بالتقدم التكنولوجي و هذا من خلال تحديث النظام الجنائي من الناحية الموضوعية بتجريم بعض السلوكيات و الجزائية من خلال فرض عقوبات عليها.
- ضرورة تدريب العناصر المختصة في الدولة و الفاعلة في نظام العدالة الجنائية على استخدام وسائل التكنولوجيا الحديثة و مختلف تطبيقاتها و اكتشاف الجرائم من خلال تزويدهم بأدوات التحليل الجنائي الحاسوبية و التحقيقية المناسبة .
- ومن اهم السياسات التي يجب ان تتخذ لمحاربة هذه الجرائم هي رفع الوعي لدى الافراد و المنظمات و المؤسسات، كونه اهم عامل يتصدى للجريمة الالكترونية كونه يمثل الجانب الوقائي لمثل هذه الجرائم.

## المراجع

### 1 الكتب

- احمد خالد العجلوني ،**التعاقد عن طريق الانترنت** ،الدار العلمية الدولية للنشر ،عمان 2002.
- أبو الغيط رشا مصطفى .(2003) .**الحماية القانونية للكيانات المنطقية** ،الإسكندرية.دار الفكر الجامعي.
- القرعان ، محمود أحمد ،. تميم عبد هلالا سيف التميمي.2016 ، **الجرائم المعلوماتية في الاعتداء على الأشخاص** ، مكتبة القانون والاقتصاد ، الرياض ، الطبعة الأولى .ص16.
- زينات طلعت شحادة .**الأعمال الجرمية التي تستهدف الأنظمة المعلوماتية** .لبنان .مطبعة صادر بيروت.
- زيدان زليخة .(2011).**الجريمة المعلوماتية في التشريع الجزائر والدولي**. ط1.الجزائر.ص42.
- نجم محمد صبحي ،2006.اصول علم الاجرام و علم العقاب .ط1.عمان .دار الثقافة للنشر و التوزيع.
- مكاوي حسن عماد .(1997). **تكنولوجيا الاتصال الحديثة في عصر المعلومات** .ط2.القاهر.الدار المصرية اللبنانية

### 2 مقالات

-بوضياف اسمهان .(2018). **الجريمة الالكترونية و الاجراءات التشريعية لمواجهتها في الجزائر . مجلة الأستاذ الباحث للدراسات القانونية والسياسية.**
**- بن داود عبد العزيز بن فهد بن محمد .2020.الجرائم السيبرانية .دراسة مقارنة تأصيلية .مجلة الاجتهاد للدراسات القانونية و الاقتصادية .المجلد 09 .العدد 03.**
- دريس نبيل .جامعة البليدة . الجريمة السيبرانية بين المفاهيم و النصوص التشريعية.
-kut brush .cybercrimhttps://searchsecurity.techtarget.com/definition/cybercrime
- Organisations Economique de commerce et développement www.oecd.org

### 3قوانين

-الدستور الجزائري
-االقانون المدني الجزائري
-قانون التأمين الجزائري
-القانون 09-04 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولجيا الاعلام و الاتصال و مكافحتها،الجريدة الرسمية العدد 07 لعام 2009.

- القانون رقم 04 - 15 المؤرخ في 10 نوفمبر 2004 المتمم لأمر رقم 22 - 15 المتضمن قانون العقوبات تحت عنوان المساس بأنظمة المعالجة الألية للمعطيات ويتضمن هذا القسم ثمانية مواد من المادة 394 مكرر إلى 394 المادة مكرر 735 .)

- الامر رقم 66-155 المؤرخ في 8 يونيو 1966 المتضمن قانون الإجراءات الجزائية ن المعدل و المتمم بمقتضى القانون 17-07المؤرخ في 27 مارس 2017،المنشور بالجريدة الرسمية عدد 20مؤرخة في 29 مارس 2017.)

- القانون رقم 97-10المتعلق بحماية حق المؤلف و الحقوق المجاورة الملغى بالأمر 03-05)

**4 اتفاقيات**

- THE BUDABEST CONVENTION ON CYBER-
- تشريعات منظمة الاسكوا للجريمة السيبرانية.