العدد الأول
مجلة مستقبل العلوم الاجتماعية
Journal Future of social siences
إبريل ٢٠٢٠

جرائم إختراق النظم الإلكترونية بين التشريع المصرى والمغربى

إعداد

جمال زين العابدين أمين أحمد

باحث دكتوراه /كلية العلوم القانونيه والإقتصاديه والإجتماعيه بطنجه /

جامعة عبدالملك السعدي /المغرب

٢٠٢٠

جرائم إختراق النظم الإلكترونية بين التشريع المصرى والمغربى

تاريخ استلام البحث: ٢٠٢٠/٣/١٥م تاريخ نشر البحث: ٢٠٢٠/٤/١م

مستخلص:

تهدف الدراسة إلى توفير الحماية القانونية للنظم الإلكترونية من قِبل التشريعات الوضعية والاتفاقيات الدولية، كما تهدف إلى تحديد المسؤولية عن اختراق النظم الإلكترونية وانتهاك الخصوصية في القوانين الوضعية والاتفاقيات الدولية، من خلال توفير الحماية القانونية على الصعيد الدولي والداخلي عن اختراق النظم الإلكترونية، وتحديث القوانين وأغراضها الجنائية بما في ذلك التدابير الاحترازية لمكافحة الإجرام الالكتروني، ومحاولة إيجاد حلول قانونية من اجل ملاحقة المجرم مجهول الهوية في هذه الجرائم بغية حماية مصالح وأمن الدول وحقوق ضحايا جرائم الاختراق، وقد توصلت الدراسة للإجابة علي كافة تساؤلاتها.

الكلمات المفتاحية: التشريع المصري، التشريع المغربي، جرائم إختراق النظم الإلكترونية.

Abastract:

The study aims to provide legal protection for electronic systems by statutory legislation and international conventions, and it also aims to determine responsibility for breaching electronic systems and violating privacy in positive laws and international agreements, by providing legal protection at the international and internal levels for penetration of electronic systems, updating laws and their criminal purposes Including precautionary measures to combat cybercrime, and trying to find legal solutions in order to prosecute the unknown criminal in these crimes in order to protect the interests and security of states and the rights of victims of hacking crimes, and the study reached an answer to all its questions.

Key words:

Egyptian legislation, Moroccan legislation, crimes of hacking electronic systems.

مقدمة:

قد أدرك العالم أهمية تقنية المعلومات كونها تدخل في أدق تفاصيل الحياة اليومية للمجتمعات على المستوى القطري والدولي(المرى، ٢٠١٩، ص٥)، ومن ثم فقد أصبحت التكنولوجيا ضرورة حتمية داخل المؤسسات الحكومية وغيرها لدى العديد من القطاعات الأخرى، كما أصبحت برامج الحاسب الآلي، وما نشأ عنها من نظم معلوماتية متقدمه حقيقة علمية أحدثت تغيرات جذرية في تسهيل وصول المعلومات للمستفيدين، وقد شهد التدخل القانوني في تنظيم تلك الظاهرة المعلوماتية تطوراً ملحوظاً في الآونة الأخيرة من خلال الاتجاهات التشريعية والقضائية والفقهية الحديثة. (حنفى، ٢٠١٧، ص٦)

ومنذ ظهور شبكة المعلومات الدولية، وتطوراتها المتتابعة كنافذة يطل منها العالم ليعرف ما يجرى من أحداث ويحصل على ما يريد من معلومات، وقد ثبت تأثير الانترنت على تاريخ الشعوب من خلال ما يبث عبر مواقعه من معلومات، وتجلى ذلك من خلال موقعي الفيس بوك" face book" واليوتيوب" YouTube" في إحداث شرارة ثورة الخامس والعشرين من يناير ٢٠١١ بالقاهرة.(الصباغ، ٢٠١٦، ص٦)

ومن هنا تتضح المزايا المختلفة للثورة المعلوماتية والتكنولوجية وقدرتها على تغيير أوجه الحياة إلى الأفضل، غير أن هذه الثورة المعلوماتية ذاتها تحمل في طياتها كذلك؛ أيضاً بذور الشر التي تتمثل في استخدام الحاسب الآلي عن طريق شبكة الانترنت للاعتداء على هذه المصنفات.(الصباغ، ٢٠١٦، ص٧)

وقد أدى ظهور العديد من مشكلات اختراق النظم الإلكترونية في جميع المجالات وفي جميع الدول إلى ظهور كثير من جرائم الاختراق، مما أدى إلى التدخل التشريعي في بعض الدول لإصدار قانون خاص بجرائم تقنية المعلومات ومن هذه الدول الإمارات والسعودية والأردن ومصر من أجل تحديد المسئول عن هذه الجرائم وتقديم الحماية القانونية للنظم الإلكترونية، ومن ثم إيجاد الوسائل المناسبة لتشجيع التعاون الدولي لمواجهة جرائم المعلومات والعمل على التوفيق بين التشريعات الخاصة التي تتناول هذه الجرائم، أن يشمل هذا التعاون الدولي في تبادل المعلومات وتسليم المجرمين القائمين على هذه الجرائم.(قورة، ٢٠٠٥، ص ٥٤)

كما أدى استخدام الثورة المعلوماتية من بعض الأشخاص الاستخدام غير المشروع في ارتكاب الكثير من الجرائم سواء ضد الأشخاص أو الأموال أو الأنظمة ومنها اختراق

النظم الإلكترونية إلى إصدار قانون بشأن مكافحة جرائم تقنية المعلومات أو اختراقها بهدف تحقيق حالة من التوازن بين الحماية الجنائية لحرمة الحياة الخاصة التي يكفلها الدستور والحافظ على المعلومات وكفالة سريتها وعدم إفشائها أو التصنت عليها إلا بأمر قضائي بسبب وبين مواجهة تلك الجرائم والأفعال ومكافحتها والحد من أثارها.(المرى، ٢٠١٩، ص٥)

مشكلة البحث:

لقد صاحب التقدم العلمي ظهور أنماط مُستحدثه من الجرائم لم يُنص على تجريمها في التشريعات الجزائية القائمة لدى بعض البلدان العربية، ولعل السبب في ذلك التطور السريع لثورة الاتصالات وتكنولوجيا المعلومات(حجازى، ٢٠٠٩، ص٩)، وعلى المستوى العالمي فقد برز نظام الأيزو والاعتماد والتقييم والتقييس "27001" لضمان أمن المعلومات، وكذلك نظام "COBT" من"ISACA" لأمن المعلومات، لذلك يعتبر الأمن المعلوماتي أحد الأعمدة التي يقام عليها الأمن القومي للدولة(المصرى، ٢٠١٩، ص٧٧)، وفي ضوء اختراق النظم الإلكترونية من الجرائم المُستحدثة التي فرضت نفسها على المستوى الدولي والوطني والتي يجب على المشرع مكافحتها والتصدي لها بتشريعات حاسمه وعقاب مرتكبيها، وإن كان التطور المستمر قد يؤدى إلى عدم استيعاب النصوص الحالية إلا أن وضع قواعد قانونية تنظم أوجه الحماية أفضل من ترك ما يُستجد على الساحة الجنائية دون حماية وهذا ما يقع على عاتق الفقه في صياغة النصوص التشريعية، ومن ورائه القضاء في تفسير وتكييف قواعد تلك النصوص. (غنية، ٢٠١٥، ص٩)

أهمية البحث:

تكمن أهمية الدراسة في كيفية إتاحة الفرصة للفرد والمجتمع لاستخدام تكنولوجيا المعلومات في التطور الاقتصادي والاجتماعي والسياسي والعلمي في ظروف آمنه وتحت مظلة قانونية تُنظم استخدام تكنولوجيا المعلومات وخاصة منع اختراق النظم الإلكترونية وتحديد المسئول عن اختراق النظم الإلكترونية وخاصة في حالة المجرم مجهول الهوية والجريمة عابرة الحدود والجريمة المنظمة، ومن ضمن ما تتضمنه أهمية مقارنة بعض التشريعات الداخلية بالقوانين والاتفاقيات الدولية الخاصة بموضوع حماية النظم الإلكترونية من الاختراق، **وعليه فإن عدة نقاط تنفرد بها الدراسة، وهي على النحو التالي:**

- ندرة الدراسات التي تناولت ظاهرة اختراق النظم الإلكترونية في المجتمع المصري والمغربي وذلك في حدود علم الباحث.

- إلقاء الضوء على خطورة المشكلة من النواحى القانونية والاجتماعية ومدى تأثيرها على الأفراد والمؤسسات، والدولة.
- الايمان الكامل بحق الافراد في الحياة في جو يسوده قدر من الخصوصية والسرية.
- مدى تأثير هذه الظاهرة على الامن القومي بصفة عامة للدولة.
- حث المشرع في جمهورية مصر العربية والمملكة المغربية على إستصدار القوانين الرادعه لمواكبة التطور في الثورة التكنولوجية، لمعاقبة مرتكبي هذه الجرائم.

أهداف البحث:

تهدف الدراسة إلى توفير الحماية القانونية للنظم الإلكترونية من قِبل التشريعات الوضعية والاتفاقيات الدولية، كما تهدف إلى تحديد المسؤولية عن اختراق النظم الإلكترونية وانتهاك الخصوصية في القوانين الوضعية والاتفاقيات الدولية، **وعليه سوف يتم إبراز أهم أهداف الدراسة:**

- توفير الحماية القانونية على الصعيد الدولي والداخلي عن اختراق النظم الإلكترونية.
- تحديث القوانين وأغراضها الجنائية بما في ذلك التدابير الاحترازية لمكافحة الإجرام الالكتروني.
- رفع الوعي لدى القضاة والعاملين في المجال القانوني والأجهزة العاملة على مكافحة تلك الجرائم.
- محاولة إيجاد حلول قانونية من اجل ملاحقة المجرم مجهول الهوية في هذه الجرائم بغية حماية مصالح وأمن الدول وحقوق ضحايا جرائم الاختراق.
- محاولة إيجاد حلول لمحاربة الجريمة عابرة الحدود والجريمة المنظمة.
- إيجاد حلول لتفعيل التعاون الدولي من أجل وضع اتفاقيات دولية لوضع تشريعات دولية لمكافحة اختراق النظم الإلكترونية، ووضع معايير لتنظيم استخدام تكنولوجيا المعلومات سواء على المستوى الفردي أو الدولي أو المؤسسات من أجل التعاون الدولي لمنع وقوع الجرائم وتسليم المجرمين.

وفي الأخير، فإن هذه الدراسة تهدف إلى جذب انتباه المشرعين والقانونيين في المجتمع المصري والمغربي بصفة خاصة والمجتمع الدولي بصفة عامة إلى ضرورة إصدار وصياغة أو إعادة صياغة العديد من القوانين والتشريعات والتي تحد من اختراق النظم الإلكترونية ووضع القوانين الرادعة لمرتكبي هذه الجرائم.

مفاهيم البحث:

تشتمل الدراسة على بعض المصطلحات الأساسية، والتي يأتي أهمها فيما يلي:

اختراق النظم الإلكترونية:

عرف المشرع المصري النظم الإلكترونية بأنها: "مجموعة برامج وأدوات معدة لغرض أدارة ومعالجة البيانات والمعلومات أو تقديم خدمة معلوماتية" (القانون رقم ١٨٥، ٢٠١٨).

كما عرف المشرع الإماراتي النظام المعلوماتي الإلكتروني بأنه: "مجموعة برامج ووسائل تقنية المعلومات المعدة لمعالجة وإدارة وتخزين المعلومات الإلكترونية أو ما شابه ذلك"(مرسوم ٥، ٢٠١٣، ص١٧)

ويُعرف الاختراق بأنه: "كل من ينفذ أو يبقى بصفة غير شرعية بكامل أو بجزء من نظام البرمجيات والبيانات المعلوماتية وترفع العقوبة إذا نتج عن ذلك ولو عن غير قصد إفساد أو تدمير البيانات الموجود بالنظام المذكور"(عمارسة، ٢٠١٥، ص ٥٣).

ويُعرف أيضاً بأنه: "الوصول بطرق احتيالية، كلياً أو جزئياً للنظام الآلي لمعالجة البيانات"(سويلم، ٢٠١٨، ص١٩)

وعرفه المشرع المصري بأنه:" الدخول غير المرخص به أو المخالف لأحكام الترخيص أو الدخول بأي طريقة غير مشروعة غلى نظام معلوماتي أو حاسب إلى أو شبكة معلوماتية وما في حكمها" (القانون ١٧٥ لسنة ٢٠١٨، ص٥)

أما الاختراق الإلكتروني فيُعرف بشكل عام بأنه: "القدرة على الوصول لنظام الكتروني بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بالهدف وبطبيعة الحال"، وهي سمه سيئة يتسم بها المخترق لقدرته على دخول نظم الآخرين بدون رغبة منهم وحتى دون علم منهم بغض النظر عن الأضرار الجسيمة التي قد يحدثها سواء بأنظمتهم الشخصية أو اختراق خصوصياتهم عند سحب ملفات وصور تخصهم وحدهم أو حتى الاطلاع عليها سوء نتج عن ذلك ضرر أو لم ينتج ضرر.

ويعرف أيضاً بأنه: "الدخول أو إتلاف أو محو أو تغيير أو نسخ أو إعادة نشر للبيانات والمعلومات الموجودة على ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي".(المرى، ٢٠١٩، ص٧٧)

وفى ضوء هذه التعريفات، يمكن للباحث صياغة تعريف إجرائي للاختراق الإلكتروني بأنه: "الدخول غير المرخص لأي من الأنظمة الإلكترونية سواء كان نظام فرد أو

مؤسسة عامة أو خاصة سواء نتج عن هذا الدخول ضرر أو لم ينتج سواء كان بقصد أو بدون قصد".

الدراسات السابقه

دراسات تناولت جرائم اختراق النظم الإلكترونية:

(١) دراسة: عبد اللطيف بن صالح السويد (٢٠٠٩):

بعنوان: "جريمة الاختراق الإلكتروني وعقوبتها، دراسة مقارنة".

تنبع أهمية تلك الدراسة في أن الجريمة أصبحت تُشكل هاجساً مخيفاً وكابوساً مزعجاً أرق الكثير من ذوى الشأن وغيرهم بل أصبحت وبكل أسف ظاهرة بدأت بالتفشي وكارثة أخذت طريقها في الانتشار، كما يستوجب تنامي هذه الجريمة أهمية توعية الآخرين بمخاطرها وتحذيرهم من آفاتها وإيجاد حصانه علمية وعملية تحميهم، وتأتي أهميتها أيضاً من أن الحاسب الآلي أصبح ومن ورائه الانترنت أحد ضروريات الحياة فلا تكاد تخلو منها دار، كما أن تعدد دوافع الجريمة وتنوع أساليبها مما أدى لتفشيها في المجتمع وظهورها بصور وأشكال شتى، وأن حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية.

وقد انبنى سبب اختيار موضوع الدراسة على أن التطور الهائل والتقدم في أنظمة الحاسب الآلي وشبكة الانترنت ساهم وبشكل مباشر في توسيع هذه الجريمة وظهورها بصوره وألوان متعددة، وأن صدور نظام مكافحة جرائم المعلومات الجديد، والذي تناول هذه الجريمة في أكثر من مادة، وأن نشر الوعي بين أوساط الناس وتقديم سبل الوقاية من هذه التجاوزات، ونشر طرق الحماية منها، وأن التصدي لهذه الجريمة ومكافحتها بكل الوسائل المشروعة.

وقد ارتكزت تساؤلات الدراسة الحالية على عدة تساؤلات فرعية يأتي أهمها في ماهية الاختراق الإلكتورني؟، وما مدى انتشار هذه الجريمة؟ وما نسبة الوعي بين مستخدمي هذه التقنية؟، وماهية الوسائل المشروعة لمكافحة هذه الجريمة؟ وما سبل الوقاية منها، **وقد توصلت الدراسة إلى عدة نتائج يأتي أهمها في:** الإجابة التساؤلات من خلال عرض الباحث النظري للدراسة حيث قسمها إلى عدد أربع فصول نظرية داخل كل فصل نظرية مجموعة من المباحث الفرعية.

(٢) دراسة: إسلام عبد الله محمد عباس (٢٠١٠):

بعنوان: "أمن المعلومات على شبكة الانترنت واستخدام طريقة حقن لغة الاستعلام الهيكلية في اختراق قواعد بيانات المواقع الإلكترونية".

هدفت الدراسة إلى إبراز خطورة الهجمات على المواقع في الشبكة العنكبوتية وبخاصة المنفذة بواسطة لغة (SQL)، ومن ضمن ما هدفت إليه الدراسة هو: تصميم برنامج لاختراق المواقع الإلكترونية والتي تعتمد على دوال تصفية البيانات، والوقوف على المخاطر التي تهدد أمن البيانات وكيفية التعامل معها، ومن ثم دراسة الأساليب المستخدمة في عمليات ألاختراق والمراحل التي تمر بها، وفي الأخير مناقشة النماذج الأمنية المستخدمة في أمن المعلومات، وقد اتبعت الدراسة المنهج الاستنباطي والتاريخي في الدراسة.

وتبرز أهمية البحث في أن معظم التطبيقات والمواقع الإلكترونية تعتمد على لغة الاستعلام الهيكلية في بناء قواعد البيانات الخاصة بها وذلك للإمكانيات الهائلة في خصائصها، مما أدى إلى استخدامها من قبل المهاجمين على هذه المواقع على حد السواء وذلك بغرض التخريب المتعمد.

وتكمن مشكلة البحث في أنه ومع التطور الواسع في استخدام التطبيقات الإلكترونية واستخدامها لقواعد البيانات في تخزين الكثير من المعلومات والبيانات الهامة ازدادت أهمية المحافظة عليها من الهجمات التي قد تواجهها، ومع تعدد أنواع الهجوم وتنوع الأضرار فإن من أقوى الهجمات التي تتعرض لها هي حقن لغة الاستعلام الهيكلية (SQL) والتي تؤدى إلى خسائر كبيرة خاصة في قواعد البيانات التي ترتبط بمواقع إلكترونية يوجد بها معاملات مالية.

(٣) دراسة: عادل المهادي (٢٠١٠):

بعنوان: "الجريمة المعلوماتية، جريمتا الدخول غير المشروع وإتلاف المعطيات، دراسة مقارنة بين التشريع المغربي والتشريعات المقارنة".

تناولت الدراسة أهمية البحث من منظور أنه إذا كانت الأسلحة المتطورة والمعدات الحديثة من الأمور الشائعة الاستخدام في ارتكاب الجريمة فإن الجديد في هذا المجال هو استهداف المجرمين للتقنية المعلوماتية، وإذا كانت الأموال المادية، هي غاية كل مجرم فإن الأموال المعنوية من معلومات وبرامج غدت هي الهدف الرئيسي للمجرم المعلوماتي، فعوض أن نسمع عن استخدام الأسلحة النارية أو البيضاء في لجريمة، ومن هنا بدأ الباحثون في حقل العلوم الجنائية للبحث في سبل معالجة هذه الجرائم المستحدثة، عن طريق إبراز الصعوبات

التي تعترض تطبيق النصوص الجنائية التقليدية على أشكال الجريمة الجديدة والتي أفرزتها الثورة المعلوماتية.

وقد بنت الدراسة إشكاليتها مرتكزة على بعض التساؤلات، والتي يأتي أهمها في: ما مدى توافق المشرع المغربي في حماية نظام المعالجة الآلية للمعطيات من الاعتداءات المتمثلة في الدخول غير المشروع وفي إتلاف المعلومات؟، وما مدى انطباق النصوص التقليدية عليها؟، وما طبيعة الجريمة المعلوماتية؟، وما أهم الدوافع التي أدت بالمشرع إلى تجريم الدخول غير المشروع والإتلاف المعلوماتي؟، وما هي الأحكام التي تخضع لها هاتين الجريمتين؟، وقد اعتمدت الدراسة على المنهج الوصفي التحليلي.

وقد توصلت الدراسة إللى عدة نتائج يأتي أهمها في الآتي:

- التعرف بجرائم الحاسب الآلي/الجريمة المعلوماتية؟
- الاختلاف الفقهي حول إيجاد تعريف موحد حول ماهية الجريمة المعلوماتية.
- خصائص الجريمة المعلوماتية والتي تميزها عن الجريمة التقليدية.
- الوقوف على السمات الخاصة بالمجرم المعلوماتي.
- التعريف بالمجرم المعلوماتي والأسباب التي تحفزه على ارتكاب الجريمة المعلوماتية.
- التعريف بالمعلومات وتميزها عن الأنظمة المشابهة لها.
- التوصل إلى أن القيمة الذاتية للمعلومات توجب حمايتها جنائياً.
- أن المشرع المغربي يعاقب على جريمة الدخول غير المشروع وأنه يأخذ بالمفهوم الواسع للمحل في جريمة الدخول غير المشروع على غرار المشرع الفرنسي.
- أن المشرع المغربي يأخذ بالقصد العام في جريمة الدخول غير المشروع وهو بذلك يجعل من هذه الجريمة جريمة عمدية وهي جريمة شكلية وليس بجريمة نتيجة.
- أن المشرع المغربي يجرم الإتلاف المعلوماتي أو ما يصطلح عليه بجريمة إتلاف المعطيات المعالجة آليا وأن المشرع المغربي قد جعل منها ظرف تشديد في جريمة الدخول غير المشروع بمقتضى الفقرة الثالثة من الفصل (٣-٦٠٧) من القانون الجنائي وجريمة مستقلة بمقتضى الفصل (٦-٦٠٧) من نفس القانون.

كما توصلت الدراسة إلى عدة توصيات يأتي أهمها في الآتي:

- ضرورة تدريس هذه الجرائم ضمن المقررات الجامعية.

- ضرورة أن يتولى المشرع المغربي إعادة النظر في النصوص المتعلقة بالمساس بنظم المعالجة الآلية للمعطيات.
- ضرورة الأخذ بمقتضيات "اتفاقية بودابيس" وتعتبر النموذج الأمثل لمواجهة هذه الجرائم.
- أهمية التأهيل الأكاديمي لمختلف المتدخلين في مكافحة الجريمة المعلوماتية من رجال الشرطة، وقضاة النيابة والحكم.
- أهمية إنشاء وحدات خاصة لمكافحة الجريمة المعلوماتية في جميع مفوضيات الشرطة ومحاكم المملكة المغربية.
- إعادة النظر في السياسة الجنائية المتبعة من قبل الدولة لتشمل هذه الجرائم المستحدثة.
- تدعيم الأجهزة الأمنية مادياً وبشرياً وذلك بمدها بالوسائل التقنية والكوادر المختلفة.

خطة البحث:

<u>المبحث الأول: ماهية إختراق النظم الإليكترونيه مخاطرها وأنواعها</u>

المطلب الأول: مخاطر إختراق النظم الإليكترونيه

المطلب الثاني: تعريف الاختراق الإلكتروني وأنواعه

<u>المبحث الثاني: أسباب اختراق النظم الإلكترونية وأثارها وحمايتها</u>

المطلب الأول: أسباب اختراق النظم الإلكترونية

المطلب الثاني: أثار اختراق النظم الإلكترونية ووسائل وحمايتها.

المبحث الأول:

المطلب الأول:المخاطر التي تتعرض لها النظم الإلكترونية:

تتضمن المخاطر التي تتعرض لها النظم الإلكترونية ما يلي: (اختراق الأنظمة الإلكترونية، والاعتداء على حق التخويل، وزراعة نقاط الضعف، ومراقبة الاتصالات، واعتراض الاتصالات، وعرقلة سير النظام، وإنكار القيام بالتصرف، وتهديد البنية الاقتصادية للدول والمؤسسات والبنية الإلكترونية وسلامة وأمن الدول، وأيضاً تتهديد النظام السياسي والاجتماعي)، وعلى النحو التالي:

١- اختراق الأنظمة الإلكترونية:

ويتحقق ذلك بولوج شخص غير مخول له الدخول إلى نظام الكمبيوتر والقيام بأنشطة غير مصرح له بها كتعديل البرمجيات التطبيقية وسرقة البيانات السرية أو تدمير الملفات أو البرمجيات أو النظام أو لمجرد الاستخدام غير المشروع، ويتحقق الاقتحام بشكل تقليدي من خلال أنشطة (الاختراق والتخفي) ويراد به تظاهر الشخص المخترق بأنه شخص آخر مصرح له بالدخول، أو من خلال استغلال نقاط الضعف في النظام كتجاوز إجراءات السيطرة والحماية أو من خلال المعلومات التي يجمعها الشخص المخِترق من مصادر مادية أو معنوية، كالتنقيب في قمامة المنشأة للحصول على كلمات السر أو معلومات عن النظام أو عن طريق الهندسة الاجتماعية كدخول المخِترق إلى مواقع معلومات حساسة داخل النظام باستغلال شخص آخر.(عباس، ٢٠١٠، ص١٦)

٢- الاعتداء على حق التخويل:

ويتم ذلك من خلال قيام الشخص المخول له استخدام النظام لغرض ما باستخدامه في غير هذا الغرض دون أن يحصل على التخويل بذلك، وهذا الحظر يعد من الأخطار الداخلية في حقل إساءة استخدام النظام من قبل موظفي المنشأة، وقد يكون أيضا من الأخطار الخارجية، كاستخدام المخترق حساب شخص مخول له باستخدام النظام عن طريق تخمين كلمة السر الخاصة به أو استغلال نقطة ضعف بالنظام للدخول إليه بطريق مشروعة أو جزء مشروع ومن ثَم القيام بأنشطة غير مشروعة.

٣- زراعة نقاط الضعف:

يتحقق هذا الخطر نتيجة اقتحام من قبل شخص غير مصرح له بذلك أو من خلال مستخدم مشروع تجاوز حدود التخويل الممنوح له حيث يقوم الشخص بزرع مدخل ما يحقق له الاختراق فيما بعد، ومن أشهر أمثلة زراعة المخاطر حصان طروادة: وهو عبارة عن برنامج يؤدى غرضاً مشروعاً في الظاهر لكنه يمكن أن يُستخدَم في الخفاء للقيام بنشاط غير مشروع، كما يُستخدَم برنامج معالجة كلمات ظاهرياً لتحرير وتنسيق النصوص في حين يكون غرضه الحقيقي طباعة كافة ملفات النظام ونقلها إلى ملف مخفي بحيث يمكن للمخِترق أن يقوم بطباعة هذا الملف والحصول على محتويات النظام.

٤- مراقبة الاتصالات:

وذلك باختراق الحاسب الآلي الخاص بالمجني عليه ليتمكن الجاني من الحصول على معلومات سرية غالباً ما تكون من المعلومات التي تسهل له مستقبلاً اختراق النظام وذلك ببساطة من خلال مراقبة الاتصالات من إحدى نقاط الاتصال أو حلقاتها.

٥- اعتراض الاتصالات:

يتحقق باختراق النظام حيث يقوم الجاني في هذه الحالة باعتراض المعطيات المنقولة خلال عملية النقل ويجري عليها التعديلات التي تتناسب مع غرض الاعتداء، ويشمل اعتراض الاتصالات قيام الجاني بخلق نظام وسيط وهمي بحيث يكون على المستخدم أن يمر من خلاله ويزود النظام بمعلومات حساسة بشكل طوعي.

٦- عرقلة سير النظام:

يتم ذلك من خلال القيام بأنشطة تمنع المستخدم الشرعي من الوصول إلى المعلومات أو الحصول على الخدمة وأبرز أنماط إنكار الخدمة إرسال كمية كبيرة من رسائل البريد الإلكتروني دفعة واحدة إلى موقع معين بهدف إسقاط النظام المستقبِل، لعدم قدرته على احتمالُها أو توجيه عدد كبير من عناوين الإنترنت على نحو لا يتيح عملية تجزئة حزم المواد المرسلة، فيؤدي إلى اكتظاظ الخادم وعدم قدرته على التعامل معه.

٧- إنكار القيام بالتصرف:

يتمثل هذا الخطر في عدم إقرار الشخص المرسِل أو المرَسَل إليه بالتصرف الذي صدر عنه، كأن ينكر أنه ليس هو شخصياً الذي قام بإرسال طلب الشراء عبر الإنترنت وتنطلق الإستراتيجية الفاعلة من القدرة على إيجاد نظام متواصل لعملية تحليل المخاطر وتحديد احتياجات الحماية، وعملية تحليل المخاطر هي في حقيقتها نظام متكامل للتحليل وسلامة التصرف تبدأ من الإعداد الجيد القائم على فهم وإدراك وتحديد عناصر النظام والعمليات والمخاطر، ومن ثَم تحديد معايير التهديد ونطاق الحماية المطلوبة لوسائل الحماية، لتنتهي ببيان معيار الخسارة المقبولة التي يتصور تحقيقها بغض النظر عن مستوى الحماية ومستوى الاستعداد للمواجهة.(داوود، ٢٠٠٠، ص١٢٥)

٨- تهديد البنية الاقتصادية للدول:

يُعد هذا من أخطر الجرائم الإلكترونية بصفة عامة وجرائم اختراق النظم الإلكترونية بصفة خاصة، إذ أن مرتكبي تلك الجرائم يعمدون في الغالب عند ارتكابهم تلك الجرائم

الحصول على أكبر المنافع المادية، حيث ظهرت إلى حيز الوجود جرائم السطو الإلكتروني على الودائع والأموال الخاصة بالمؤسسات الاقتصادية المالية العامة أو الخاصة.(أبوسكى، ٢٠٠٦، ص٣٢١)

٩- تهديد البنية الإلكترونية للدول والمؤسسات:

حيث يعمد مرتكبي الجرائم الإلكترونية في الغالب إلى إثبات مهاراتهم وتفوقهم من خلال قيامهم باختراق الأنظمة الإلكترونية للدول ومؤسساتها العامة والخاصة، وكذلك تعطيل أو إيقاف تلك الأنظمة عن العمل سواء بشكل مؤقت أو لفترات طويلة،سواء كان التعطيل كلى أم جزئي، وذلك بغرض الحصول على ما بتلك الأنظمة من بيانات ومعلومات.(عبد الحميد، ٢٠٠٧، ص٣٨)

١٠- تهديد أمن وسلامة الدول:

يتحقق ذلك عن طريق اختراق المواقع الخاصة للمؤسسات الأمنية الداخلية والخارجية والتجسس واختراق المواقع الخاصة بوزارة الدفاع بدولة ما.

١١- تهديد النظام السياسي والاجتماعي للدول:

يتحقق ذلك عن طريق نشر الأفكار الهدامة والشائعات التي تهدف إلى السيطرة الفكرية على الأفراد من أجل هدم النظم السياسية والاجتماعية في الدول.

المطلب الثاني: تعريف الاختراق الإلكتروني وأنواعه

أ- تعريف الاختراق الإلكتروني:

يعتبر الاختراق قيام أحد الأشخاص غير المصرح لهم بالدخول إلى نظام التشغيل في جهاز ما بطريقة غير شرعية ولأغراض غير سوية مثلاً الاعتراض أو الإتلاف أو السرقة أو البقاء غير المشروع أو تتجاوز حدود الدخول من حيث الزمان والمكان، حيث يتاح للشخص المخِترق أن ينقل أو يمسح أو يضيف ملفات أو برامج كما أنه بإمكانه أن يتحكم في نظام التشغيل فيقوم بإصدار أوامر مثل إعطاء أمر الطباعة أو التصوير أو التخزين أو الحذف.

وعرف بعض الفقهاء الاختراق بأنه: "قيام شخص بمحاولة الوصول إلى جهاز شخص ما أو الشبكة الخاصة به عن طريق شبكة الإنترنت باستخدام برامج متخصصة في فك الرموز والكلمات السرية وكسر الحواجز الأمنية واستكشاف مواطن الضعف في جهاز أو شبكة المعلومات الخاصة بذلك الشخص وعادة ما تكون المخارج (بوابات العبور للمعلومات)

الخاصة بالشبكة المحلية وهذه أسهل الطرق إلى جميع الملفات والبرامج الموجودة في ذلك الجهاز".(أحمد، ٢٠١٧، ص٢٤)

كذلك عرف بعض الفقهاء اختراق الأنظمة بأنه: "دخول شخص غير مخول بذلك إلى نظام الكمبيوتر والقيام بأنشطة غير مصرح له بها كتعديل البرمجيات التطبيقية وسرقة البيانات السرية أو تدمير الملفات أو البرمجيات أو النظام أو لمجرد الاستخدام غير المشروع".(عباس، ٢٠١٠، ص١٨)

كما يعرف الاختراق بأنه: "عبارة عن فعل دخول غير مصرح به إلى جهاز الحاسب الآلي العائد للغير وشبكته الإلكترونية ويتم هذا الاختراق باستخدام برامج متطورة يستخدمها أشخاص لديهم الخبرة والقدرة على استخدامها في الدخول غير المصرح به".(العبيدى، ٢٠١٢، ص ١٣)

وعرف جانب من الفقه الاختراق بأنه: "الدخول غير المشروع على نقطة ارتباط أساسية أو فرعية متصلة بالإنترنت من خلال نظام إلى (PC–Server) أو مجموعة نظم مترابطة شبكياً (Intranet) بهدف تخريب نقطة الاتصال أو النظام".(الزنط، ٢٠١٠، ص٤)

وعرف القانون العربي النموذجي الاختراق بأنه: "الدخول غير المصرح به أو غير المشروع لنظام المعالجة الآلية للبيانات وذلك عن طريق انتهاك الإجراءات الأمنية"، بينما لم يعرف المشرع المغربي الاختراق الإلكتروني تاركاً ذلك للفقه والقضاء، ولم يعرف المشرع الإماراتي الاختراق في القانون رقم ٢لسنة٢٠٠٦ المعدل بالقانون رقم ٥لسنة٢٠١٢ بشأن مكافحة جرائم تقنية المعلومات، تاركاً ذلك للفقه والقضاء وهو ذات اتجاه المشرع المغربي.

بينما عرف المشرع المصري الاختراق بأنه: "الدخول غير المرخص به، أو المخالف لأحكام الترخيص، أو الدخول بأي طريقة غير مشروعة على نظام معلوماتي أو حاسب إلى أو شبكة معلوماتية وما في حكمها".(المادة الأولى من القانون المصرى رقم ١٧٥ لسنة ٢٠١٨)

ويمكن تعريف اختراق النظم الإلكترونية بأنه: هو الدخول أو البقاء غير المصرح به أو تجاوز حدود الترخيص أو إعاقة النظام الإلكتروني أو الاعتداء على حاسب آلي، أو شبكة معلوماتية أو وسيلة من وسائل التقنية الحديثة أو ما في حكمها باستخدام وسائل التقنية الحديثة أو غيرها سواء نتج عن هذا السلوك ضرر أم لا.

كما تعد قرصنة البرامج من الجرائم التي ارتبطت بنشأة الحاسبات الآلية بصفة عامة، إلا أن ظهور شبكات المعلومات والنظم الإلكترونية قد ساعد على نحو كبير في زيادة حجم هذه الجرائم لما وفرته هذه الشبكات من مجال خصب لارتكابها، حيث أن طبيعة الشبكة المعلوماتية التي عن طريقها أضحى العالم قرية صغيرة، كذلك ارتفاع القيمة المادية لهذه البرامج وسهولة إعادة النسخ، وسهولة التسويق لهذه البرامج المنسوخة، أصبحت القرصنة الإلكترونية داخل شبكات المعلومات مجالاً خصباً.(عتيق، ٢٠٠٠، ص ٢٤)

ويرى جانب من الفقه تقسيم قرصنة برامج الحاسبات الآلية عبر شبكات الإنترنت إلى ثلاثة طوائف رئيسية: (Millard, 1994, p221)

- الطائفة الأولى: هم منفذو عملية القرصنة الذين يقومون بعد ذلك بنقل البرامج عبر شبكة الإنترنت ويكون الهدف منها إما تحقيق ربح مادي أو استعراض التقنية وقدرات مهاراتهم.
- الطائفة الثانية: هم مستخدمو الشبكة الذين يقومون بتلقي هذه البرامج وتحميلها واستخدامها مع العلم أنها برامج قد تم نسخها.
- الطائفة الثالثة: القائمون على إدارة شبكات المعلومات، والذين يقومون بتلقي هذه البرامج أثناء عملية نقلها.

ب- أنواع الاختراق الإلكتروني:

يمكن تقسيم الاختراق من حيث محل الاعتداء إلى ثلاثة أنواع(أحمد، ٢٠١٧، ص ٣٤)

١- اختراق المزودات أو الأجهزة الرئيسية للشركات والمؤسسات أو الجهات الحكومية وذلك باختراق الجدران النارية والتي توضع عادة لحمايتها وغالباً ما يتم ذلك باستخدام المحاكاة.
٢- اختراق الأجهزة الشخصية والعبث بما تحويه من معلومات وهي طريقة للأسف شائعة لسذاجة أصحاب الأجهزة الشخصية من جانب ولسهولة تعلم برامج الاختراقات وتعددها من جانب آخر.
٣- التعرض للبيانات أثناء انتقالها والتعرف على شفرتها إن كانت مشفرة وهذه الطريقة تستخدم في كشف أرقام بطاقات الائتمان وكشف الأرقام السرية للبطاقات البنكية (ATM) وفي هذا السياق يجب الحفاظ على أمرين وهما:

- عدم كشف أرقام بطاقات الائتمان لمواقع التجارة الإلكترونية إلا بعد التأكد بالتزام تلك المواقع بمبدأ الأمان.
- أن البعض عندما يستخدم بطاقة السحب الآلي من آلات البنوك النقدية (ATM) لا ينتظر خروج السند الصغير المرفق بعملية السحب أو أنه يلقى به في أقرب سلة مهملات دون أن يكلف نفسه عناء تمزيقه جيداً، ونظراً إلى ذلك المستند سنجد أرقاماً تتكون من عدة خانات طويلة هي بالنسبة لنا ليست ذات أهمية ولكن في حقيقة الأمر هذه الأرقام ما هي إلا انعكاس للشريط الممغنط الظاهر بالجهة الخلفية للبطاقات البنكية وهذا الشريط حلقة الوصل بيننا وبين رصيد البنك والذي من خلاله تتم عملية السحب النقدي لأدركنا أهمية التخلص من هذا المستند الصغير بطريقة مضمونة ونقصد بالضمان هنا عدم تركها لمخترق يمكنه استخراج رقم الحساب البنكي بل والتعرف على الأرقام السرية للبطاقة البنكية.

كما يمكن تقسيم أنواع الاختراق إلى ما يلي

١- **الدخول إلى النظام والبقاء غير المشروع فيه:** تقع هذه الجريمة من أي إنسان أيا كانت صفته سواء كان يعمل في مجال الأنظمة أم ليست له علاقة بالحاسب الآلي وشبكاته وسواء كانت لدية المقدرة الفنية على الاستفادة من النظام أم لا، إنما فقط يكفي أن يكون له حق الدخول إلى النظام (الشوا، ٢٠٠٣، ص١٧٢)، ومن الممكن التحقق من الدخول متى كان الدخول مخالفاً لإرادة صاحب النظام ومن له حق السيطرة عليه مثل تلك الأنظمة التي تتعلق بأسرار الدولة أو دفاعها أو تتضمن بيانات شخصية تتعلق بحرمة الحياة الخاصة للفرد.

٢- **إعاقة أو تخريب تشغيل نظم معالجة البيانات:** السلوك الإجرامي في هذه الجريمة ينصرف إلى كل عمل من شأنه إرباك عمل نظام معالجة البيانات ويستوي أن يكون من شأن نشاط الجاني إعاقة أو إفشاء نظام التشغيل في الإرسال، كذلك يستوي أن يؤدي نشاط الجاني إلى توقف النظام عن العمل بصورة دائمة أو مؤقتة أو أن يستخدم الجاني في ارتكاب الجريمة أي وسيلة من شأنها أن تعيق سير النظام كالاعتداء المادي أو المعنوي على النظام ومن أمثلة ذلك إعاقة النظام

بطريق مادي هو أعمال العنف المادي على أجهزة الحاسب وشبكة الاتصالات عن طريق تخريبها بكسرها أو سكب أي مادة عليها، أما الإعاقة غير المادية فتكون عن طريق إدخال فيروس للجهاز أو عمل بعض التغييرات على كلمة المرور (حجازى، ٢٠٠٧، ص٣٧١)

٣- **التلاعب في بيانات نظم معالجة البيانات:** النشاط الإجرامي في هذه الصورة من صور الاختراق يتمثل في أفعال الإدخال أو المحو والتعديل ولا يشترط اجتماعها وإنما يكتفي بتوافر إحداهما، فالجريمة في هذه الحالة تقع على المعطيات أو البيانات المعالجة آلياً دون المعلومة ذاتها، لكن القاسم المشترك بين هذه الأفعال جميعاً هو انطواؤها على تلاعب في المعطيات التي يتضمنها نظام معالجة البيانات بإدخال معطيات جديدة أو غير صحيحة أو محو أو تعديلات أخرى قائمة(شافى، ٢٠٠٧، ص٢٧٣).

كما قسم المشرع المصري أنواع جريمة الاختراق إلى: (الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات، وجريمة الدخول غير المشروع، وجريمة تجاوز حدود الحق في الدخول، وجريمة الاعتراض غير المشروع، وجريمة الاعتداء على سلامة البيانات والمعلومات والنظم المعلوماتية، وجريمة الاعتداء على البريد الإلكتروني أو المواقع الخاصة، وجريمة الاعتداء على تصميم موقع)، بينما لم يتطرق كل من المشرع المغربي والإماراتي إلى تقسيم جرائم الاختراق ولكن جرم الاعتداء على النظم الإلكترونية أو المعلوماتية بصفة عامة دون التطرق إلى تقسيم الجرائم ذاتها تاركاً هذه التقسيمات إلى الفقه والقضاء والقواعد العامة في قانون العقوبات(قانون رقم ١٧٥ لسنة ٢٠١٨).

كما يمكن تقسيم أنواع الاختراق إلى ما يلي

٤- **الدخول إلى النظام والبقاء غير المشروع فيه:** تقع هذه الجريمة من أي إنسان أيا كانت صفته سواء كان يعمل في مجال الأنظمة أم ليست له علاقة بالحاسب الآلي وشبكاته وسواء كانت لدية المقدرة الفنية على الاستفادة من النظام أم لا، إنما فقط يكفي أن يكون له حق الدخول إلى النظام (الشوا، ٢٠٠٣، ص ١٧٢)، ومن

الممكن التحقق من الدخول متى كان الدخول مخالفاً لإرادة صاحب النظام ومن له حق السيطرة عليه مثل تلك الأنظمة التي تتعلق بأسرار الدولة أو دفاعها أو تتضمن بيانات شخصية تتعلق بحرمة الحياة الخاصة للفرد.

٥- **إعاقة أو تخريب تشغيل نظم معالجة البيانات:** السلوك الإجرامي في هذه الجريمة ينصرف إلى كل عمل من شأنه إرباك عمل نظام معالجة البيانات ويستوي أن يكون من شأن نشاط الجاني إعاقة أو إفشاء نظام التشغيل في الإرسال، كذلك يستوي أن يؤدي نشاط الجاني إلى توقف النظام عن العمل بصورة دائمة أو مؤقتة أو أن يستخدم الجاني في ارتكاب الجريمة أي وسيلة من شأنها أن تعيق سير النظام كالاعتداء المادي أو المعنوي على النظام ومن أمثلة ذلك إعاقة النظام بطريق مادي هو أعمال العنف المادي على أجهزة الحاسب وشبكة الاتصالات عن طريق تخريبها بكسرها أو سكب أي مادة عليها، أما الإعاقة غير المادية فتكون عن طريق إدخال فيروس للجهاز أو عمل بعض التغييرات على كلمة المرور (حجازى، ٢٠٠٧، ص ٣٧١).

٦- **التلاعب في بيانات نظم معالجة البيانات:** النشاط الإجرامي في هذه الصورة من صور الاختراق يتمثل في أفعال الإدخال أو المحو والتعديل ولا يشترط اجتماعها وإنما يكتفي بتوافر إحداهما، فالجريمة في هذه الحالة تقع على المعطيات أو البيانات المعالجة آلياً دون المعلومة ذاتها، لكن القاسم المشترك بين هذه الأفعال جميعاً هو انطواؤها على تلاعب في المعطيات التي يتضمنها نظام معالجة البيانات بإدخال معطيات جديدة أو غير صحيحة أو محو أو تعديلات أخرى قائمة(شافى، ٢٠٠٧، ص ٢٧٣).

كما قسم المشرع المصري أنواع جريمة الاختراق إلى: (الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات، وجريمة الدخول غير المشروع، وجريمة تجاوز حدود

الحق في الدخول، وجريمة الاعتراض غير المشروع، وجريمة الاعتداء على سلامة البيانات والمعلومات والنظم المعلوماتية، وجريمة الاعتداء على البريد الإلكتروني أو المواقع الخاصة، وجريمة الاعتداء على تصميم موقع)، بينما لم يتطرق كل من المشرع المغربي والإماراتي إلى تقسيم جرائم الاختراق ولكن جرم الاعتداء على النظم الإلكترونية أو المعلوماتية بصفة عامة دون التطرق إلى تقسيم الجرائم ذاتها تاركاً هذه التقسيمات إلى الفقه والقضاء والقواعد العامة في قانون العقوبات(قانون رقم ١٧٥ لسنة ٢٠١٨).

المبحث الثاني: أسباب اختراق النظم الإلكترونية وأثارها وحمايتها

المطلب الأول: أسباب اختراق النظم الإلكترونية

هناك أسباب كثيرة لوقوع عملية اختراق النظم الإلكترونية ومنها الآتي:(المشد، ٢٠١٧، ص ٣٤٥)

١- استخدام كلمات سر ضعيفة يمكن تخمينها ومن ثم التأثير سلباً باختراق النظم الإلكترونية.

٢- عدم استخدام الأنظمة الإلكترونية برامج وقائية لحمايتها من القراصنة والهاكرز أو عدم التحديث لبعض البرامج التي تعمل على التنبيه في حالة وجود اختراق للنظم الإلكترونية.

٣- لجوء بعض الأنظمة إلى برامج أو شركات ضعيفة في مجال تأمين الدعم الفني وبالتالي تتعرض تلك الأنظمة لخطر الاختراق.

٤- عدم اهتمام الأنظمة بعملية التحديث المستمر لنظم التشغيل والتي تكتشف في كثير من الأحيان وجود مزيد من الثغرات الأمنية لهذه الأنظمة وبالتالي فلابد من القيام بسد تلك الثغرات من خلال برامج تنتجها شركات متخصصة لمواجهة عملية القرصنة أو الاختراق.

٥- عدم القيام بالنسخ الاحتياطي لقواعد البيانات المرتبطة بالأنظمة مما يعرض جميع المعلومات الموجودة في تلك القواعد للضياع وعدم الاسترجاع لذا تجدر الإشارة لأهمية وجود نسخة احتياطية لقواعد البيانات ومحتوياتها في ظل تفاقم مشكلة الاختراقات، ويعد

عام ٢٠٠٢ من أكثر الأعوام اختراقاً فقد تضاعفت حالات الاختراق والتدمير لوجود ثغرات أمنية في النظم الإلكترونية، وانتشار كثير من الفيروسات.

المطلب الثاني: أثار اختراق النظم الإلكترونية ووسائل وحمايتها.

أ- أثار اختراق النظم الإلكترونية:(أحمد، ٢٠١٥، ص١٤)

١- تغيير الصفحة الرئيسية لموقع الويب كما حدث لموقع قناة الجزيرة الفضائية مؤخراً إثر عرضها لصور الأسرى الأمريكيين على شاشتها وموقعها حيث قامت جهة ما باختراق موقعها ونظامها وتعطيلهما وغيرت الصفحة الرئيسية لها بصورة العلم الأمريكي.

٢- السطو بقصد الكسب المادي كتحويل حسابات البنوك أو الحصول على خدمات مادية أو معلوماتية كأرقام بطاقات الائتمان والأرقام السرية الخاصة بالبطاقات البنكية (ATM).

٣- اقتناص كلمات السر التي يستخدمها الشخص للحصول على خدمات مختلفة كالدخول إلى الإنترنت حيث يلاحظ الضحية أن ساعاته تنتهي دون أن يستخدمها وكذلك انتحال شخصية في منتديات الحوار، أو الاستيلاء على بريد شخص ما.

٤- آثار فردية مما يترتب على الفرد من انتهاك الخصوصية وسرقة بياناته ومعلوماته.

٥- آثار اجتماعية حيث يترتب على الاختراق العديد من الأضرار الاجتماعية مثل نشر الرذيلة والاتجار بالمخدرات والاتجار بالأطفال والنساء.

٦- آثار مجتمعية وهي ما ترتبط بالحفاظ على الدولة ككل مثل التعدي على الأمن القومي الداخلي أو الخارجي.

٧- آثار إدارية مثل تدمير النظم الإدارية الإلكترونية للدولة أو المؤسسات الخاصة.

٨- يؤدى الاختراق إلى تدمير البنية التحتية المعلوماتية للدولة.

ب- وسائل حماية النظم الإلكترونية من جرائم الاختراق.

١- خلق أجهزة دولية متخصصة هدفها مراقبة شبكات الاتصال ومهمتها الكشف عن الفيروسات التي تروج عبر الشبكات والعمل على ضبط المخالفات في هذا الميدان وهكذا في حالة انتشار الفيروسات عبر شبكات الاتصال ومعرفة مصدره والعمل على الكشف عن الشخص أو الجهة المروجة له وتقديمها للجهات المكلفة بالمحاكمة، وعليه فإنه يمكن القول بأن عمل هذه اللجان يشبه إلى حد ما عمل اللجان الدولية، إلا أن هذه

اللجان تمتاز بكونها تشمل عناصر فنية متخصصة في ميدان النظم الإلكترونية وتكنولوجيا المعلومات، الشيء الذي يتيح لها العمل للتمكن من حماية المعلومات الإلكترونية من الانتهاكات التي ترتكب عبر شبكات الاتصال، والتي يتم من خلالها الاعتداء على الأنظمة(محمود، ٢٠٠٥).

٢- التأكد دائماً من وجود الحماية للنظم الإلكترونية، وتأمين حسابات المستخدمين ونظم التحقيق من الهوية(المشد، ٢٠١٧، ص٣٨٠).

٣- الحماية المادية والإدارية والشخصية للنظم الإلكترونية.

٤- العمل على ترتيب إجراءات هيكلية من أجل مكافحة جرائم الاختراق التي ترتكب ضد النظم الإلكترونية عبر الشبكة المعلوماتية

٥- التعاون على المستوى المحلي والإقليمي والدولي لمكافحة جرائم اختراق النظم الإلكترونية

٦- تنمية الوعي الثقافي للمجتمعات من خلال تدريب أفراده ومؤسساته على أساليب التعامل مع وسائل التقنية الحديثة.

٧- التنسيق والشراكة بين مختلف الأجهزة الرسمية وغير الرسمية لمكافحة جرائم اختراق النظم الإلكترونية.

وسائل الحماية القانونية للنظم الإلكترونية في التشريع المصري:

جاء المشرع المصري بالقانون رقم ٨٢لسنة٢٠٠٢ لحماية حقوق الملكية الفكرية والحقوق المجاورة ففرض أسلوباً تقنيا جديداً للحماية الجنائية الفعلية لأصحاب الحقوق على المصنفات وذلك بمنع أي اعتداء على أي حق أدبي أو مالي من حقوق المؤلف أو الحقوق المجاورة في هذا القانون(رشدى، ٢٠٠٤، ص٣٥).

فقد نص المشرع المصري في ذلك القانون في المادة (١٨١) على أنه: "مع عدم الإخلال بأية عقوبة أشد في قانون آخر يعاقب بالحبس مدة لا تقل عن شهر وبغرامة لا تقل عن خمسة آلاف جنيه ولا تتجاوز عشرة آلاف جنيه أو بإحدى هاتين العقوبتين كل من ارتكب إحدى الأفعال الآتية:(عبد السلام، ٢٠٠٤، ص١٢٣)

أ) التصنيع أو التجميع أو الاستيراد بغرض البيع أو التأجير لأي جهاز أو وسيلة أو إدارة معدة للتحايل على حماية تقنية يستخدمها المؤلف أو صاحب الحق المجاور كالتشفير وغيره.

ب) الإزالة أو التعطيل أو التخريب بسوء نية لأية حماية تقنية يستخدمها المؤلف أو صاحب الحق المجاور كالتشفير وغيره)، وبالإطلاع على هذا النص يتضح أنه يتفق مع الالتزامات

القانونية التي نصت عليها اتفاقية الوايبو سنة ١٩٩٦ ومع التوجه الأوربي رقم ٢٩لسنة٢٠٠١ في مادته السادسة في شأن حقوق المؤلف حيث لم يكتف بصور الاعتداء التقليدي على المصنف بل أضاف صورًا أخرى للاعتداء تتناسب مع طبيعة التقدم الهائل في مجال المعلوماتية.

حيث جاءت المادة (١٢) من اتفاقية الوايبو سنة ١٩٩٦ لتفرض عقوبات ضد أي عبث متعمد بمعلومات إدارة الحقوق في مواجهة ما يسمى الطريق السريع للمعلومات، وهو ما تضمنه أيضا التوجه الأوربي رقم ٢٩ لسنة ٢٠٠١ في شأن حقوق المؤلف في المادة السادسة منه.

وبالرجوع لنصوص القانون رقم ٨٢لسنة٢٠٠٢ الخاص بحماية الملكية الفكرية المصري نجده قد خلا من تجريم أفعال الاعتداء على معلومات إدارة حقوق المؤلف وهو ما يؤخذ على المشرع المصري فلا بد من النص على جزاءات فعالة تتماشى مع ما نصت عليه اتفاقية الوابيو سنة ١٩٩٦ في شأن جريمة الاعتداء على معلومات إدارة الحقوق (الصباغ، ٢٠١٦، ص١١١).

حيث نصت المادة (٣١) من الدستور المصري الصادر عام ٢٠١٤ على الآتي: "أمن الفضاء المعلوماتي من منظومة الاقتصاد والأمن القومي وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه على النحو الذي ينظمه القانون"، لذلك تدارك المشرع المصري الفراغ التشريعي ونص على هذه الحماية بالقانون رقم ١٧٥لسنة٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات، ونص في المادة (١٣) من هذا القانون على الآتي: "يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز خمسين ألف جنيه أو بإحدى هاتين العقوبتين، كل من انتفع بدون وجه حق عن طريق شبكة النظام المعلوماتي أو إحدى وسائل تقنية المعلومات بخدمة اتصالات أو خدمة من خدمات قنوات البث المسموع أو المرئي". (المادة ١٣ من القانون المصرى رقم ١٧٥ لسنة ٢٠١٨)

كما نصت المادة (١٤) من القانون المصري رقم ١٧٥لسنة٢٠١٨ على الآتي: "يعاقب بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن خمسين ألف جنيه ولا تتجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين كل من دخل عمداً أو دخل بخطأ غير عمدي وبقي بدون وجه حق على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه".(المادة ١٣ من القانون المصرى رقم ١٧٥ لسنة ٢٠١٨)

كـذلك جـرم المشـرع المصـري فـي المـواد (١٥،١٦،١٧) مـن القـانون رقـم ١٧٥لسنة٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات، تعدي حدود حق الدخول من حيث الزمان والمكان أو الاعتراض بدون وجه حق على أي معلومات أو بيانات أو كل ما هو متداول عن طريق شبكة معلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها أو عطل أو أتلف أو عدل مساراً أو ألغى كلياً أو جزئياً متعمداً أو بدون وجه حق البرامج والبيانات أو المعلومات المخزنة أو المعالجة أو المولدة أو المخلقة على أي نظام معلوماتي وما في حكمها، أيا ما كانت الوسيلة المستخدمة في ارتكاب الجريمة وبذلك يكون المشرع المصري جرم الاعتداءات على إدارة الحقوق والنظم والمعلومات.

ومما سبق نجد أن المشرع المصري تبنى الاتجاه التشريعي المختلط وهو الحماية القانونية للمعلومات وكذلك أنظمة المعلومات وشبكات المعلومات وهذا الاتجاه وهو ذات الاتجاه الذي سار عليه المشرع الفرنسي والمشرع المغربي والمشرع الإماراتي.

وسائل الحماية القانونية للنظم الإلكترونية في التشريع المغربي:

تُعد حماية الحقوق بمثابة وسيلة مناسبة للإفصاح الفعال عن المعرفة الحديثة بما يؤدي إلى مزيد من الرفاهية الاقتصادية والاجتماعية، كما يؤدي إلى تشجيع الاستثمار الداخلي وجلب الاستثمار الخارجي ليساعد على تحقيق الرخاء ويعمل على دفع عجلة النمو الاقتصادي(محمود، ٢٠٠٠، ص٨٣)، الأمر الذي يوضح العلاقة الوطيدة التي تربط المعلوماتية بالاستثمار (رزق، ٢٠٠٠، ص١٨٧)، بل أصبح يقابل هذه الحقوق جرم أخلاقي واجتماعي في حرمان يكمن في الاعتداء على الحقوق المعنوية والمادية للنظم الإلكترونية التي هي نتاج فكر ونبض وعرق أصحابها(غالى، ٢٠٠٠، ص٨)، ويتمثل هذا الجرم في إفشاء معطيات برامج الحاسوب والاعتداء عليها بالقرصنة أو الاستغلال غير المشروع وهذا ما يعد ضرباً حقيقياً ليس فقط لحقوق مبتكريها الخاصة، بل أيضا مساس خطير بحقوق المجتمع ككل، إلى جانب ما ينتج عنه من تأثيرات سلبية على الاقتصاد الوطني وعلى خلخلة أركان الأمن الاجتماعي(النية، ٢٠٠٢، ص ٦٤)، كما أن هذه الاعتداءات التي قد تمس النظم الإلكترونية ومنها التبادل الإلكتروني للمعطيات قد تتطابق والنموذج القانوني لإحدى الجرائم المنصوص عليها في قانون حق المؤلف (قانون حماية الملكية الأدبية والفنية).

نتج عن ذلك أن شمل المشرع المغربي النظم الإلكترونية بالحماية بالقانون رقم (٠٥-٣٤) في ١٤فبراير٢٠٠٦ بظهير شريف رقم (١,٠٥,١٩٢) بتغيير وتتميم القانون رقم

(٢,٠٠) المتعلق بحماية حقوق المؤلف والحقوق المجاورة والذي نصت المادة (٦٥) من ذلك القانون المشار إليه الحماية الجنائية الخاصة بالمعطيات من خلال حق المؤلف، فلقد قام المشرع المغربي بإلغاء الظهير الشريف رقم ٢٩لسنة١٩٧٠ بشأن حماية حق المؤلفات الأدبية والفنية، وذلك بمقتضى الظهير الشريف رقم (١,٠٠,٢٠) الصادر في ١٥فبراير ٢٠٠٠ بتنفيذ القانون رقم (٢,٠٠) المتعلق بحقوق المؤلف والحقوق المجاورة، لكن هذا القانون شابه بعض القصور، حيث أغفل التنصيص على السرقة عن طريق التحميل، وإعمالاً لمبدأ الشرعية الجنائية تدارك المشرع المغربي هذا الفراغ ثم قام المشرع المغربي بعد ذلك بإصدار القانون رقم (٠٥-٣٤) المتعلق بحقوق المؤلف والحقوق المجاورة والقاضي بتتميم وتغيير القانون رقم (٠٠-٠٢) وكان هذا النص الخاص بالفعل محاولة من المشرع المغربي لمواكبة المد الإجرامي المتعلقة بالتحميل اللامشروع وإعادة البيع للبرامج أو تأجيرها أو استغلالها.

وباستقراء القانون المشار إليه نجد أن المشرع شمل بالحماية في البند السابع عشر من المادة الأولى، ونص المشرع المغربي في الفقرة الثانية من المادة الثالثة من هذا القانون على استفادة برامج الحاسوب من الحماية المقررة للمصنفات الأدبية والفنية، وبذلك فإن حماية برامج الحاسوب في القانون المغربي أصبحت بمقتضى نص القانون حسماً للتأويلات الفقهية والاجتهادات القضائية(بوسيبة، ٢٠١٠، ص٨٦)، والمقصود بالحماية برامج التشغيل والتي يطلق عليها عادة برامج الاستغلال التي تمكن الحاسوب من أداء وظيفته المحددة له والتي تعتبر بالتالي جزءاً من الجهاز، بل يتعلق الأمر ببرامج التطبيق التي تستهدف تحقيق نتيجة معينة وتبدأ حماية الحقوق التي تترتب على المصنف بمجرد إنجازه البرنامج ولمدة خمس وعشرين سنة.(غالى، ٢٠٠١، ص١٣)

يرى بعض من الفقهاء أن هناك برامج تم تصميمها خصيصاً لحماية هذه المصنفات، لذلك فالمساس بهذه الأنظمة يشكل اعتداء خطيراً معاقباً عليه، ويمكن إجمال هذه الاعتداءات في صورتين(رزق، ٢٠١٦، ص١٣٠): **أولهما:** جريمة فض مفاتيح التشفير، **وثانيهما:** جريمة المس بالبيانات المشفرة.

ويؤخذ على هذا الرأي أنه حصر جرائم الاعتداء على النظم الإلكترونية فقط فض مفاتيح التشفير ولكن هناك جرائم كثيرة نذكر منها القرصنة والسرقة والإتلاف والاعتراض وكذلك عرقلة سير النظام والدخول غير المشروع والبقاء غير المشروع والتزوير والتزييف.

بعد ذلك استشعر المشرع المغربي الحاجة إلى إسدال الحماية الجنائية على الجرائم التي تستهدف المس بسرية وسلامة الأنظمة المعالجة آلياً للمعطيات وكذلك الجرائم التي تنتهك المعطيات (البيانات) والوثائق المعلوماتية عن طريق الإخلال بسيرها والاعتداء عليها، سواء من خلال الولوج إلى هذه الأنظمة عن طريق الاحتيال أو البقاء غير المشروع فيها أو ما يسمى "بالها كينغ" أو من خلال عرقلة سير نظام المعالجة الآلية أو إحداث خلل فيها نظراً لاستفحال هذه الفئة من الجرائم في المملكة المغربية على غرار باقي دول العالم(سليمان، ٢٠١٧، ص٧١).

لذا لم يكن المشرع المغربي بمنأى عن التوجه الذي سار فيه المجتمع الدولي، فقد سن سنة ٢٠٠٣ القانون رقم (٠٧٠٣) المتعلق بالمس بنظم المعالجة الآلية للمعطيات وكذلك بعض القوانين ذات الصلة بالموضوع نذكر منها قانون (٠٩٠٨) المتعلق بمعالجة المعطيات ذات الطابع الشخصي وكذلك إدخال تعديلات على قانون المسطرة الجنائية بموجب القانون رقم (٥٣) ليتماشى مع خصوصية الإجرام المعلوماتي، حيث جرم المشرع الدخول غير المشروع للنظام بالمادة (٠٣/٦٠٧) على أنه يعاقب بالحبس من شهر إلى ثلاثة أشهر وبالغرامة من (٢٠٠٠-١٠٠٠٠) درهم أو بإحدى العقوبتين فقط كل من دخل إلى مجموعة أو بعض نظم للمعالجة الآلية للمعطيات عن طريق الاحتيال(قانون رقم ٣- ٧، ٢٠٠٣).

أما بخصوص جريمة عرقلة سير نظام المعالجة الآلية يمكن تعريفها بأنها: "الحول دون أداء النظام لوظيفته بشكل منتظم وعادي" حيث يتمثل الركن المادي لهذه الجريمة في إعاقة أو تشويه عمل النظام المبرمج للبيانات، وذلك بتحطيم أو تعطيل وحدة التخزين المركزية أو تخريب الدعامات المنسوخ عليها المعلومات أو إفراغ كأس قهوة على الكمبيوتر، وقد تأخذ العرقلة شكلاً غير مادي حينما يلجأ المتهم إلى الهجوم على النظام عن بعد كتدمير الملفات أو البرامج المعلوماتية قصد إعاقة النظام عن طريق إدخال الفيروسات.

والمشرع المغربي اكتفى بذكر عبارة "عرقلة سير النظام أو إحداث خللٍ فيه" دون أن يحدد تشريعياً صور هذه العرقلة، إذ نص الفصل (٦٠٧-٥) على أنه يعاقب بالحبس من سنة إلى ثلاث سنوات وبالغرامة من (١٠٠٠٠-٢٠٠٠٠) درهم أو بإحدى هاتين العقوبتين كل من عرقل عمداً سير نظام المعالجة الآلية أو أحداث خللاً فيه.

وهو توجه يمنح للقاضي سلطة تقديرية واسعة في إدخال كل سلوك بإمكانه عرقلة سير النظام أو إحداث خلل فيه وهذا أمر من شأنه الإخلال بمبدأ الشرعية الجنائية الذي

يقضي بضرورة تحديد وحصر الأفعال الجنائية المجرمة حتى يكون الشخص على بينة من أمره(سليمان، ٢٠١٧، ص٨٤).

يمكن القول بأن المشرع المغربي عندما جرم عرقلة سير نظام المعالجة الآلية أو إحداث خلل فيه أحسن صنعاً في عدم تحديد صور العرقلة لأن العرقلة يمكن أن تتم بصور كثيرة وغير محددة بسبب التقدم المتسارع في التكنولوجيا تاركاً ذلك للسلطة التقديرية للقضاء حيث أن المشرع أراد فرض الحماية للنظام أياً ما كانت صور الاعتداء.

المراجع:

أبوسكى، بيتر نمر(٢٠٠٦): **جرائم الحاسب الآلي الأبعاد الدولية**، ورقة عمل مقدمة بندوة شبكات الإنترنت وتأثيراتها الاجتماعية والأمنية، مركز البحوث والدراسات الأمنية شرطة أبوظبي، الإمارات العربية المتحدة.

أحمد، هالة كمال(٢٠١٥): **جرائم اختراق البيئة المعلوماتية واستشراف الاتجاهات الحديثة في مجال أمن المعلومات، دراسة إبستيمولوجية في ضوء آراء عينية من المتخصصين**، المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية، كلية علوم الحاسب والمعلومات، جامعة الإمام محمد بن سعود، المملكة العربية السعودية.

أنظر: المادة (١٣) من القانون المصري رقم ١٧٥لسنة٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات.

أنظر: المادة (١٤) من القانون المصري رقم ١٧لسنة٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات.

أنظر: المادة الأولى من القانون المصري رقم ١٧٥لسنة٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات، الجريدة الرسمية، العدد (١٤)، ٣١-٨-٢٠١٨.

أنظر: المواد (١٣-١٩) من قانون رقم ١٧٥لسنة٢٠١٨، بشأن مكافحة جرائم تقنية المعلومات.

أنظر: قانون رقم (٠٣-٠٧) مجموعة القانون الجنائي فيما يتعلق بالجرائم المتعلقة بنظم المعالجة الآلية للمعطيات، والمادة (٦٠٧-٠٣)، منشور في الجريدة الرسمية عدد (٥١، ٧١)، ٢٠٠٣/١٢/٢٢.

أنظر: قانون رقم (٠٣-٠٧) مجموعة القانون الجنائي فيما يتعلق بالجرائم المتعلقة بنظم المعالجة الآلية للمعطيات.

حجازي، عبد الفتاح(٢٠٠٩): **نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي**، منشأة المعارف، ط١، الإسكندرية.

حنفي، وليد إبراهيم (٢٠١٧): **عقد إنتاج المعلومات الإلكترونية، دراسة مقارنة**، دار النهضة العربية، ط١، القاهرة.

داود، حسن طاهر(٢٠٠٠): **جرائم نظم المعلومات**، أكاديمية نايف للعلوم الأمنية، الرياض، المملكة العربية السعودية.

رزق، عبد الحكيم(٢٠٠٠): **المعلوماتية والاستثمار: أية علاقة؟**، مجلة الحقوق المغربية، العدد (١٠).

رزق، عبد الحكيم(٢٠١٦): **الجرائم المعلوماتية في التشريع المغربي**، منشورات الشؤون القانونية والمنازعات مرصد الدراسات والأبحاث، دار القلم للطباعة والنشر والتوزيع، ط١، الرباط.

رشدي، محمد السيد(٢٠٠٤): **الإنترنت والجوانب القانونية لنظم المعلومات**، دار النهضة العربية، القاهرة.

الزنط، سعد عطواة:(٢٠١٠) **الإرهاب الإلكتروني وإعادة صياغة إستراتيجيات الأمن القومي**، مقدمة إلى مؤتمر الجرائم المستحدثة كيفية إثباتها ومواجهتها، المنعقد في الفترة من ١٥-٢٠١٠/١٢/١٦، المركز القومي للبحوث الاجتماعية والجنائية، القاهرة.

السويد، عبد اللطيف بن صالح(٢٠٠٩): **جريمة الاختراق الإلكتروني وعقوبتها، دراسة مقارنة**، رسالة ماجستير، المعهد العالي للقضاء، جامعة الإمام محمد بن سعود الإسلامية، المملكة العربية السعودية.

سويلم، محمد على(٢٠١٨): **الحماية الجنائية للمعاملات الإلكترونية**، دار المطبوعات الجامعية، ط١، الإسكندرية.

شافي، نادر عبد العزيز(٢٠٠٧): **نظرات في القانون**، منشورات زين الحقوقية، بيروت، لبنان.

الصباغ، أسامة فرج الله محمود (٢٠١٦): **الحماية الجنائية للمصنفات الإلكترونية**، دار الجامعة الجديدة، الإسكندرية.

عباس، إسلام عبد الله محمد(٢٠١٠): **أمن المعلومات على شبكة الانترنت واستخدام طريقة حقن لغة الاستعلام الهيكلية في اختراق قواعد بيانات المواقع الإلكترونية**، أطروحة دكتوراه، كلية الدراسات العليا، جامعة النيلين، السودان.

عبد الحميد، محمد(٢٠٠٧): **الاتصال والإعلام على شبكة الإنترنت**، عالم الكتب، القاهرة.

عبد السلام، سعيد سعد(٢٠٠٤): **الحماية القانونية لحق المؤلف والحقوق المجاورة في ظل قانون حماية حقوق الملكية الفكرية رقم ٨٢لسنة٢٠٠٢**، دار النهضة العربية، القاهرة.

العبيدي، أسامة بن غانم(٢٠١٢): **جريمة الدخول غير المشروع إلى النظام المعلوماتي، دراسة قانونية في ضوء القوانين المقارنة**، مجلة دراسات المعلومات، عدد (١٤).

عتيق، السيد(٢٠٠٢): **جرائم الإنترنت**، دار النهضة العربية، ط١، القاهرة، ص٢٤، وجميل عبد الباقي الصغير: **الإنترنت والقانون الجنائي، الأحكام الموضوعية للجرائم المتعلقة بالإنترنت**، مرجع سابق، ٢٠٠١، ص٤، ومدحت عبد الحليم رمضان: **جرائم الاعتداء على الأشخاص والإنترنت**، مرجع سابق، ٢٠٠٠، ص٣٠.

غالي، عبد الكريم(٢٠٠١): **إشكالية حماية البرامج المعلوماتية على ضوء القانون المتعلق بحقوق المؤلف والحقوق المجاورة الصادر في ١٥ فبراير ٢٠٠٠**، مجلة كتابة الضبط، العدد (٩).

غمارسة، منية بنت ترديات (٢٠١٥): **جرائم المعلوماتية في القانون التونسي، والقانون المقارن، والقانون الدولي**، لامنيرون للنشر والتوزيع.

غنية، باطلي(٢٠١٥): **الجريمة الإلكترونية، دراسة مقارنة**، بحث منشور، منشورات الدار الجزائرية، الجزائر.

القانون رقم (١٧٥) لسنة٢٠١٨، بشأن مكافحة جرائم تقنية المعلومات، الجريدة الرسمية، العدد (٣٢مكرر)، السنة (٦١)، القاهرة.

قورة، نائلة عادل محمد فريد(٢٠٠٥): **جرائم الحاسب الآلي الاقتصادية، دراسة نظرية تطبيقية**، منشورات الحلبي الحقوقية، ط١، بيروت، لبنان.

محمود، جميل زكريا(٢٠٠٥): **الفيروسات وطرق الوقاية منها كوسيلة لأمن البيانات**، ورقة عمل مقدمة للمؤتمر الدولي حول أمن المعلومات نحو تعامل رقمي آمن، المنعقد في مسقط، عمان.

محمود، ياسر محمد جاد الله(٢٠٠٠): **حماية حقوق الملكية الفكرية والنمو الاقتصادي في مطلع القرن القادم**، مجلة آفاق الاقتصادية، مركز البحوث والتوثيق، المجلد (٢١)، العدد (٨٤)، دولة الإمارات العربية المتحدة.

مرسوم رقم (٥)لسنة٢٠١٣ بشأن قانون مكافحة جرائم تقنية المعلومات الإماراتي، ط١، دائرة قضاء أبوظبي.

المري، بهاء(٢٠١٩): **شرح قانون مكافحة جرائم تقنية المعلومات وحجية الدليل الرقمي في الإثبات**، العربية للنشر والتوزيع، القاهرة.

المشد، أحمد(٢٠١٧): **القرصنة الإلكترونية وأمن المعلومات**، مؤسسة الأمة العربية للنشر والتوزيع القاهرة.

المصري، هشام (٢٠١٩): الأمن **المعلوماتي أحد الأعمدة الرئيسية للأمن القومي (اختراقه – احتوائه)**، دار الوفاء القانونية، ط١، الإسكندرية.

المهادي، عادل(٢٠١٠): **الجريمة المعلوماتية، جريمتا الدخول غير المشروع وإتلاف المعطيات، دراسة مقارنة في التشريع المغربي والتشريع المُقارن**، رسالة ماجستير، كلية العلوم القانونية والاقتصادية والاجتماعية، جامعة القاضي عياض، مراكش، المملكة المغربية.

النية، بشرة(٢٠٠٢): الحماية الجنائية لبرامج الحاسوب، دراسة مقارنة، رسالة ماجستير، كلية العلوم القانونية والاقتصادية والاجتماعية، جامعة محمد الخامس، الرباط.

() Millard (Christopher): "Copyright"، in Chris Reed & John Angel (eds), Computer law, 2000,p.201; Short (Greg), Combating Piracy: Can Felony Penalties for Copyright Infringement Curtail the Copying of computer Software?, S.C.C.H.T.L.J.,1994, vol.10, p. 221.