جامعة الأزهر
كلية الشريعة والقانون
بالقاهرة

مجلة الشريعة والقانون

مجلة علمية نصف سنوية محكمة

تعنى بالدراسات الشرعية والقانونية والقضائية

تصدرها

كلية الشريعة والقانون بالقاهرة

جامعة الأزهر

العدد الخامس والأربعون

مايو ٢٠٢٥م

توجه جميع المراسلات باسم الأستاذ الدكتور: رئيس تحرير مجلة الشريعة والقانون

جمهورية مصر العربية – كلية الشريعة والقانون – القاهرة – الدراسة – شارع جوهر القائد

ت: 201221067852+

ت: 201028127441+

البريد الالكتروني

Journal.sha.law@azhar.edu.eg

جميع الآراء الواردة في هذه المجلة تعبر عن وجهة نظر أصحابها، ولا تعبر بالضرورة عن وجهة نظر المجلة وليست مسئولة عنها

رقم الإيـــداع

٢٠٢٥ / ١٨٠٥٣

الترقيم الدولي للنشر

ISSN: 2812–4774

الترقيم الدولي الإلكتروني

ISSN: 2812–5282

الموقع الإلكتروني

https://mawq.journals.ekb.eg/

المسؤولية الجنائية تجاه إرسال البرمجيات الخبيثة
دراسة في التشريعات المقارنة

Criminal liability for Sending Malware
A Study in Comparative Legislation

إعداد

د. عبد العزيز منصور الميل

أكاديمية سعد العبد الله للعلوم الأمنية
وزارة الداخلية الكويت - دولة الكويت

المسؤولية الجنائية تجاه إرسال البرمجيات الخبيثة
دراسة في التشريعات المقارنة

عبد العزيز منصور الميل

قسم القانون العام، أكاديمية سعد العبد الله للعلوم الأمنية، وزارة الداخلية، دولة الكويت.

البريد الإلكتروني: aziz@almailgroup.com

ملخص البحث:

هدفت الدراسة الحالية إلى السعى نحو بلورة عناصر المسؤولية الجنائية تجاه إرسال البرمجيات الخبيثة في التشريعات المقارنة.

وقد خلصت الدراسة للنتائج التالية:

١. تعتبر جريمة إعاقة الوصول إلى الخدمات الإلكترونية من الجنح التي تتمثل بتعطيل الوصول أو إعاقة الوصول إلى الخدمات الإلكترونية أو الأجهزة أو البرامج أو المعلومات الإلكترونية.

٢. هناك العديد من البرمجيات الخبيثة Malware التي تستهدف تعطيل الأجهزة الإلكترونية أو الحواسيب، وجميع أشكالها وأنواعها تقع بها الجريمة.

٣. حاول المشرع توفير هذه الحماية للبرامج الإلكترونية انطلاقا من حق المستخدم في الوصول إلى الجهاز الإلكتروني الخاص أو الخدمات الإلكترونية.

خلصت الدراسة لتقديم التوصيات التالية:

١. حماية البرامج من البرمجيات الخبيثة Malware لدى المستخدمين من خلال رفع مستويات الأمان في الحواسيب على اختلاف أنواعها.

٢. ضرورة المراجعة الدورية للتشريعات الجزائية القائمة وإزالة أي غموض أو ثغرات من الممكن أن يستغلها الجناة للإفلات من العقاب.

الكلمات الدالة: المسؤولية الجنائية، البرمجيات الخبيثة، التشريعات المقارنة.

Criminal liability for Sending Malware
A Study in Comparative Legislation

Abdul Aziz Mansour El Mel
Public Law Department , Saad Al Abdullah Academy for Security Sciences, Ministry of Interior Kuwait, The State of Kuwait.
E-mail: aziz@almailgroup.com

Abstract:

The current study aimed to seek to develop elements of criminal responsibility towards the sending of malware in comparative legislation.

The study concluded as follows:

1. The crime of obstructing access to electronic services is a misdemeanor, which is to disable access or obstruct access to electronic services, devices, software or electronic information.

2. There are many malware malware malware aimed at disabling electronic devices or computers, and all forms and types are subject to crime.

3. The legislator tried to provide this protection for electronic programs starting from the security of the user's right to access the private electronic device or electronic services, and you disable or obstruct access to electronic devices, electronic network and accessories constitutes an attack on this right.

The study concluded with the following recommendations:

1. Protect programs from malware in users by raising the levels of security in computers of all kinds Avoiding unsafe websites, making sure antivirus software and operating systems are up to date, and making sure firewalls are turned on. Not to open an email or attachment from unknown persons, Activate IDS and IPS intrusion detection systems at the network level, and activate ad blocker applications.

2. The need to periodically review existing penal legislation and remove any ambiguities or loopholes that may be exploited by perpetrators of impunity.

3. Strengthen international cooperation in combating cybercrime, with a view to bringing together national penal laws, collecting evidence and extraditing criminals, and exchanging experiences and information in this regard.

Keywords: Criminal Liability, Malware, Comparative Legislation.

المبحث التمهيدي
الإطار العام للدراسة

مقدمـــة

يعرف البرنامج الضار الخبيث (Malicious Software) وتكتب اختصارا Malware بأنه برنامج حاسوبي تم تطويره بشكل خبيث ليتم تثبيته على أجهزة الحاسوب دون موافقة المستخدمين. وتهدف هذه البرمجيات إلى تعطيل الأجهزة الإلكترونية أو أجهزة الحاسب الآلي كالاستحواذ على مساحة القرص الصلب أو على جزء من المعالج Processor، أو تخريب البيانات، وإظهار رسائل مزعجة على شاشة المستخدم، أو رصد لوحة مفاتيح المستخدم ومعرفة ما يكتب المتجسس على المستخدمين، كذلك إرسال رسائل بريدية غير مرغوب فيها لجهات اتصال المستخدم، وقد يشمل معرفة استراتيجيات العمل وتخريب النظام الخاص بالعمل وغيرها، ويستخدم أحياناً مصطلح الفيروسات (viruses) بوصفه مصطلحا عاما عوضاً عن البرمجيات الخبيثة (Malicious Malware) لأن الفيروس يعتبر نوعاً من أنواع البرامج الخبيثة.

وقد تأتي البرمجيات الخبيثة Malware بأشكال عديدة تحت أسماء متنوعة وأكثرها شيوعًا هي الفيروسات (viruses)، والديدان (worms)، وأحصنة طروادة Trojan (horses). والجذور الخفية (Root kit)، وبرامج التجسس (Spyware)، وبرامج الإعلانات المتسللة (Adware)، والبرمجيات التخريبية (Scareware)، وبرمجيات خاطفة المتصفح Browser Hijacker). ويعد فيروس الحاسوب أحد أكثر المصطلحات المعروفة في عالم الأمن الإلكتروني مثل أي فيروس بيولوجي خطير ينذر العلماء ، وأن المصطلح «فيروسات الحاسوب» يجلب الخوف للمسؤولين أو مستخدمي أي نظام حاسوبي (Pfleeger et al.196 ، ١٥

وقد كانت شبكات المعلومات – وفي مقدمتها الإنترنت العنوان الجديد لعصر المعلومات قد أتاحت وتتيح التبادل الواسع لمختلف أنماط المعلومات، كما تتيح التراسل الفوري، وفي الوقت ذاته خلقت بيئة للاستثمار والأعمال فيما يعرف بالأسواق الافتراضية أو

بيئة الأعمال الإلكترونية [١]. ولأن تقنية المعلومات عموماً، أفرزت ولا تزال تفرز تحديات قانونية، فإن الجهات التشريعية والقانونية في النظم المقارنة أولت آثار تقنية المعلومات على النظم القانونية عناية استثنائية وذلك لإيجاد البيئة الملائمة لضمان سلامة استخدام التقنية وتشجيع اعتمادها)[٢] . ومن بين أكثر التحديات القانونية إثارة للجدل وتأثيراً على الثقة بالتقنية وتطبيقاتها فكرة المسئولية الجنائية عن المساس بالأفراد والمؤسسات عند إساءة

(١) المركز الوطني للمعلومات بالجمهورية اليمنية، مادة معلوماتية عن الأعمال الإلكترونية وأمن المعلومات، مارس ٢٠٠٥ ، ص ٢١.

(٢)د/ هشام محمد فريد رستم قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، ١٩٩٢، ص١٨٠ . يعرف الحق في الخصوصية أو كما يعرف في الفقه الفرنسي بالحق في الحياة الخاصة، بأنه أحد حقوق الإنسان الرئيسة التي تتعلق بكرامة الإنسان وبقيم مادية ومعنوية أخرى، كالحق في الرأي والحق في التعبير. وقد أصبح يقصد به حق احترام سرية وخصوصية الأشخاص من أي تدخل مادي أو معنوى. مادة معلوماتية عن الأعمال الإلكترونية وأمن المعلومات، المرجع السابق، ص٢٢ . وجرى الاعتراف بالخصوصية ضمن ثقافات ونظم غالبية الدول، فجرى حمايتها في الإعلان العالمي لحقوق الإنسان؛ حيث نصت المادة (١٢) من الإعلان العالمي على أنه " لا يعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو سكنه أو مراسلاته أو لحملات على شرفه وسمعته. ولكل شخص الحق في حماية القانون من هذا التدخل أو تلك الحملات" . وفي العهد الدولي للحقوق المدنية والسياسية، وفي غالبية اتفاقيات حقوق الإنسان الدولية والإقليمية؛ حيث ورد النص عليه في الاتفاقية الأوروبية لحقوق الإنسان – روما ١٩٥٠ – ف – في المادة الثامنة منها "١ – لكل إنسان الحق في احترام حياته الخاصة، وحرمة منزله ومراسلاته. ٢ – يمنع تدخل السلطة العامة في ممارسة الإنسان لحقه المذكور إلا في الأحوال التي بينها القانون، وفي حالة حماية الأمن القومي للمجتمع الديمقراطي، أو لحماية سلامة الناس أو المصلحة الاقتصادية أو لمنع حالات الفوضي أو ارتكاب الجرائم، أو لحفظ الصحة والأخلاق العامة، أو لحماية ورعاية حقوق وحريات "الآخرين وأكدت ذلك المادة (١١) من الاتفاقية الأمريكية لحقوق الإنسان التي جاء نصها مطابقاً تقريباً للنص المقرر في الإعلان العالمي لحقوق الإنسان وضمنت كل دولة في العالم تقريبا دستورها حكما ما بشأن الخصوصية في حدها الأدنى كغالبية النصوص التي تحمي الحق في حرمة المسكن وسرية الاتصالات المفهوم المادي للخصوصية)، ومعظم الدساتير الحديثة تتضمن نصوصاً خاصة تعترف بالحق في الوصول والسيطرة على المعلومات الشخصية (المفهوم المعنوي للخصوصية)، وحتى في الدول التي لم تتضمن دساتيرها أو قوانينها اعترافا بالخصوصية. فإن المحاكم فيها قد أقرت هذا الحق بشكل أو آخر استنادا إلى الاتفاقيات الدولية التي اعترفت بهذا الحق حيثما تكون الدولة عضواً فيها.

وتطبيقاتها فكرة المسئولية الجنائية عن المساس بالأفراد والمؤسسات عند إساءة التعامل مع بياناتهم الشخصية المخزنة في نظم الكمبيوتر على نحو يمس أسرارهم وحقهم في الخصوصية Privacy"[١].

مشكلة الدراسة

لما كان الإنترنت قد أصبح أحد ركائز الحياة المعاصرة، فقد تم استغلاله من البعض من أجل السطو على المعلومات أو تخريبها من خلال إرسال البرمجيات الخبيثة Malware التي تقوم بتدمير هذه المعلومات أو إختراقها، وهو الأمر الذي يستدعي البحث في جوانب المسئولية القانونية لتلك البرمجيات الخبيثة Malware وموردي المحتوى أو الخدمة التي تحتوي على تلك البرمجيات.

وترتيبا على ما سبق يمكن للباحث صياغة المشكلة البحثية للدراسة الحالية على هيئة تساؤل رئيس كما يلي: **كيف يمكن بلورة عناصر المسؤولية الجنائية تجاه إرسال البرمجيات الخبيثة في التشريعات المقارنة؟**

تساؤلات الدراسة

يمكن طرح مجموعة من التساؤلات أبرزها ما يلى:

١. ما المقصود بأمن المعلومات في البيئة الرقمية؟ وما هى اللآليات التشريعية لحمايتها؟

٢. كيف يمكن تحديد الركن الجرمي لإرسال البرمجيات الخبيثة عبر شبكة الإنترنت؟

وقد تضمنت غالبية الدساتير الحديثة نصوصاً صريحة بشأن حماية الخصوصية ببعديها المادي والمعنوي، وأن عدداً منها تضمن نصوصاً بشأن حماية الحق في البيانات الشخصية، والوصول إليها وإدارتها. انظر النصوص الواردة في هذه الدساتير في العديد من مواقع القانون على الإنترنت ومنها:

http://www.uniwuerzbwrg.de/law/index.html6/10/2010
http://www.internationalprivacy.org6/10/2010

(١) يونس عرب، المخاطر التي تتهدد الخصوصية وخصوصية المعلومات في العصر الرقمي، الأردن، ٢٠٠٩، ص١.

٣. ما الأبعاد المرتبطة بالمسئولية الجنائية لمزودي خدمة الإنترنت عن إرسال البرمجيات الخبيثة Malware؟

٤. ما أبرز الآليات التشريعية الدولية لمكافحة الفيروسات الخبيثة؟

أهمية الدراسة

يمكن تحديد أهمية هذه الدراسة في ضوء الاعتبارات التالية:

على الجانب النظري

١ – حداثة موضوع الدراسة على المستوى العربي ، خاصة أن موضوع البرمجيات الخبيثة Malware هى مسألة بحثية جديدة على عالمنا العربي بينما ظهرت بقوة خارج الدول العربية ومن ثم يستمد هذا الموضوع أهميته من طبيعة تلك البرمجيات وتأثيرها على أمن المعلومات.

٢ – لاشك أن الأدبيات النظرية المتعلقة بالموضوع الحالي ركزت معظمها على مسألة الجرائم الإلكترونية بينما يجد الباحث ندرة في الأدبيات التي تتناول البرمجيات الخبيثة Malware وأثرها السلبي على قواعد البيانات وأمن المعلومات وهو ما يوضح الأهمية العلمية للدراسة.

على الجانب التطبيقي

١ – الوقوف على واقع وحقيقة تلك البرمجيات الخبيثة Malware وأثرها على أمن المعلومات وعلاقتها بخلق عوالم جديدة من التحديات التقنية والتشريعية أمام التشريع العربي والدولي.

٢ – لاشك أن الآثار الكارثية لإرسال برمجيات خبيثة لتدمير أنظمة حاسوبية ونظم معلومات وقواعد بيانات تتطلب وجود نظم تشريعية حاكمة لمنع انتشار تلك البرمجيات والحفاظ على أمن المعلومات في التشريعات العربية وكذلك على المستوى الدولي.

الدراسات السابقة

دراسة عبد الله ذيب محمود، جرائم الاعتداء على البرامج الإلكترونية في التشريعات الفلسطينية، كلية القانون – جامعة خضوري، فلسطين، ٢٠٢٤

تشير مشكلة الدراسة إلى أن التطور والانتشار الكبيرين لتكنولوجيا المعلومات وأجهزة الاتصال وزيادة الاعتمادية على الشبكة العنكبوتية إلى استخدامها بشكل واسع في الحياة اليومية للمواطن الفلسطيني، وبالتالي؛ ظهور العديد من الجرائم الإلكترونية المتصلة بها.

وتدور هذه الدراسة حول الحديث عن جرائم الاعتداء على البرامج الإلكترونية في التشريعات الفلسطينية، التي تتمثل في تعطيل أو إعاقة الوصول إلى الخدمات الإلكترونية أو الأجهزة أو البرامج أو المعلومات الإلكترونية على اختلاف أنواعها، فمحل الحماية في جريمة الاعتداء على الأجهزة الإلكترونية والشبكة الإلكترونية هو البرامج المكونة أو الملحقة بالحواسيب والشبكات، بالإضافة إلى البيانات والمعلومات المخزنة، وأيضاً الخدمات التي تقدمها،

وقد اتبع الباحث المنهج الوصفي التحليلي في دراسة هذه الجرائم، وذلك بالرجوع إلى نصوص القرار بقانون رقم ١٠لسنة ٢٠١٨ بشأن الجرائم الإلكترونية، والمعدل بموجب القرار بقانون رقم – ٣٨ – لسنة ٢٠٢١ الذي أقرّته الحكومة الفلسطينية للحد من انتشار هذه الجرائم، ومحاولة لاستخلاص وتحليل ومناقشة إرادة المشرع الفلسطيني فيما يتعلق بالحماية القانونية التي وفرها للبرامج الإلكترونية، ومحاولة مزج الجانب التقني مع الجانب القانوني.

ويشير البحث إلى أن المشرع الفلسطيني حاول توفير حماية قانونية للبرامج الإلكترونية انطلاقاً من حق المستخدم في الوصول إلى الجهاز الإلكتروني الخاص به، واستخدام هذه البرامج على الوجه المشروع، وأن تعطيل أو إعاقة الوصول إلى الأجهزة الإلكترونية والشبكة الإلكترونية والبرامج الملحقة يشكّل اعتداء على هذا الحق.

دراسة سعد عاطف عبد المطلب حسنين، أحكام المسئولية الجنائية عن الجرائم المعلوماتية دراسة مقارنة، مجلة الدراسات القانونية والإقتصادية، ٢٠٢١

جاءت أهمية الدراسة محل البحث فى دوره نحو تطوير التشريع الجنائي المصري في مكافحة الجرائم الإلكترونية لمحاصرتها وعدم إفلات مجرميها من العقاب

ولقد خلصت الدراسة الى استكمال المنظومة التشريعية الجنائية الوطنية فى مكافحة الجرائم الالكترونية فى ضوء التشريعات الجنائية الوطنية والمقارنة والدولية مما ينير الطريق أمام العدالة الجنائية بشأن مكافحتها.

دراسة نادية خدام، كيفية معاقبة مجرمي الإنترنت: دراسة للتحقيق في العقوبات القائمة على الهدف والعواقب لهجمات البرامج الضارة في المملكة المتحدة والولايات المتحدة والصين وإثيوبيا وباكستان

لقد سلطت الدراسة الضوء على النمو الهائل لهجمات البرمجيات الخبيثة في جميع أنحاء العالم، مما يشكل تهديدًا كبيرًا للمجتمع. أصبح مجرمو الإنترنت بلا رحمة بشكل متزايد ولا يظهرون أي علامات شفقة تجاه الأفراد أو المنظمات. من الواضح أن مجرمي الإنترنت لن يتوقفوا عند أي شيء للحصول على وصول غير مصرح به إلى المعلومات السرية . لمكافحة هجمات البرمجيات الخبيثة بشكل فعال، هناك حاجة إلى قوانين إلكترونية صارمة، واستخدام البرمجيات الخبيثة يعاقب عليه القانون في العديد من البلدان. ومع ذلك، لم يتطرق الأدبيات إلى ما إذا كانت هذه العقوبات تخلق ردعًا أم لا. تناولت هذه المقالة البحثية هذه الفجوة. في هذه الدراسة، تم تحليل فعالية القوانين الجنائية المتعلقة بالجرائم المتعلقة بالبرمجيات الخبيثة في ولايات قضائية مختلفة باستخدام منهجية البحث العقدي. تم فحص قوانين الإنترنت في الولايات المتحدة الأمريكية والمملكة المتحدة وإثيوبيا وباكستان والصين لتحديد ما إذا كانت العقوبات المفروضة على هذه الجرائم مناسبة بالنظر إلى شدة الضرر الناجم. وخلصت الدراسة إلى أن عقوبات البرمجيات الخبيثة يجب أن تأخذ في الاعتبار إنشاء أو استخدام التعليمات البرمجية الخبيثة ، واستهداف الأفراد أو المنظمات، وحجم العواقب، بغض النظر عما إذا كان هناك نية جنائية أم لا.

منهجية الدراسة

سعى الباحث إلى الاستفادة من بعض المناهج في دراسة موضوع البحث وذلك على النحو التالي :

١- المنهج القانوني" يتم استخدام هذا المنهج وذلك من خلال معالجة وتحليل الأساليب والطرق والإجراءات التي تم اللجوء إليها في حماية أمن المعلومات تجاه البرمجيات الخبيثة Malware عبر الإنترنت.

٢- المنهج المقارن" تعتمد الدراسة على المنهج التحليلى المقارن فى محاولة لكشف الاتجاهات المختلفة لتشريعات مكافحة البرمجيات الخبيثة Malware في التشريعات العربية والدولية.

بنية الدراسة

تم تقسيم الدراسة الحالية إلى أربعة مطالب رئيسة وذلك كما يلي:

المطلب الأول: الأحكام العامة لأمن المعلومات الرقمية والآليات التشريعية لحمايتها .

المطلب الثاني: أركان جريمة إرسال البرمجيات الخبيثة

المطلب الثالث: المسئولية الجنائية لمزودي خدمة الإنترنت عن إرسال البرمجيات الخبيثة

المطلب الرابع: الآليات التشريعية الدولية لمكافحة الفيروسات الخبيثة

المطلب الاول
الأحكام العامة لأمن المعلومات الرقمية والآليات التشريعية لحمايتها

لقد اختلفت المفاهيم التي أوردها الباحثون بشأن تحديد مفهوم أمن المعلومات وفيما يأتي بعض المفاهيم كما وردت في كتابات عدد من الباحثين يقصد بأمن المعلومات حماية وتأمين الموارد المستخدمة كافة في معالجة المعلومات، إذ يكون تأمين الشركة نفسها والأفراد العاملين فيها وأجهزة الحاسبات المستخدمة فيها ووسائط المعلومات التي تحتوي على بيانات الشركة[١].

وأيضا أمن المعلومات هو وقاية لسرية، وسلامة المعلومات قانونيا[٢]، في حين عرف أمن المعلومات بأنه هو اختصار الطرق والوسائل المعتمدة للسيطرة على أنواع ومصادر المعلومات كافة وحمايتها من السرقة ، والتشويه والابتزاز، والتلف، والضياع والتزوير، والاستخدام غير المرخص ، وغير القانوني [٣].

وكذلك أمن المعلومات يعني كل السياسات والإجراءات والأدوات التقنية التي تستخدم لحماية المعلومات من أشكال الاستخدام غير الشرعي كلها للموارد مثل السرقة، والتغير، والتعديل، وإلحاق الضرر بالمعلومات المتعمد[٤]، وهناك من يرى أن أمن المعلومات يتكون من العديد من المكونات ذات المدلول التي تشير إليها علي النحو التالي:-

فكلمة الأمن تشير إلى طيف واسع من المجالات ضمن وخارج حقل تقنية المعلومات. ويشمل أمن المعلومات الخصائص الخمسة الآتية :٢ السرية ١ - التحقق من الهوية ٣ -

---

(١) حسن طاهر داوود ، الحاسب وامن المعلومات ، مركز الدراسات والبحوث ، المملكة العربية السعودية ، ٢٠٠٠م ، ص٢٣ .

(2)Micki Krause ; Harold F. Tipton, Information Security Management Hand book, Sixth Edition, Auerbach Publication, New York, 2008

(٣) هيثم محمد الزعبي ، إيمان فاضل السامرائي ، نظم المعلومات الإدارية ، الطبعة الأولى ، دار صفاء للنشر والتوزيع ، عمان ، ٢٠٠٤م ص ٢٣٨ .

(٤) سعد غالب ياسين ، نظم المعلومات الإدارية الطبعة العربية دار اليازوري العلمية للنشر والتوزيع ، عمان الأردن ، ٢٠٠٩ ، ص٣٤٨.

الكمال ٤ التوفير ١ – مكافحة الإنكار (المسؤولية)[١] ، فعند ذكر كلمة أمن المعلومات فإن ما يتبادر إلى الذهن غالبا هو كشف المعلومات التي كان يجب أن تبقى سرا ، والحقيقة أن الحفاظ على المعلومات وسريتها يكون جانبا واحدا من جوانب الأمن[٢]. ومما تقدم نلحظ أن البعض أخذ مفهوم أمن المعلومات من زاوية قانونية وذلك بوجوب وضع التشريعات والقوانين لحماية المعلومات . والبعض الآخر أخذه من زاوية تقنية بوضع الأدوات والوسائل لحماية المعلومات . ولكون أمن المعلومات أحد عناصر البنية الأساسية التي يجب أن تتاح لأمن نظام المعلومات الخاص بالشركة فعند التخطيط له يجب توازن قيمة المعلومات لإدارة الشركة مع الحجم النسبي لأنواع المعلومات في مواجهة حد الأمن المتوسط في الأساس. وفي كثير من الشركات والأجهزة الحكومية تتوافر منظومات أمن صارمة لمعالجة وتخزين واسترجاع المعلومات ونقلها بطريقة تحمي سريتها وسلامتها في مستودعاتها المقروءة آليا[٣].

أولا : المعلومات الرقمية في ضوء التحديات الأمنية

في الوقت الذي تدخل الإنترنت في شتى مناحي الحياة اليومية أكثر فأكثر ، فإن الأخطار اليومية المتعلقة بالإنترنت تزايدت بشكل غير مسبوق ، فلم يصبح السؤال " هل من الممكن الاختراق " ولكن " متى سيتم الاختراق؛ إذ إن معظم أجهزة الإنترنت تفتقر إلى الأمن والخصوصية الكافية لحماية مستخدميها، وقد كشفت شركة HP أن ٧٠٪ من إنترنت الأشياء تحتوي على ثغرات أمنية يمكن لمرتكبي الجرائم الإليكترونية استغلالها ومنها-:

ضعف المستوى الأمني لواجهات الويب WEB INTERFACES في بيئة الإنترنت.

افتقار المعايير والمقاييس الموحدة للتواصل بين الأجهزة الطرفية والإنترنت يعوق تعزيز المستوى الأمني في بيئة الإنترنت.

---

(١) نجم عبد الله الحميدي ، نظم المعلومات الإدارية مدخل معاصر ، الطبعة الثانية ، دار اليازوري للنشر والتوزيع، عمان ، الأردن ، ٢٠٠٩ م ، ص١.

(٢) محمد بن عبد الله القحطاني ، أمن المعلومات ، جامعة الملك عبد العزيز للعلوم والتقنية، الرياض، ٢٠٠٩ م ،ص٢٣.

(٣) أيمن محمد مصطفى، أمن المعلومات في البيئة الإلكترونية، القاهرة، بدون ناشر، ٢٠٢٣، ص. ١٠

قلة الرقابة القانونية بين الحكومات في مجال الإنترنت تزيد من فرص القرصنة الإليكترونية.

أكثر الناس المستهدفين في الاختراقات الأمنية هم الأشخاص الذي يقومون بتصفح الإنترنت حيث يتسبب الاختراق في مشاكل مزعجة مثل بطء حركة التصفح وانقطاعه على فترات منتظمة ويمكن أن يتعذر الدخول إلى البيانات وفي أسوأ الأحوال يمكن اختراق المعلومات الشخصية للمستخدم.

تحدي الحق في الخصوصية يعد الحق في الخصوصية من أسمى الحقوق المدنية الأصيلة للإنسان ، أو حقه في احترام حياته الخاصة فهذا الحق أصبح مهما فالفرد لا يعيش فقط لمصالحه المادية ، وإنما يلزم لحياته حقوق ملتصقة لشخصيته ملازمة لها[١] .

وقد حرصت مختلف الاتفاقيات الدولية المعنية بحقوق الإنسان والحريات والدساتير الوطنية و مختلف القوانين الوطنية على وضع العديد من الضوابط الشرعية ، والإجراءات الماسة بالحقوق والحريات الفردية ، ومن ثم فإن مخالفة هذه النصوص في تحصيل الدليل الجنائي يضفي عليه عدم المشروعية ، وعليه فإن الدليل أيا كان نوعه متى تعارضت طريقة الحصول عليه والقواعد القانونية العامة التي توجب احترام حقوق الإنسان وحرياته وقيم العدالة وأخلاقياتها والنزاهة في الحصول على الأدلة واحترام حقوق الدفاع [٢].

---

(١) أحمد فتحي سرور :- الحق في الحياة الخاصة ، مجلة القانون والاقتصاد للبحوث القانونية والاقتصادية . مطبعة جامعة القاهرة ، العدد ٥٤، ١٩٨٦م ، ص ٣٥ .، أسامة عبد الله قايد :- الحماية الجنائية للحياة الخاصة وبنوك المعلومات ، بدون دار نشر ورقم طبعة ، ١٩٨٠ ، ص ١٤ ، هشام محمد فريد :- الحماية الجنائية للإنسان في صورته ، مكتبة الآلات الحديثة ، أسيوط ، ص ٧٠.

Samuel D. Warren &Louis D. Brandeis, The right of piracy, Harvard law review, Vol. IV., Dec. 15, 183-220.

(٢) على سبيل المثال فإن النظام اللاتيني يشترط من أجل أن يستطيع القاضي الاستناد إلى دليل معين عليه، أن تكون طريقة الحصول على الدليل قد جرت بصورة مشروعة ، وذلك لأن القاضي الجنائي ليس له مطلق الحرية في تكوين عقيدته من الأدلة غير المشروعة التي يتحصل عليها ، ومن الأمثلة لذلك الحصول على الدليل بالإكراه أو التهديد ، أو تفتيش باطل راجع:- ممدوح خليل بحر :- نطاق حماية الحياة الخاصة في القانون الجنائي ، دار الثقافة للنشر والتوزيع ، الأردن ، ٢٠٠٦م ، ص ٣٠٣.

وعليه فإن الدليل الجنائي بما فيه الأدلة الرقمية لا يكون مشروعا ومن ثم الاعتماد عليه أمام القضاء الجنائي إلا إذا كان الحصول عليه في إطار أحكام القانون، وقيم العدالة وأخلاقياتها التي يحرص على حمايتها [١].

ومن خلال ذلك تتحدد أبعاد مفهوم التهديدات الأمنية على النحو التالي :-

- التهديدات توجد متى وجدت نقاط الضعف، ويمكن أن يوجد أكثر من تهديد لكل نقطة ضعف
- قد تتسبب المشكلات الفنية نتيجة للهجمات المختلفة التي يتعرض لها النظام، فغالبا تدخل الفيروسات في النظام من خلال البرمجيات المصابة وبعض الوسائل الفنية المستخدمة لتعطيل النظام وتشويهه وعرقلة وظائفه المختلفة، وإتلاف أو تحريف بياناته[٢].

- Todd G. Shipley, Henory R. Reeve, Collecting evidence from a running computer, The national consortium for justice information and statistic,2006, p.4

(١) عائشة بن قارة مصطفي -:- حجية الدليل الإليكتروني في مجال الإثبات الجنائي ، دار الجامعة الجديدة الإسكندرية ، ٢٠٠٩م ، ص ٢١٣ ، علي محمود علي حمودة :- الأدلة المتحصلة من الوسائل الإليكترونية في إطار نظرية الإثبات الجنائي ، مقدم للمؤتمر العلمي الأول حول الجوانب القانونية الأمنية للعمليات الإليكترونية . أكاديمية شرطة دبي ، ٢٨ - ٢٠٠٣/ ٤/ ٢٩م ٢٠٢ ، ممدوح عبد الحميد عبد المطلب ، زبيدة محمد قاسم ، عبد الله عبد العزيز، أنموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في جرائم الكمبيوتر ، مؤتمر الأعمال الخاصة، المصرفية الإليكترونية ، كلية الشريعة والقانون ، الإمارات ، غرفة تجارة وصناعة دبي، ٥-٢٠٠٣/ ١٢/ ١٠م. - ويرى البعض أن الاستعانة بوسائل علمية حديثة تهدف من استخدامها الحصول على دليل على وقوع الجريمة يستهدف المصلحة العامة ، وذلك حتى تتمكن الدولة من حماية النظام الاجتماعي لا يجوز التذرع باحترام الحقوق والحريات للاعتراض على الدليل بحجه عدم مشروعيته راجع فاطمة مرينز : الاعتداء على الحق في الحياة عبر شبكة الإنترنت ، رسالة دكتوراه، جامعة أبو بكر بلقان ، تلمسان ، الجزائر ، ٢٠١٢-٢٠١٣م . ، وقد حرص الدستور المصري ٢٠١٤ على النص على هذه الحريات الأساسية فقد جاء في المادة ٥٧ من النص علي أن حرمة الحياة الخاصة هي مصونة ولا تمس ، والمادة ٧٠ حرية الصحافة والنشر.

(٢)- أيمن محمد مصطفى، أمن المعلومات في البيئة الإلكترونية، مرجع سابق، ص. ١٦

وقد أظهر تقرير صدر في الولايات المتحدة الأمريكية عام ٢٠٠٣ أن ٣٦٪ من الجهات تعتبر أن المستخدمين الداخليين هم أشد خطراً على أنظمة المعلومات المتاحة داخل هذه المؤسسات من الخطر الخارجي. ولكن ولأسباب إعلامية وللحفاظ على هيبة الشركات والمؤسسات فإن معظمها تركز سياساتها على عمليات تأمين شبكات المعلومات فيها من الأخطار الخارجية دون الداخلية.

ثانيا: أنماط التهديدات السيبرانية لأمن المعلومات

يمكن تحديد أبرز تلك الأنماط على النحو التالي:

القرصنة :ـ القرصان هو الشخص الذي يتجاوز عناصر التحكم في الوصول إلى النظام من خلال الاستفادة من نقاط الضعف الأمنية التي تركها مطورو الأنظمة في النظام SYSTEM'S VULNERABILITY ، بالإضافة إلى براعة المتسللين في اكتشاف كلمات السر، وتمثل القرصنة تهديدات خطيرة للمعلومات السرية في أنظمة الحاسب[١].

الاختفاء : المتخفي أو المقنع MASQUERADERS هو المستخدم الذي حصل على كلمة المرور لمستخدم آخر على النحو الذي يمكنه من الوصول إلى الملفات المتاحة للمستخدم الآخر سرقة كلمة السر Password cracking اختراق الشبكة والاطلاع على المعلومات الخاصة بالشركة من خلال سرقة كلمة السر الخاصة بالمعنيين داخل الشركة.

التحميل للملفات دون حماية حيث يتم نقل الملفات من بيئة آمنة في الحاسب المصنف إلى الحاسبات الصغيرة غير المحمية[٢].

حصان طروادة TROJAN HORSE . وهو برنامج يظهر بأن يعمل بشكل معين ومفيد للمستخدم بينما هو في الواقع يقوم بعمل ضار وخفي عن المستخدم مثل الإضرار بالحاسوب أو إرسال معلومات إلى المحتال[٣].

---

(1) Romney , M& Steinbart ,P. , Accounting information's system ,12ed., ENGLAND. Pearson education,2012.

(٢) أشرف صلاح الدين، طرق الحماية التكنولوجية بأنواعها وأشكالها المختلفة ، ورشة عمل بعنوان أمن وحماية نظم المعلومات في المؤسسات العربية ، القاهرة ، ٢٠٠٧.

(٣) ذيب بن عايض القحطاني ، أمن المعلومات ، مدينة الملك عبد العزيز للعلوم التقنية ، الرياض ١٤٣٦هـ - ٢٠١٥م ، ص ٢١٨ وما بعدها

ـ التعـرض للاخـتراق أثنـاء محاولـة معالجـة اخـتراق سـابق -ZERO-DAY ATTACK

الهندسة الاجتماعية SOCIAL ENGINEERING ويقصد بها تحفيز المستخدم على الإفصاح عن بيانات سرية من خلال طرح أسئلة بسيطة بهدف جمع معلومات دون إثارة أي شبهة.

هجمات حقن قواعد البيانات مثال من خلال إدخال برمجية ضارة مكان كلمة السر أو اسم المستخدم إذا تمكن المحتال من الوصول إلى قواعد البيانات بهدف سرقتها أو التعديل فيها أو تدميرها [١].

شبكات المناطق المحلية حيث تشكل هذه الشبكات تهديدا خاصة للسرية لأن البيانات تتدفق من خلال LAN يمكن مشاهدتها في أي عقدة في الشبكة.

الأجهزة المحمولة التي تعد من التحديات الجديدة التي تتزايد خطورتها يوما بعد يوم من خلال البرمجيات الضارة التي تستهدفه، وسرقة البيانات، وفقدانها وسرقتها ، وقضايا أخرى تظهر في كل وقت مثل القدرة على تحديد الموقع الجغرافي للفرد من خلال أجهزتهم .

ثالثا: البيئة التشريعية تجاه الحفاظ على أمن المعلومات في البيئة السيبرانية

يقوم النظام الأمريكي على مجموعة من التشريعات على المستوى الفيدرالي ، وعلى المستوى المحلي في مختلف الولايات، **فعلى المستوى الفيدرالي**، يمثل الفصل ١٨٠ من قانون الولايات المتحدة التشريع الرئيس لجرائم التقنية الحديثة من خلال سن العديد من القوانين الفيدرالية كان أولها قانون الاحتيال وإساءة استخدام الكمبيوتر أو COMPUTER FRAUD AND ABUSE (CFAA) عام ١٩٨٤م وتم تعديله عام ١٩٨٤م و ١٩٩٤م للتعامل مع البرامج الخبيثة لإتلاف أو تغيير البيانات ، ونص القسم ١٠٣٠ من الفصل ١٨ على تجريم العديد من الأفعال أهمها :[٢]

---

(١) يوسف خليل يوسف عبد الجابر ، مدى فاعلية إجراءات الرقابة الداخلية في توفير أمن المعلومات الإليكترونية في الشركات الصناعية الأردنية ، رسالة ماجستير ، جامعة الشرق الأوسط ،٢٠١٣م ، ص٢٨.

(٢) أيمن محمد مصطفى، أمن المعلومات في البيئة الإلكترونية، مرجع سابق، ص. ٣٣

- الدخول غير المصرح به إلى أحد أنظمة الحاسب للحصول على معلومات أمنية وطنية بنية الإضرار بالبلاد ، أو لمنفعة دولة أجنبية.
- الدخول غير المصرح به لأنظمة الحاسب الآلي للحصول على معلومات خاصة بأموال محمية.
- الدخول غير المصرح به إلى النظام الخاص بالحكومة الفيدرالية.
- الدخول غير المصرح به إلى أي نظام بنية الاحتيال.
- الدخول غير المصرح به إلى أي نظام مع تعمد إلحاق أضرار به
- الاتجار الاحتيالي في كلمات سر الحاسوبية ، وغيرها من المعلومات للوصول لنظام محمي.
- بث أو تهديد بارتكاب ضرر لأي نظام محمي عبر الولايات المتحدة ، أو للتجارة الأجنبية بغرض ابتزاز أموال ، أو منافع من أي شخص طبيعي أو معنوي.

القسم ١٤٦٢ من الفصل ١٨ تعلق باستخدام الحاسب لاستيراد مواد مخلة بالآداب ، القسم ٢٢٥١ جرم توظيف أي قاصر أو إغرائه للمشاركة في أنظمة جنسية ، القسم ١٠٢٨ جرم إنتاج ، أو نقل ،أو إدارة تتضمن نظام حاسوبي بقصد استخدامه في تزوير الوثائق ،أو إنشاء وثائق مزورة.

وفي عام ٢٠٠٣م أصدر الكونجرس الأمريكي قانون مكافحة البريد الإليكتروني غير المرغوب فيه(ANTI SPAM LAW) ، ودون في القسم ١٥٣٧ من الفصل١٨ ، ويحظر إرسال الرسائل غير المرغوب فيها ، وأن تشمل رسائل البريد الإليكتروني آلية تتيح للمتلقي الإشارة أنه لا يريد استقبال هذه الرسائل.

وعلى مستوى الولايات المتحدة تملك كل ولاية حرية التشريع الخاص بها والإطار العام لتوحيد قوانين جرائم التقنية يعتمد على مشروع قانون نموذجي MODEL STATE COMPUTER CRIMES CODE الذي تم وضعه من قبل هيئة أكاديمية ١٩٩٨م[١].

وعلى مستوى التشريع الفرنسي، تعتبر فرنسا من أوائل الدول التي تعاملت مع جرائم تقنية المعلومات فقد صدر قانون العقوبات الفرنسي في عام ١٩٩٨ وبموجبه تم تجريم الدخول إلى نظام المعالجة الآلية للمعلومات أو البقاء فيها بطريق غير مشروع وعاقب على ذلك بالحبس مدة تتراوح بين شهرين وعام وبغرامة من ٣٠٠٠-٥٠٠٠ فرنك أو بإحدى هاتين العقوبتين ، وبعدها صدر قانون رقم ١١٧٠ لسنة ١٩٩٠ الذي اشتملت مادته (٢٨) لبيان معنى التشفير وضمان سرية المعلومات والاستيلاء على المعلومات بطريق اختراق التشفير)[٢] .

صدر قانون العقوبات الفرنسي الجديد لعام ١٩٩٤ الذي عالج بدوره تنظيم المعالجة الآلية للبيانات في المادة ٣٢٣ بفقراتها الأربع فالفقرة الأولى ذهبت لتجريم الوصول أو البقاء بطريقة مخادعة في كل جزء من نظام المعالجة الآلية للمعطيات ،أما الفقرة الثانية فقد جرمت إعاقة النظام وتزوير المعطيات والمعالجة الآلية ، وما يسجل بشأن القانون الفرنسي الجديد (قانون العقوبات) أنه جاء خالياً من الإشارة للجرائم المالية والجرائم التي تهدد الشخصية الفردية والجرائم غير الأخلاقية كما أنه جاء خالياً من تجريم المقامرة عبر الإنترنت والاتجار بالبشر وجرائم الاختراقات وصناعة ونشر الفيروسات[٣].

---

(١) يونس عرب ، جرائم الكومبيوتر والانترنت ، إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات ، ورقة عمل مقدمة إلى مؤتمر الأمن العربي ٢٠٠٢م تنظيم المركز العربي للدراسات والبحوث الجنائية ، أبو ظبي ، ص ١١ ، ١ - ١٢/ ٢ ٢٠٠٢م.

(٢) عبد الفتاح بيومي حجازي، التجارة الإليكترونية وحمايتها القانونية ، دار الفكر الجامعي ، الإسكندرية ، ٢٠٠٤م ، ص ص ٣٩-٤١.

(٣) محمد حماد مرهج الهيتي، "جرائم الحاسوب ، ط ، إدارة المناهج للنشر والتوزيع ، عمان، ٢٠٠٦م ص ١٧٩ ، مفتاح بوبكر المطردي ، الجريمة الإليكترونية ، ورقة عمل مقدمة إلى المؤتمر الثالث لرؤساء

وفي ضوء التشريع السعودي[1] احتلت المملكة العربية السعودية المركز السادس عالمياً بين الدول التي تنطلق منها الهجمات الإلكترونية نسبة إلى عدد مستخدمي الإنترنت في البلاد (). فكان لا بد لها من إصدار تشريع خاص بذلك ، حيث سبقت السعودية قانون جديد لمكافحة جرائم المعلوماتية ، فقد صدر المرسوم الملكي رقم م ١٧/ في ٣/ ٨/ ١٤٢٨هـ بناء على قرار مجلس الوزراء رقم ٧٩ بتاريخ / ٧/ ٣ ١٤٢٨هـ ، وقد تضمن هذا المرسوم بيان معاني المصطلحات والمسميات ومنها الجريمة المعلوماتية أما المادة الثالثة فقد عاقبت على العديد من الأفعال الجرمية بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال أو بإحدى هاتين العقوبتين وهي التصنت على ما هو مرسل عبر شبكة المعلوماتية ، أو أجهزة الحاسب دون مسوغ نظامي، صحيح ، والدخول غير المشروع لتهديد شخص أو ابتزازه لحمله على القيام بفعل أو الامتناع عن القيام به، والمساس بالحياة الخاصة باستخدام الهاتف النقال المزود بكاميرا وما في حكمها والتشهير بآخرين وإلحاق الضرر بهم عبر وسائل تقنية المعلومات كما أن المادة الخامسة من هذا المرسوم عاقبت بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال أو بإحدى هاتين العقوبتين كل شخص يرتكب أياً من الجرائم المعلوماتية كالدخول غير المشروع لإلغاء بيانات خاصة أو حذفها أو تدميرها أو تسريبها أو إتلافها أو تغييرها أو تدميرها أو مسح البرامج أو البيانات المستخدمة وكذلك إعاقة الوصول إلى الخدمة أو تشويشها أو تعطيلها بأي وسيلة كانت وقد عاقبت المادة السادسة بالسجن مدة لا تزيد على خمس سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال أو بإحدى هاتين العقوبتين كل شخص يرتكب جريمة إنتاج ما من شأنه المساس بالنظام العام أو القيم الدينية أو الآداب العامة أو

المحاكم العليا في الدول العربية ، السودان ٢٣ - ٢٠ أيلول ٢٠٠١م ، مدحت رمضان ، جرائم الاعتداء على الأشخاص والإنترنت ، دار النهضة العربية ، القاهرة ، ٢٠٠٧م ، ص١٧ .

(١) نظام مكافحة جرائم المعلوماتية ، هيئة الاتصالات وتقنية المعلومات ، المملكة العربية السعودية .

حرمة الحياة الخاصة أو إعداده أو إرساله أو تخزينه عن طريق شبكة المعلوماتية كما جرمت إنشاء المواقع الخاصة بنشر ما يتعلق بالاتجار بالجنس البشري وتسهيل التعامل به وجرمت أيضا إنشاء المواد والبيانات المتعلقة بالشبكات الإباحية أو أنشطة الميسر المخلة بالآداب العامة أو نشرها أو ترويجها وكذلك ما يتعلق بالمخدرات والمؤثرات العقلية كما جرم هذا المرسوم في مادته السابعة إنشاء المواقع لمنظمات إرهابية على الشبكة المعلوماتية والتعامل معها ومساعدتها والترويج لأفكارها وكل ما يتعلق بنشاطاتها وقد بين هذا المرسوم الظروف المشددة في هذه الجرائم م ٨ / ووسائل الإسهام الجنائي والعقاب على الشروع في الجرائم التي طواها م / ١٠ والحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة في ارتكاب هذه الجرائم م / ١٣ . وجدير بالذكر أن القانون السعودي كان قد انفرد بالنص على تجريم إنتاج ونشر كل ما من شأنه المساس بالقيم الدينية والاعتداء على الأديان باستخدام وسائل تقنية المعلومات وكذلك تجريمه لإنشاء مواقع للمنظمات الإرهابية ولكل ما يتعلق بها من تمويل ونشر وترويج وغيرها[١].

وفيما يتعلق **بقانون العقوبات المصري** فقد وردت المواد ٣٠٩ مكرر (أ) و ٣١٠ في شأن حماية الحياة الخاصة ، أما نص المادة ٣١٠ من قانون العقوبات فإنه يجرم إفشاء السر الذي وصل إلى علم ١ أصحاب المهن أو الحرف على الرغم من أنهم مؤتمنون على هذه الأسرار [٢].

ومؤخرا أصدر المشرع المصري وحسنا فعل القانون رقم ١٧٥ لسنة٢٠١٨م في شأن مكافحة جرائم تقنية المعلومات[٣].

---

(١) أيمن محمد مصطفى، أمن المعلومات في البيئة الإلكترونية، مرجع سابق، ص. ٣٧

(٢) عبد الفتاح بيومي حجازي ، مرجع سابق ، ٦٦٤-٦٦٥.

(٣) القانون رقم ١٧٥ لسنة ٢٠١٨م في شأن مكافحة جرائم تقنية المعلومات المنشور بالجريدة الرسمية العدد ٣٢ مكرر في ١٥ أغسطس ٢٠١٨.

جاءت المادة الأولى منه لتعريف المصلحات الواردة بالقانون، ونصت المادة الثانية على التزامات وواجبات مقدم الخدمة ومنها الالتزام بالمحافظة على سرية المعلومات التي تم حفظها وتخزينها (م (٢/ ٢) ، وكذا التأكيد على تأمين البيانات والمعلومات بما يحافظ على سريتها وعدم اختراقها (م ٣/ ٢) .

ونصت المادة الثالثة على نطاق تطبيق القانون المكاني ، وحرص كذلك القانون على النص على التعاون الدولي في مجال مكافحة جرائم تقنية المعلومات من خلال التعاون الدولي والاتفاقيات الدولية وحرص القانون على أن يكون المركز الوطني لطوارئ الحاسب والشبكات هو المنوط به في هذا الشأن.

وجاء في الباب الثاني من القانون النص على الأحكام والقواعد الإجرائية ومأموري الضبط القضائي (المواد ٥ ، ٦) ، وإجراءات حجب المواقع (م ٧) ، والتظلم من تلك القرارات ، (م٨) وحرص القانون على التأكيد على حجية الأدلة الرقمية في الإثبات الجنائي متى توافرت بها الشروط الفنية الواردة في اللائحة التنفيذية بهذا القانون.

كما جرم القانون الدخول غير المشروع سواء بخطأ عمدي أو غير عمدي الدخول غير المشروع به على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه (م١٤) ، وعاقب عليه بالحبس لمدة لا تقل عن سنة وبغرامة لا تقل عن ٥٠٠٠٠ ولا تزيد عن ١٠٠٠٠٠ ألف جنيه أو بإحدى هاتين العقوبتين.

كما جرم القانون تجاوز حدود الحق في الدخول (م ١٥) ، وكذا الاعتراض غير المشروع بدون وجه حق أي معلومات أو بيانات أو كل ما هو متداول على شبكة المعلومات أو أحد أجهزة الحاسب الآلي أو ما في حكمها (م (١٦) ، كما جرم القانون الاعتداء على سلامة البيانات والمعلومات والنظم المعلوماتية (م ١٧) ، وكذا جريمة الاعتداء على البريد الإليكتروني أو المواقع أو الحسابات الخاصة (م ١٨) ، وجريمة الاعتداء على تصميم موقع (م ١٩). كما جرم القانون الاعتداء على سلامة الشبكة المعلوماتية (م ٢١) ، وحرص

القانون على تجريم حيازة أو إحراز أو جلب أو بيع أو إتاحة أو إنتاج أو صنع أو استيراد أو تصدير كل ما يسهل ارتكاب أي من الجرائم المنصوص عليها في القانون (م٢٢)[١].

وخصص الفصل الثاني من هذا الباب للجرائم المرتكبة بواسطة أنظمة وتقنيات المعلومات والاحتيال والاعتداء على بطاقات البنوك والخدمات وأدوات الدفع الإليكتروني (م٢٣)، والجرائم المتعلقة باصطناع المواقع والحسابات الخاصة والبريد الإليكتروني (م٢٤). وخصص الفصل الثالث لجرائم الاعتداء على حرمة الحياة الخاصة والمحتوى المعلوماتي غير المشروع (م (٢٥) ، كما جرم القانون كل من تعمد استعمال برنامج معلوماتي أو تقنية معلوماتية في معالجة معطيات شخصية للغير لربطها بمحتوى مناف للآداب العامة ، أو لإظهارها بطريقة من شأنها المساس باعتباره أو شرفه (م٢٦)[٢].

(١) حرص القانون على تجريم الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة أو أحد الأشخاص الاعتبارية بالحبس لمدة لا تقل عن عامين وبغرامة لا تقل عن ٥٠٠٠٠ولا تزيد عن ٢٠٠٠٠٠ ألف جنيه ، وشدد العقوبة للسجن وغرامة لا تقل عن ١٠٠٠ ولا تزيد عن ٥٠٠٠٠٠ متى كان الدخول بقصد الاعتراض أو الحصول على بيانات أو معلومات حكومية ، وإذا ما ترتب على ذلك إتلاف أو تدمير لتلك المعلومات أو البيانات تكون العقوبة السجن والغرامة لا تقل عن مليون ولا تجاوز خمسة ملايين جنيه مصري(م٢٠)

(٢) أيمن محمد مصطفى، أمن المعلومات في البيئة الإلكترونية، مرجع سابق، ص. ٤٠

المطلب الثاني
أركان جريمة إرسال البرمجيات الخبيثة

يتمثل تاريخ البرمجيات الخبيثة Malware بالفيروسات التي ظهرت بوصفها فكرة في بحث بعنوان «نظرية الجسم الآلي ذاتي النسخ» لعالم الرياضيات John von Neumann في نهاية أربعينيات القرن العشرين ونشرت هذه الورقة البحثية في عام ١٩٦٦ بعنوان نظرية الجسم الآلي ذاتي النسخ، وقد شكلت الورقة البحثية تجربة فكرية، حيث تكهنت بأنه يمكن لكائن «آلي» تدمير أجهزة ونسخ نفسه وإصابة مضيفات جديدة ولادة النسخ المتماثل الآلي، تماماً مثل الفيروس البيولوجي[١].

ومع ظهور الحواسيب وشبكات الإنترنت ظهر ما يعتبر أول فيروس في العام ١٩٧١، وما يطلق عليه الزاحف Creeper، وقد كان إنتاجه كاختبار أمني لمعرفة ما إذا كان إيجاد برنامج ذاتي النسخ أمرًا ممكنًا، فمع كل إصابة محرك أقراص جديد، كان برنامج Creeper يحاول حذف نفسه من المضيف السابق[٢].

وفي العام ١٩٧٤ تم تطوير فيروس Rabbit (أو Wabbit)، وقد كان له هدف خبيث وكان بإمكانه نسخ نفسه، فبمجرد تسلله إلى أحد الحواسيب، كان ينسخ نفسه عدة نسخ مقللاً بدرجة كبيرة من كفاءة أداء النظام ومؤديا في نهاية المطاف إلى تعطل الجهاز ، وكانت سرعة النسخ هي سبب تسمية الفيروس بهذا الاسم، أما في عام ١٩٧٥، فقد تم إنشاء

---

(١) موقع شركة كاسبر العالمية لمكافحة الفيروسات
https://me.kaspersky.com/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds
تاريخ الزيارة ٢٥ يوليو ٢٠٢٤ راجع
عبد الله ذيب محمود، جرائم الإعتداء على البرامج الإلكترونية في التشريعات الفلسطينية، مجلة جامعة العين للأعمال والقانون، الإمارات، جامعة العين، الإصدار الأول، السنة السابعة، ٢٠٢٣، ص.٨١

(٢) برنامج Creeper هدف خبيث، فكلما كان يحدثه هو إظهار رسالة بسيطة ألا وهي: I'M THE CREEPER (أنا) CREEPER, CATCH ME IF YOU CAN ، أمسك بي إن استطعت».

أول حصان طروادة [١] ، عرف باسم ANIMAL (على الرغم من أنه أثار حوله الجدل ما إذا كان حصان طروادة أم مجرد فيروس آخر) من تصميم مبرمج الحاسوب John Walker في العام ١٩٧٥.

وقد بدأ أول فيروس يصيب الحاسوب الشخصي، في إصابة الأقراص المرنة بحجم ٥.٢ بوصات في العام ١٩٨٦، حيث يطلق على هذا الفيروس Brain Boot Virus ، وكان هذا الفيروس من تصميم شخصين يديران متجراً لبيع الحواسيب في باكستان، وعندما سئما من العملاء الذين يقومون بالنسخ غير القانوني لبرامجهما، طورا فيروساً Brain، الذي يستبدل قطاع التمهيد في القرص المرن بالفيروس الذي كان أيضًا أول فيروس متسلل، على رسالة مخفية بحقوق النشر، لكنه في واقع الأمر لم يتلف أي بيانات.

وأدت زيادة انتشار الشبكة الإلكترونية على نطاق واسع في مطلع القرن ٢١ إلى تغيير طريقة انتقال البرامج الضارة، فلم يعد انتقالها مقتصرًا على الأقراص المرنة أو شبكات الشركات، لكنها أصبحت قادرة على الانتشار بسرعة كبيرة جدًا عبر البريد الإلكتروني أو عبر مواقع الويب الشائعة أو حتى عبر الإنترنت مباشرة، فمن هنا، بدأت البرامج الضارة الحديثة في التبلور، وأصبحت بيئة التهديد مختلطة؛ تتألف من الفيروسات والديدان وأحصنة طروادة، ومن ثم ظهر اسم البرامج الخبيثة الضارة بوصفها مصطلحا شاملا البرامج الخبيثة، كما سيأتي ذكره لاحقا خلال الحديث عن الركن المادي[٢].

أولا: الركن المادي لجريمة إرسال البرمجيات الخبيثة Malware

تعد هذه الجريمة من الجنايات حيث يتمحور فيها الركن المادي حول إنتاج برمجيات خبيثة تؤدي إلى تعطيل البرامج الإلكترونية، ومن أبرز البرمجيات التي تؤدي إلى تعطيل

---

(١) انتشرت في بداية الثمانينات برامج الحيوانات التي تحاول تخمين الحيوان الذي يفكر فيه المستخدم من خلال لعبة مؤلفة من ٢٠ سؤالاً، وكان هناك إقبال شديد على الإصدار الذي صممه Walker.

(٢) عبد الله ذيب محمود، جرائم الإعتداء على البرامج الإلكترونية في التشريعات الفلسطينية، مرجع سابق، ص.٨٢.

البرامج وإتلافها الفيروسات، حيث تعرف على أنها تلك البرامج الضارة التي تقوم بعملية نسخ لنفسها على أجزاء الحاسوب المختلفة كالبرامج الأخرى أو حتى الملفات أو غيرها لتلحق به الضرر وتغير من طريقة عمله، وتنتشر هذه البرامج بين أجزاء الكمبيوتر بشكل غير مرئي، حيث يقوم الركن المادي لجريمة إنتاج الفيروسات بقصد تعطيل البرامج وحذفها على السلوك الجرمي والنتيجة الجرمية والعلاقة السببية[١]، والمقصود بالسلوك النشاط الذي يتبعه الجاني من خلال إنتاج الفيروسات الضارة بالحواسيب والشبكات بقصد تعطيلها.

ويتصور الركن المادي في النشاط الجرمي الإيجابي الذي يتمثل بتصنيع وإنتاج الفيروسات التي لها من الخصائص ما يمكنها من التناسخ المتضاعف) والانتشار والتخفي إضافة إلى إلحاق الضرر بالبرامج الإلكترونية على اختلاف أشكالها[٢]، كما أن كثيرا من الفيروسات تربط نفسها ببرنامج آخر يسمى المضيف host في جهاز الحاسوب، مع الإشارة إلى أن الفيروسات لا تنشأ من ذاتها، وإنما بحاجة إلى فاعل.

كما يتصور النشاط الجرمي في كل ما يقوم بإنتاجه الفاعل من برمجيات خبيثة تهدف إلى تعطيل البرامج الإلكترونية والنظام المحوسب بشكل عام، كالملفات ذاتية التنفيذ مثل ملفات ذات امتداد (.EXE ,.DLL, COM) ضمن أنظمة التشغيل (دوس وميكروسوفت ويندوز)، أو (ELF) في (أنظمة) لينكس)، وسجلات الملفات والبيانات – VOL UME BOOT RECORD) في الأقراص المرنة والصلبة والسجل رقم (٠) في القرص الصلب MASTER BOOT، وكذلك ملفات الأغراض العامة مثل ملفات الباتش والسكريبت في ويندوز) وملفات (الشل في يونيكس)، وملفات الاستخدام المكتبي في نظام تشغيل (مايكروسوفت ويندوز) التي تحتوي ماكرو) مثل مايكروسوفت وورد ومايكروسوفت إكسل ومايكروسوفت أكسس)، وقواعد البيانات وملفات (الأوتو) لوك) لها دور كبير في

---

(١) محمد صبحي نجم. (٢٠١٠)، قانون العقوبات القسم العام، الطبعة الثالثة، دار الثقافة للنشر والتوزيع، الأردن.ص. ٢١١

(٢) مجدي أبو العطا. (٢٠١٦)، أمن المعلومات والإنترنت، الطبعة الأولى، شركة علوم الحاسبة (كمبيوسانيس)، مصر.ص. ٣٤

الإصابة ونشر الإصابة لغيرها لما تحتويه من عناوين البريد الإلكتروني، والملفات من النوع نسق المستندات المنقولة) وبعض نصوص لغة ترميز النص الفائق احتمال احتوائها على كود خبيث، والملفات المضغوطة مثل ((ZIP وملفات (mp3) وغيرها من الملفات الملحقة[١].

وبالتالي؛ تتصور النتيجة الجرمية بمجرد وصول الفيروسات إلى آلاف الضحايا، وبالتالي؛ تعتبر الجريمة قائمة حتى لو وصل الفيروس إلى مستخدم في دولة أخرى، بحيث يكون الهدف من نشر الفيروسات هو تعطيل الأجهزة والبرامج الإلكترونية، أو حذفها أو تعديلها البيانات التي تحتويها، وهو ما أشار إليه المشرع الفلسطيني في المادة السادسة من القرار بقانون رقم ١٠ لسنة ٢٠١٨ بشأن الجرائم الإلكترونية، حيث يمكن ملاحظة هذه الفيروسات من خلال أعراض تظهر على جهاز الحاسوب الخاص في المستخدم في بعض الأحيان، كتكرار رسائل الخطأ في أكثر من برنامج، وظهور رسالة تعذر الحفظ لعدم كفاية المساحة، وتكرار اختفاء بعض الملفات التنفيذية، بالإضافة إلى حدوث بطء شديد في بدء تشغيل إقلاع نظام التشغيل أو تنفيذ بعض التطبيقات، كذلك رفض بعض التطبيقات الإلكترونية لأوامر التنفيذ[٢].

ويكمن السبب الرئيس وراء هذه الأنواع من الأنشطة هو إنشاء برنامج خبيث معين يعرف باسم البرامج الضارة لخاطف المتصفح ، ويستخدم هذا الرمز لتمهيد الطريق لأنواع مختلفة من الهجمات الإلكترونية على جهاز الحاسوب الخاص أو على أجهزة الحاسوب الأخرى على الشبكة.

---

(١) يوسف المصري. (٢٠١١) ، الجرائم المعلوماتية والرقمية للحاسوب والإنترنت، الطبعة الأولى، دار العدالة، مصر. ص. ٩

(٢) عبد الله ذيب محمود، جرائم الإعتداء على البرامج الإلكترونية في التشريعات الفلسطينية، مرجع سابق، ص.٨٤

ثانيا: الركن المعنوي لجريمة إرسال البرمجيات الخبيثة Malware

تجدر الإشارة هنا إلى أن هذه الجريمة تعتبر من الجنايات التي تقع ضمن اختصاص المحاكم الإبتدائية، حيث يعاقب الجاني بالسجن، وبغرامة مالية، ويلاحظ أن المشرع جعل عقوبة هذه الجريمة مشددة بسبب الأضرار الكبيرة التي يمكن أن تصيب الأجهزة الإلكترونية والخسارات المالية أو الاقتصادية نتيجة تعطيل البرامج الإلكترونية، وخصوصا أن معظم التجارة أصبحت الكترونية. مع الإشارة إلى أن محل الحماية هو البرامج والأجهزة الإلكترونية والبيانات والمعلومات الموجودة عليها، كما يلاحظ أن المشرع جعل عقوبة السجن ملازمة لعقوبة الغرامة.

المطلب الثالث
المسئولية الجنائية لمزودي خدمة الإنترنت
عن إرسال البرمجيات الخبيثة Malware

يطلق على مزود الخدمة تسميات كثيرة منها متعهد الوصول أو متعهد الخدمة أو مقدم الخدمة الذي قد يكون شخصا طبيعيًّا أو معنويًّا، ويقصد به هو من يقدم للجمهور خدمة الاتصال بشبكة الإنترنت، فهو إذن لا يقدم المعلومات ولكن يحقق اتصال الغير بالشبكة، وليس له سيطرة علي المادة محل البث، لكن يمكن تدخله لقطع هذا الاتصال إذا لاحظ مخالفات تتعلق بمحتوي تلك المادة(١) وقد عرفه القانون الفرنسي الصادر في سنة ٢٠٠٠ بأنه الذي " يقوم بمقابل أو بدون مقابل بالتخزين المباشر والدائم لإشارات أو مكاتب أو صور أو رسائل من أى نوع يمكن الحصول عليها تُوضع تحت تصرف الجمهور(٢). ويتصف عمل مزود الخدمة بأنه عمل ذو طبيعة فنية، فهو الذي يمكن مستخدمي الإنترنت من الوصول إلى المواقع أو البريد الالكتروني للأطراف الأخرى في المحادثة(٣)؛ حيث يتمثل دوره في ربط مستخدمى الإنترنت بالشبكة عن طريق عقود اشتراك تؤمن لهم هذه الخدمة.

وقد بنى القضاء هذه المسئولية على أسس متعددة. فاتجه رأى في الفقه إلى أن دور مزود الخدمة عبر الشبكة يقتصر على ربط المستخدم بالموقع الذي يريده، فهو مجرد دور فنى خالص لا يتضمن أية رقابة على مضمون أو محتوى الموقع الذي يختاره المستخدم بمحض

---

(١) د/ عبد الفتاح بيومي حجازي، الكتاب الأول، النظام القانوني للحكومة الالكترونية، دار الفكر الجامعي، ٢٠٠٣، ص٣٤٤& د/ جميل عبد الباقي الصغير، الانترنت والقانون الجنائي، الأحكام الموضوعية للجرائم المتعلقة بالانترنت، دار النهضة العربية، ٢٠٠١، ص ١١٥.

(2) 1 article 43-8 de la loi n 2000-719 dispose que (assurent a titre gratuity ou onéreux. le stockage direct et permanent pour mise a disposition du public de signaux. d'écrits. d'images de sens ou de messages de toute nature accessible par ces services).

(٣) د/ محمد حسين منصور، المسئولية الإلكترونية، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٣، ص٢٠٩.

إرادته[١] . وعلة ذلك أن عمل مزود الخدمة يشبه شخصا نصح المستخدم بأن يشترى صحيفة أو يشاهد قناة تليفزيونية تبث محتوى غير مشروع[٢] . أما غالبية الفقه فيرى أن مسئولية مزود الخدمة تتوقف على نوع الخدمة التي يؤديها. فإذا اكتفى بدوره الأصيل في ربط مستخدم الإنترنت بالشبكة فهو غير مسئول عن عدم مشروعية المحتويات التي تبث عبر الموقع. أما إذا تعدى دوره المنوط به وقام بوظيفة متعهد الإيواء الذى يسمح لمستغل الموقع من نشر المضمون الذي يبغيه هنا يمكن مساءلته عن المحتوى غير المشروع؛ لقدرته على الإطلاع على المحتوى قبل نشره [٣].

أما القضاء فلم تستقر أحكامه على مسئولية مزود الخدمة، فتارة يقيم مسئوليته، وتارة أخرى يبرئ ساحته. فقد أكدت المحكمة الابتدائية في باريس في أكتوبر ١٩٩٩ في قضية EDV عدم مسئولية مزود الخدمة عن طبيعة ومشروعية المعلومات المقدمة للمستخدمين؛ بحجة أن عمله قد اقتصر على نقل المعلومات من الموقع إلى المستخدم[٤]. وفي قضية اتحاد الطلاب اليهود التي رفعها ضد شركة Yahoo باعتبارها مزود خدمة، انتهت المحكمة إلى أنها تعد مسئولة عن المحتويات غير المشروعة (بيع أشياء متعلقة بالنازية المتاحة عبر الموقع منذ تحقق العلم بالمحتوى غير المشروع"[٥].

---

(١) د/ سمير حامد عبد العزيز الجمال، التعاقد عبر تقنيات الاتصال الحديثة، دار النهضة العربية، الطبعة الأولى، ٢٠٠٦، ص ٢٩٨.

(٢) فى ذات الاتجاه تبنى الفقه والقضاء الإيطالى عدم مسئولية مزود الخدمة ؛ لأنه لا يقوم بتوريد هذه المعلومات، ولكنه يؤمن خدمة الوصول إليها فقط. راجع:

LEBRUN (N.) et MBEUTCHA (E.), Evolution de la responsabilité des intermediaries techniques en Italie, in http://www.juriscom.net/variations/ responsabilité des intermediaries techniques en Italie.html 12/12/2010, P.2.

(3) SÉDALLIAN (V.), Droit de l'Internet: réglementation, responsabilités, contrats, Net Press, 1997, P.15.

(٤) راجع وقائع القضية في:

http://www.afa-france.com/html/action/jugement2.html19/12/2010

(5) TGI, Paris, 22 mai 2000, ligue internationale contre le racisme et l'antisémitisme Union des Etudants Juifs France, in"
http://www.legalis.net/breve-impimer.php3?id article=736 19/12/2010

ويتضح من أحكام القضاء الخاصة بمسئولية مزود الخدمة أنها تشير إلى أن مناط مسئولية مزود الخدمة يرتبط بعلمه بمحتوى الموقع الذي يربط بينه وبين مستخدم الشبكة. فانتفاء العلم بالمحتوى غير المشروع يُفيد عدم قدرته على القيام بأية رقابة سابقة، أما علمه بمضمون المحتوى دون منع المستخدمين من الوصول إلى ذلك الموقع يقيم مسئوليته منذ تمام العلم؛ لقدرته على القيام بالرقابة من خلال غلق الخدمة أو قطع الاتصال بها وهو ما يتضح في قضية اتحاد الطلاب اليهود؛ حيث قضت المحكمة بإلزام مزود الخدمة بمنع وصول المستخدمين الفرنسيين إلى الموقع منذ العلم بالمحتوى غير المشروع[١].

أولا: المسئولية عن مسألة مزودي خدمة الإنترنت

تم التوصل إلى إقرار مسئولية مقدمي خدمات الإنترنت إذا كانت لديهم المعرفة الفعلية عن المحتوى غير القانوني الموجود على السيرفرات الخاصة بهم. ويؤكد ذلك ما نصت عليه نصوص القانون المدنى الإنجليزي في الفصل الأول منه والخاص بالتشهير[٢] الصادر عام ١٩٩٦ الذى ينص على أنه في خصوص إجراءات التشهير، يكون للشخص حق الدفاع عن نفسه اذا أثبت ما يدل على أنه

١ - لم يكن صاحب البلاغ، أو المحرر أو الناشر للبيان محل الشكوى.

٢ - بذل العناية المعقولة فيما يتعلق بمشروعية النشر.

---

(١) اعترض المستخدمون الفرنسيون على الحكم للصعوبة الفنية في منع وصول المستخدمين الفرنسيين إلى الموقع؛ لأن غلقه يعني غلق الموقع تماما على كل الدول وليس فرنسا فقط يُضاف إلى ذلك أن المستخدمين الفرنسيين يمكنهم الوصول إلى الموقع بعناوين إلكترونية تابعة لدول أخرى. راجع أكمل يوسف السعيد يوسف، المسئولية الجنائية لمقدمي المواد الإباحية للأطفال عبر الإنترنت، مجلة البحوث القانونية والاقتصادية، جامعة المنصورة، كلية الحقوق، ٢٠١١، ص. ٤

(2) A similarity can be found in civil law within section 1 of the Defamation Act 1996 in England and Wales which provides that: In defamation proceedings a person has a defence if he shows that -
(a) he was not the author, editor or publisher of the statement complained of,
(b) he took reasonable care in relation to its publication, and
(c) he did not know, and had no reason to believe, that what he did caused or contributed to the publication of a defamatory statement.

٣- لم يكن يعرف، وليس لديه سبب للاعتقاد بأن ما فعله تسبب أو أسهم في نشر بيان التشهير. وإذا كان الفصل الأول من قانون ١٩٩٦ يشير مباشرة الى مسئولية مقدمي خدمات الإنترنت، إلا أنه لا يوجد في النظام الجنائي الإنجليزى ما يوجب المسئولية الجنائية لمزودي خدمات الإنترنت[١]. وفي هذا الصدد أصدرت وزارة التجارة والصناعة الإنجليزية جدول أعمال التجارة الإلكترونية في المملكة المتحدة في أكتوبر (١٩٩٨)[٢]، الذي أجاب بشكل واضح على إمكانية وجود مسئولية رئيسة عن المواد غير المشروعة عبر الإنترنت من فرد أو كيان قام بنشرها. فبموجب القانون الإنجليزي، تقوم مسئولية مزودي الخدمات بوصفهم شركاء في الجريمة عن المواد أو الأنشطة غير المشروعة، إذا فشلوا في اتخاذ خطوات معقولة لإزالتها"[٣].

وأشار الجدول إلى أن العلم بتحميل المحتويات غير المشروعة يجلب مسئولية مزودي خدمات الإنترنت في المملكة المتحدة، على الرغم من أن المعرفة الفعلية ليست الشرط المنصوص عليه في قانون ١٩٧٨ . وعلاوة على ذلك، أدى التعاون بين وزارة الصناعة في المملكة المتحدة والشرطة، إلى إنشاء منظمة مراقبة الإنترنت من قبل رابطة مزودي خدمات الإنترنت التي تختص بوضع مدونة لقواعد السلوك (ISPA)[٤]. وتأخذ المحاكم بما يصدر

---

(1) Section 3 of the 1978 Act states, where a body corporate is guilty of an offence under this Act and it is proved that the offence occurred with the consent or connivance of, or was attributable to any neglect on the part of, any director, manager, ... he, as well as the body corporate, shall be deemed to be guilty of that offence and shall be liable to be proceeded against and punished accordingly.' See, for an interpretation,G. LEONG, 'Computer Child Pornography: The Liability of Distributors?' (1998), Crim. L.R., Special Edition: Crime, Criminal Justice, and the Internet, December, 19-29.

(2) DTI, Net Benefit: the electronic commerce agenda for the UK, DTI/Pub 3619, October 1998. See also Speech by Mrs. Barbara Roche MP at the OECD Electronic Commerce Ministerial Meeting, Ottawa: 9 October 1998

(3) Under UK law, however, an Internet Service Provider which has been made aware of the illegal material (or activity) and has failed to take reasonable steps to remove the material could also be liable to prosecution as an accessory to a crime.
Y. AKDENIZ, Internet Child Pornography and the Law National and International Responses University, P.R., P.251.

(4) Internet Service Providers Association

عنها من معلومات بوصفها أدلة على قيام مقدمي خدمات الإنترنت ببذل الجهود المعقولة للامتثال للقانون[١].

وعلى الرغم من وجود نصوص جنائية في قانون ١٩٧٨، فإن النظام الجنائي للمملكة المتحدة قد أقر تجنب الملاحقة القضائية في المحاكم إذا كان مزودو خدمات الإنترنت قد تعاونوا بشكل كافٍ وفعال منظمة مع مراقبة الإنترنت وما تفرضه من إجراءات الإعلام والإخطار وإنهاء الخدمة. وقد انتقدت فكرة المسئولية، وفق الوضع الحالي في القانون الإنجليزي لعدم الوضوح واليقين. وأمام ذلك الغموض يجب أن تفسر تلك المسألة في ضوء التطورات الأوروبية، وتوجيهات الاتحاد الأوروبي[٢]. ويسير جنبًا إلى جنب مع تلك التوجيهات إدخال شرط المعرفة الفعلية لإزالة المحتوى من الأوروبي" قبل مقدمي خدمات الإنترنت[٣]، والإخطار عن تلك المحتويات[٤] ويمكن تقديم هذه الإخطارات إما عن طريق الخطوط الساخنة مثل مؤسسة مراقبة الإنترنت في إنجلترا، أو من قبل شركات خاصة

(1) On this issue Net Benefit stated: Compliance with this code of practice (essentially the removal of material from their UK servers following IWF notification) would likely be taken in court as evidence of the ISP having made reasonable efforts to comply with the law. Y. AKDENIZ, Internet Child Pornography and the Law National and International Responses University, P.R., P.251.

(2) European Commission, 'Proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the internal market', COM(1998) 586 final, 98/0325 (COD), Brussels, 18 November 1998; European Commission, Amended proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the Internal Market (presented by the Commission pursuant to Article 250 (2) of the Entreaty), COM(1999) 427 final, 98/0325 (COD). Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') v 43, OJ L 178, 17 July 2000, p. 1.

(3) Articles 13 and 14 of the Directive.

(4) For a critique of notice and takedown provisions in relation to defamation, see Cyber- Rights and Cyber-Liberties (UK) Press Release, 'UK ISP found liable for defamation', 26 March 1999, at <http://www.cyber-rights.org/press20/10/2010; R. UHLIQ, 'Libel setback for Demon', Daily Telegraph, 'Connected' Section, 1 April 1999; and Y. AKDENIZ, 'The case for free speech', Guardian (Online Section), 27 April 2000.

أو أفراد لإزالة أشكال أخرى من المحتويات بما في ذلك المحتويات التي تنتهك حقوق الطبع والنشر والعلامات التجارية[١]. فكان مقدمو خدمات الإنترنت هدفًا للدعاوى الخاصة بحقوق الطبع والنشر[٢]، ودعاوى التشهير في كل من الولايات المتحدة[٣] والمملكة المتحدة[٤]، كما كانوا متهمين بارتكاب جرائم جنائية متعلقة بتوفير المواد الإباحية داخل الولايات الأعضاء في الاتحاد الأوروبي، وتحديدًا ألمانيا[٥]. وفرنسا [٦]. وأصبح مقدمو خدمات الإنترنت هم الأشخاص المشتبه بهم عادة لتوفير هذه المواد عبر الإنترنت في هذه الحالات[٧].

(1) This is already possible under section 1 of the Defamation Act, and 'notice and takedown' is common practice for the removal of content alleged to be defamatory. Y. AKDENIZ, 'Case Analysis: Laurence Godfrey v. Demon Internet Limited' (1999), Journal of Civil Liberties, 4(2), 260-67; 'Cyber-Rights and Cyber-Liberties' (UK), Hulbert's Case, the Lord Chancellor and Censorship of the Internet, 11 November 1999; and Y. AKDENIZ. and W.R.H. ROGERS, 'Defamation on the Internet', in Y. AKDENIZ, C. WALKER and D. WALL (eds), The Internet, Law and Society, Harlow: Addison Wesley Longman, 2000, 294–317. 30 This is the case in the United States with the Digital Millennium Copyright Act 1998

(2) Religious Technology Center v. F.A.C.T.Net, Inc., 901 F. Supp. 1519 (D. Colo. 1995), Religious Technology Center v. Netcom On-line Communication Services, Inc., 907 F. Supp. 1361 (N.D. Cal. 1995).

(3) Cubby, Inc. V. CompuServe Inc. 776 F. Supp. 135 (1991), Stratton Oakmont, Inc. v. Prodigy Servs. Co. 23 Media L. Rep. (BNA) 1794 (1995), and Kenneth M. Zeran v. America Online, Inc. U.S. District Court, E.D. Virginia, 958 F.Supp (1997); U.S Court of Appeals, 4th Circuit, CA-96-1564-A, 129 F.2d 327 (1997); U.S. Supreme Court, Certiorari denied, Pet. 97-1488.

(4) Godfrey v. Demon Internet Ltd, QBD, [1999] 4 All ER 342; [2000] 3 WLR 1020; [2001] QB 201. See further, Y. AKDENIZ, 'Case Analysis: Laurence Godfrey v. Demon Internet Limited' (1999), Journal of Civil Liberties, 4(2), 260–67.

(5) C. MACAVINTA, CompuServe manager convicted', Cnet News.Com, 28 May 1998.

(6) The managers of two Internet providers, WorldNet and France Net, have been charged with distribution of child pornography on 'alt.binaries' newsgroups. They faced the possibility of three years in jail and £65,000 fines. See Rooney, B., 'Net porn crackdown', Daily Telegraph, 15 May 1996.

(7) Y. AKDENIZ, "To Link or Not to Link: Problems with World wide web links on the Internet' (1997), International Review of Law, Computers and Technology 11(2), 281-98.

وفي هذا الصدد يقدر بعض الفقه علم مزود الخدمة الفعلي بمحتوى الموقع بالحالة الظاهرة للمحتويات التي تضمنها الموقع. فإذا كانت المواد ظاهرا عدم مشروعيتها أو تتضمن اعتداءات على حقوق الأطفال ويسهل لأى شخص التعرف عليها، قام الدليل على علم مزود الخدمة بعدم المشروعية. فإذا استبان له ذلك تقوم مسئوليته الجنائية إن استمر في تقديم خدمة الوصول إلى ذلك الموقع(١).

ثانيا: موقف الاتحاد الأوروبي بشأن بعض الجوانب القانونية لأمن المعلومات(٢).

أشار توجيه الاتحاد الأوروبي إلى أن الاختلافات بين الدول الأعضاء في التشريعات والسوابق القضائية المتعلقة بمسئولية مقدمي خدمات الانترنت قد أدى إلى التأثير على حسن سير الخدمات المتاحة في مجتمع الإنترنت، في إشارة منه إلى قضية CompuServe prosecution in Germany

واقترح التوجيه أن تلتزم جميع الدول الأطراف المعنية بتوفير خدمات مجتمع المعلومات بعد اعتماد وتنفيذ الإجراءات التي تزيل وتعيق الوصول إلى المعلومات غير المشروعة، في حين أكد على عدم التزام الوسطاء الفنيين برقابة مشروعية المعلومات التي تبث عبر الإنترنت. إلا أن التوجيه قد أورد بعض الاستثناءات التي تحدد شروط الإبراء من المسئولية على أساس نوع النشاط وليس نوع الوسط القائم بالنشاط،(٣). وهى الحالات التي تعتمد فيها أنشطة مزودي خدمات مجتمع المعلومات على العملية التقنية للتشغيل –

(1) HERTZ - ELCHENRODE (CH.), Questions juridiques du droit allamand relative à; a publicité sur internet, Gaz. Pall., 1997,II, doct.,P.1513

(2) Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, Official Journal of the European Communities, v 43, OJ L 178, 17 July 2000, p. 1. Note also Common Position (EC) No. 22/2000 of 28 February 2000 adopted by the Council, acting in accordance with the procedure referred to in Article 251 of the Treaty establishing the European Community, with a view to adopting a Directive on electronic commerce, OJ C 128, 8 May 2000 pp. 32-50.

(3) Section 4 of the Directive: Liability of intermediary service providers: Articles 12 (Mere Conduit), 13 (Caching), 14 (Hosting), 15 (No General Obligation to Monitor).

إجراءات تقنية أوتوماتيكية أو آلية – في تعزيز الوصول إلى شبكة الاتصالات، وهو ما يجعل المعلومات متاحة من قبل أطراف أخرى تبثها أو تقوم بتخزينها مؤقتا من أجل إجراءات نقل أكثر كفاءة. مما يعني أن مزودي خدمات الإنترنت أثناء ممارستهم تلك الأنشطة ليست لديهم المعرفة ولا السيطرة على المعلومات التي تبث أو التي يتم تخزينها. وعلى الرغم من ذلك يمكن أن تختلف اتجاهات المحاكم في المطالبة بإنهاء أو منع أي انتهاك، بما في ذلك إزالة المعلومات غير المشروعة أو تعطيل الوصول إليها.

ويختص الفصل الرابع من التوجيه الأوروبي المتعلق بمسئولية مقدمي الخدمات عن العمليات الوسيطة بمعالجة هذه القضايا في المادة ١٢ منه وهي المتعلقة بالنقل المجرد أو البسيط للمعلومات وبموجب هذه المادة ١٢ (١) يجب أن تكفل الدول الأعضاء حماية مزودي خدمات المعلومات من المسئولية عن المعلومات المنقولة غير المشروعة التي يتضمنها الموقع، بشرط أن يكون مزود الخدمة لم يبدأ النقل لم يكن مصدر الضرر) أو لم يحدد المتلقي أو المرسل إليه المعلومات أو لم يحدد أو يعدل المعلومات محل النقل[١].

ومن شأن ذلك أن يغطي التخزين التلقائي والوسيط والناقل للمعلومات التي لم يتم تخزينها لفترة أطول من الفترة المعقولة الضرورية للنقل بموجب المادة (١٢(٢) بما يفيد عدم مسئولية مزود الخدمة عن التخزين التلقائي المؤقت؛ لأن عمله لم يصل بعد إلى عمل متعهد الإيواء بشرط أن يكون التخزين ضروريًّا لنقل المعلومات وأن يستمر لمدة قصيرة تقتضيها إجراءات النقل. ولا تؤثر أحكام تلك المادة على قدرة المحكمة أو السلطة الإدارية – وفقا للنظم القانونية في الدول الأعضاء أن تلزم مزود الخدمات إنهاء أو منع حدوث تلك الانتهاكات"[٢].

---

(1) Article 12 deals with the issue of mere conduit' and under article 12(1) 'Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:
(a) does not initiate the transmission;
(b) does not select the receiver of the transmission; and
(c) does not select or modify the information contained in the transmission
(2) Article 12 (3).

فالقضايا ذات الصلة بنقل أو تحميل المعلومات (مثل التخزين المؤقت) من مزودي خدمة الإنترنت إلى مستخدميها بموجب المادة ١٣ (١)، تتطلب من الدول الأعضاء التأكيد على عدم مسئولية مزودي الخدمة عن التخزين التلقائي والوسيط والتخزين المؤقت لتلك المعلومات التي تتم لغرض واحد هو إجراءات نقل أكثر كفاءة للمعلومات إلى المتلقين للخدمة بناء على طلبهم- بشرط:

١ - عدم تعديل مزودي الخدمة للمعلومات.

٢ - قدرة مزودي الخدمة على التعامل مع ظروف الوصول إلى المعلومات.

٣ - قدرة مزودي الخدمة على التعامل مع القواعد المتعلقة بتحديث المعلومات، المعترف بها على نطاق واسع والتي يتم استخدامها من قبل منتجيها.

٤ - عدم تعارض استخدام مزودي الخدمة مع الاستخدام القانوني للتكنولوجيا المعترف بها على نطاق واسع التي يتم استخدامها من قبل منتجيها، بهدف الحصول على بيانات عن استخدام تلك المعلومات.

٥ - قيام مزودي الخدمة على وجه السرعة بإزالة أو تعطيل الوصول إلى المعلومات المتوفرة لديها والمخزنة، التي من شأنها الحصول على المعرفة الحقيقية عن مصدر تلك المعلومات، سواء من تلقاء نفسها أم بناء على أمر من المحكمة أو السلطة الإدارية.

وإذا كانت المادة ١٢ توجب إنهاء أو منع حدوث التعدي أو الانتهاك من قبل المحكمة أو أمر إداري من السلطة الإدارية، فإنه بموجب المادة ١٤(١) يمكن تقرير عدم مسئولية مزودي الخدمة عن المعلومات المخزنة بناء على طلب المستفيد من الخدمة، بشرط :

١ - غياب المعرفة الفعلية لمزودي الخدمات سواء عن عدم قانونية النشاط أم المعلومات، وكذلك عدم مسئوليتهم عن المطالبات أو الدعاوى المتعلقة بالأضرار؛ نظرا لغياب الوعي الواضح والكافي عن الوقائع أو الظروف التي من شأنها أن تجعل النشاط أو المعلومات غير قانونية.

٢ - وإذا توافرت مثل هذه المعرفة أو الوعي، فإنه على مزودي الخدمة القيام على وجه السرعة بالأفعال التي تُزيل أو تعطل الوصول إلى تلك المعلومات غير القانونية.

ومما سبق يتضح أن هذا التوجيه بما يتضمنه من نصوص لا يوفر حماية مطلقة لمزودي خدمات الإنترنت، بل يلزم الأخير باتخاذ إجراءات سريعة لإزالة أو تعطيل الوصول إلى المعلومات غير المشروعة، وذلك بعد تحقق المعرفة الحقيقية أو الفعلية. ويجب أن تراعي هذه الإجراءات النظم القانونية للدول الأعضاء دون الافتئات على حرية الرأي والتعبير المكفولة قانونًا[١]. كما لا تؤثر المواد السابقة على قدرة المحاكم أو السلطات الإدارية فى منع وإزالة المعلومات والمحتويات غير المشروعة[٢].

وبالإضافة إلى ما سبق، يمنع التوجيه بموجب المادة ١٥ الدول الأعضاء من فرض واجب الرقابة على مقدمي الخدمات أثناء تقديم الخدمات التي تشملها المواد ١٢ ودون التعرض للالتزامات العامة أو القرارت الإدارية الصادرة من السلطات الوطنية وفقًا للتشريعات الوطنية. ومع ذلك، فإن الدول الأعضاء قد تُنشىء التزامات على مزودي الخدمات بإبلاغ السلطات العامة المختصة على وجه السرعة عن الأنشطة غير المشروعة من تلقاء نفسها أو بناء على طلبها.

وعلى الرغم من وجود الالتزامات العامة بالمراقبة على مزودي الخدمات، فإنها لم تمنع الدول الأعضاء من إصدار أوامر حظر لبعض المواقع والصفحات. ففي عام ٢٠٠٢ أصدرت الحكومة الألمانية أمرًا إلى مزودي الخدمات بمنع سبل الوصول إلى المواقع الموجودة خارج ألمانيا وخاصة في الولايات المتحدة، التي تحرض على العنصرية والأفكار النازية"[٣].

---

(1) Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee - First report on the application of Directive 2000/31/EC on November 2003, at electronic commerce, COM(2003) 702 final, Brussels, 21 http://europa.eu.int/eur-lex/en/com/rpt/2003/com2003_0702en01.pdf, section 4.7.

(2) Out of those Member States which have transposed the Directive, only Finland has included a legal provision setting out a notice and take down procedure concerning copyright infringements only: This information has been taken from the above-mentioned Commission Report: COM(2003) 702 final.

(3) Ban on neo-Nazi web content in German state; upheld', National Journal's Technology Daily, 22 December 2004. Between 2002 and 2004 the Düsseldorf District Administration issued 90 ordinances against Internet

على الرغم من وجود جدل دائر رحاه بين المحاكم حول قانونية الحظر ومدى الالتزام به، إلا أن عددا كبيرا من الأحكام الصادرة من المحاكم الإدارية الألمانية قد أكدت أحقية السلطات الألمانية في أن تستمر بطلبها لمقدمي خدمات الإنترنت لمنع مثل هذه الصفحات والمواقع. فقد بعث Jurgen Bussow رئيس المحكمة في مقاطعة Dusseldorf قبل إصدار أمر الحجز، إلى أربعة من مقدمي ٢٠٠٠ يطلب منها منع الوصول إلى المواقع التي خدمات الإنترنت في الولايات المتحدة في أغسطس تحتوي على الأفكار المناهضة لقيم المجتمع كالعنصرية والنازية والإباحية وتأكيدًا على تفعيل هذا الإجراء بعث أيضا إلى أربعة من مزودي خدمات الإنترنت الألمانية من أجل عرقلة إصدار تلك الصفحات والمواقع"[1].

ثالثا: موقف الولايات المتحدة بشأن مسئولية مقدمي خدمات الإنترنت:

اعتمدت الولايات المتحدة نهجًا مختلفًا لمسئولية مقدمي خدمات الإنترنت؛ حيث تفرض مزيداً من الحماية لمزودي خدمات الإنترنت، واعتبرتهم طرفًا ثالثًا في علاقة ثنائية بين متعهدى الإيواء والمستخدم، يتم فيها نقل واستقبال المعلومات ومختلف خدمات الإنترنت عبر السيرفرات Servers دون معرفة أو علم منهم بماهيتها.

فالفصل ١/ C/230 من قانون سرية الاتصالات ١٩٩٦ ينص على أنه لا يعامل مزودو خدمات الإنترنت والمستخدمون بوصفهم ناشرين أو محدثين للمعلومات والمحتويات

---

providers in North Rhine-Westphalia, forcing them to block access to certain websites with rightwing extremist content. See US Bureau of Democracy, Human Rights, and Labor, Report on Global Anti-Semitism, January 2005, at <http://www.state.gov/g/drl/ rls/40258.htm18/11/2010. Note also Combating racism, racial discrimination, xenophobia and related intolerance and comprehensive implementation of and follow-up to the Durban Declaration and Programme of Action Note by the UN Secretary- General, A/59/330, 4 October 2004.

(1) E.T. EBERWINE, 'Note and Comment: Sound and Fury Signifying Nothing?: Jurgen Bussow's Battle against Hate-speech on the Internet' (2004), 49 N.Y.L. Sch. L. Rev 353; and C.D. VAN BLARCUM, 'Internet Hate Speech: The European Framework and the Emerging American Haven' (2005), 62 Wash and Lee L. Rev 781.

المقدمة عبر معلومات ومحتويات ويقصد بذلك أن الفصل ١/ C/230 لا ينطبق إلا على المعلومات والمحتويات مزودي الخدمات[١].

ويقصد بذلك أن الفصل ٢٣٠/ C/1 لا ينطبق إلا علي المعلومات والمحتويات التي تنتقل عبر السيرفرات الخاصة بهم من خلال أطراف أخرى متعهدى الإيواء والمستخدم)، في حين تقوم مسئوليتهم عن المعلومات التى يتم إنشاؤها وتطويرها من قبل مزودي الخدمات.

ويهدف الكونجرس الأمريكي من هذا القانون إلى تعزيز التطوير المستمر للإنترنت وغيرها من خدمات الكمبيوتر ووسائل الإعلام بغية الحفاظ على حيويتها وقدرتها على المنافسة الحرة في سوق هذه الخدمات[٢]. ومع الاعتراف بسرعة نشر المحتويات واستحالة تنظيم مجتمع المعلومات، قرر الكونجرس الأمريكي عدم معاملة مقدمي خدمات الإنترنت كغيرهم من مزودي خدمات المعلومات الأخرى كالصحف والمجلات أو المحطات التلفزيونية والإذاعية، فجميعها لها الحق في التعبير بالقول أو الكتابة أو النشر إلا في حالة التعسف في استعمال الحق[٣].

---

(1) Section 230 defines interactive computer service' as any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.' 47 U.S.C. § 230(e)(2). The term 'information content provider' is defined as 'any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service.' Ibid, § 230(e) (3). The statute goes on to define the term 'Information content provider' as 'any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service.' 47 U.S.C. § 230(e) (3)However, for copyright infringement a different policy has been established with the passage of the Digital Millennium Copyright Act (H. R. 2281) 1998.

(2) 47 USC $ 230(b)(1) and (2).

(3) However, for copyright infringement a notice and actual knowledge-based liability policy has been established with the enactment of the Digital Millennium Copyright Act (H. R. 2281) 1998.

وتأسيسا على ما سبق فإن مبررات الحفاظ على الطابع القوي لمجتمع الانترنت، والتغير المتنامي في حجم المعلومات والتوازن بين دور القانون فى الحفاظ على النظام والآداب العامة وحق الأفراد في التعبير وحرية الكلام، قد أدى بالقضاء إلى إقامة قرينة تعمل كحد فاصل بين مختلف الحقوق من خلال الاعتداد بضابط عدم الإضرار بالغير.

وقد طبقت الدائرة الرابعة لمحكمة الاستئناف ما نص عليه الفصل C/1 /٢٣٠ في قضية التشهير Zeran . America Online Inc[1]، وقررت حماية قانونية بعدم الاعتداد بأى سبب إجرائي من شأنه أن يقيم مسئولية مزودي خدمات الإنترنت عن المعلومات والمحتويات التي يكون مصدرها مستخدم خدمات الانترنت. ولا يقدح في هذه الحماية القول بأن مزود الخدمات كان عليه مراقبة نقل المواد غير المشروعة. فقد منع الفصل C/230 /١ المحاكم من إقامة التماثل بين مزود خدمات الانترنت (متعهد الإيواء) ورؤساء تحرير الصحف، فالأخير تقوم مسئوليته عن ممارسته مهام النشر التقليدية بما يمارسه من دور رقابي قبل نشر المحتوى)تحديد ما يمكن نشره وما يمكن سحبه أو تأجيل نشره أو تغيير المحتوى أو منع نشره(فى حين أن مزود الخدمة يقوم بدور رقابي بعد نشر المحتوى؛ حيث يمكنه التدخل بغلق الموقع أو الصفحة التي تحتوى على مادة معاقب على نشرها.

(1) Zeran v. America Online [1997] 129 F3d 327. Note that Zeran was adopted by other state and federal appeal courts: Blumenthal v. Drudge (D.D.C. 1998) 992 F.Supp. 44, 51; Ben Ezra, Weinstein, and Co. v. AOL, Inc., 206 F3d 980, 986 (10th Cir. 2000); Doe One v. Oliver (Conn.Super.Ct. 2000) 755 A.2d 1000, 1003-4; Morrison v. America Online, Inc. (N.D.Ind. 2001) 153 F.Supp.2d 930, 933-4; Schneider v. Amazon.com, Inc. (Wn.App. 2001) 31 P.3d 37, 40-42; PatentWizard, Inc. v. Kinko's, Inc. (D.S.D. 2001) 163 F.Supp.2d 1069, 1071; Green v. AOL, 318 F3d 465, 471 (3d Cir. 2003); Batzel v. Smith, 333 F3d 1018, 1027 n.10 (9th Cir. 2003); Carafano v. Metrosplash.com, Inc. (9th Cir. 2003) 339 F3d 1119, 1123–4; Barrett v. Fonorow (Ill.App.Ct. 2003) 799 N.E.2d 916, 923–5; Donato v. Moldow (N.J. Super.Ct.App. Div 2005) 865 A.2d 711, 720-27; Austin v. CrystalTech Web Hosting (Ariz.App. 2005) 125 P.3d 389, 392-4. See further, Dowling, J., 'Noah v. AOL Time Warner: Are There Legitimate Barriers to Civil Rights Protection on the Internet? (2004), 14 Alb. L.J. Sci. and Tech. 775.

المطلب الرابع
الآليات التشريعية الدولية لمكافحة الفيروسات الخبيثة

يعتقد أن أول استخدام للسلاح البيولوجي كان علي يد القائد سولون، حيث استخدم جذور نبات الهيليوروس (وهو نبات الزين السام) في تلويث مياه النهر الذي يشرب منه أعداؤه، لإمراضهم وتسهيل اللحاق بهم لهزيمتهم ، وتوالت الأحداث بعد ذلك وبدأ تطور الأسلحة البيولوجية، ففي عام ١٩١٥ وأثناء الحرب العالمية الأولي اتهمت ايطاليا ألمانيا باستخدام ميكروب الكوليرا [١] في حربها ضدهم، وميكروب الطاعون في حربهم ضد الروس، وثبت بالفعل استخدام الألمان لبكتريا الأنثراكس العضوية في (بوخارست) من أجل نشر العدوى[٢].

ومن هذا المنطلق، ظهرت أولي المحاولات الدبلوماسية لتقليل انتشار مثل هذه الأسلحة بعد الحرب العالمية الأولي من خلال بروتوكول جنيف ١٩٢٥ الذي يمنع استخدام الوسائل البيولوجية، لكن لوحظ أن المعاهدة لم تمنع إجراء الأبحاث علي الأسلحة البيولوجية أو امتلاكها، ولهذا فقد زادت عدد الدول التي تجري أبحاثا علي هذا النوع من الأسلحة، وبعد الحرب العالمية الأولي أنشأت العديد من الدول كفرنسا وغيرها مختبرات لتحضير أنواع مختلفة من الفيروسات والجراثيم التي تستخدم بوصفها أسلحة بيولوجية مع إنتاج الأمصال المضادة لها.

---

(١)واحدة من أسرع الأمراض القاتلة، حيث ينخفض ضغط الدم في الشخص السليم في غضون ساعة من بداية ظهور أعراض المرض ، وقد يموت المرضي المصابون في غضون ثلاث ساعات إذا لم يتم تقديم العلاج الطبي، لمزيد من التفاصيل راجع

Mintz, Eric, Dr Guerrant Richard L. " A Lion in Our Village The Unconscionable Tragedy of Cholera in Africa" New England Journal of Medicine" 360 (11), 2009, p. 1060-10630.

(٢) د. صفا عزام، الحماية الدولية للبيئة من التلوث البيولوجي مع دراسة للجهود الدولية المبذولة لمكافحة جائحة كوفيد ١٩، مجلة الدراسات القانونية والإقتصادية، مصر: جامعة السادات، كلية الحقوق،المجلد ١٠، العدد الاول، مارس ٢٠٢٤، ص. ٣٨٢١

خلال الحرب العالمية الثانية اهتمت ألمانيا بالسلاح الكيميائي أما اليابان فاهتمت بالسلاح البيولوجي وكان مقر المعامل اليابانية في هربن قرب منشوريا، وقد تم الاستيلاء علي هذه المعامل من قبل الاتحاد السوفيتي ونقلت الأبحاث والتجارب إلي معامل بروسيا، حيث اعترف العلماء اليابانيون أمام محكمة مجرمي الحرب التي تم أسرهم بعد انتهاء الحرب العالمية الثانية بأنهم استخدموا الأسلحة البيولوجية ضد الجنود الصينيين في ١٩٤٢ وضد المدنيين الصينيين عن طريق نشر فئران وبراغيث تحمل ميكروب الطاعون[١].

أولا: الآليات الدولية لحماية البيئة الطبيعية والرقمية من التلوث البيولوجي والبرمجيات الخبيثة Malware

على الرغم من الاتفاقيات الدولية التي وقعتها الدول لمنع انتشار وإنتاج الأسلحة البيولوجية باعتبارها من أسلحة الدمار الشامل [٢] ، ومنع استعمالها في الحروب نجد أن بعض الدول لازالت تنتج الملوثات البيولوجية [٣]، وتنشرها بوسائل متعددة لإضعاف الشعوب، لدرجه أنها قد تنفق مبالغ طائلة علي العلاج ومكافحة الأمراض الناتجة عنه دون اكتشاف المسبب المباشر، بالإضافة للخسائر البشرية والحيوانية والزراعية [٤] التي تسببها ،

---

(١) راجع ستيف توليو وتوماس شمالبرغر ، نحو الاتفاق علي مفاهيم الأمن : قاموس مصطلحات تحديد الأسلحة ونزع السلاح وبناء الثقة، جنيف : الأمم المتحدة ٢٠٠٣ ، معهد الأمم المتحدة لبحوث نزع السلاح، UNIDIR/ 2003/ 22، ص ٣٩.

(٢) أن شبح الحرب البيولوجية هو شئ لا يحب أحد أن يواجهه ، غير أن هذا الشبح حقيقي لأن الإنسان تعلم كيف يستعمل البيولوجيا لشن الحرب علي نفسه ، ولحسن الحظ فإن المجتمع الدولي قرر في عام ١٩٧٢ أن الأسلحة ليست مشروعة ، راجع فالنتين أ. رومانوف، البعد الإنساني لاتفاقية الأسلحة الصامتة، المجلة الدولية للصليب الأحمر ، السنة العاشرة ، العدد ٥٥، مايو ١٩٩٧، ص ٢٨٩

(٣) راجع د طلعت إبراهيم الأعرج ، التلوث الهوائي والبيئة، مطابع الهيئة المصرية العامة للكتاب، مصر، ١٩٩٩ ص١٤٨ .

(٤) د/ عامر طراف ، التلوث البيئي والعلاقات الدولية المؤسسة الجامعية للدراسات بيروت الطبعة الأولي ٢٠٠٨م ، ص ٦٣.

لذلك زاد قلق المجتمع الدولي ازاء احتمالات تجاهل القيود المفروضة علي استخدام الأسلحة البيولوجية[١] بسبب التطورات الحديثة في العلوم الحيوية والتكنولوجيا البيولوجية.

وبدأت الجهود الدولية في الظهور بداية من **بروتوكول جنيف لعام** ١٩٢٥ الذي اتفقت فيه الأطراف علي منع استخدام الأساليب والوسائل الجرثومية في الحرب، وهنا نلاحظ أنه برغم أن الاتفاقية حظرت استخدام الوسائل الجرثومية إلا أنه لا يحظر إنتاج وتخزين وتطوير مثل هذه الوسائل.

وبذل المجتمع الدولي العديد من الجهود لوضع اتفاق جديد يكمل بروتوكول جنيف لعام ١٩٥٢، حيث تم فتح باب التوقيع علي **اتفاقية حظر الأسلحة البيولوجية عام ١٩٧٢م** ودخلت حيز النفاذ عام ١٩٧٥، والتي حظرت الدول الأطراف في الاتفاقية من استحداث أو إنتاج أو تخزين العوامل الجرثومية أو العوامل البيولوجية الأخرى وفقا لنص المادة الأولي من الاتفاقية[٢]. **وهنا نجد أن** الاتفاقية لم يرد فيها تكرار حظر استخدام الأسلحة البيولوجية، حيث سبق ورود هذا الحظر في بروتوكول ١٩٢٥ ، ولكن عززت هذا الأمر من ناحية أخري، بحظرها استحداث أو إنتاج أو تخزين مثل هذه الأسلحة.

كما تتعهد كل دولة من الدول الأطراف في الاتفاقية بعدم نقل أي من الوسائل الجرثومية أو البيولوجية بأي صورة من الصور سواء أكانت مباشرة أو غير مباشرة، وبألا تقوم بمساعدة أو تشجيع أو تحريض أية دولة أو مجموعة من الدول أو أية منظمة دولية على صنعها أو اقتنائها على

---

(١) راجع اللجنة الدولية للصليب الأحمر icrc.org

(٢) راجع دليل التنفيذ الوطني للقانون الدولي الإنساني، المركز الإقليمي للإعلام، مطبوعات اللجنة الدولية للصليب الأحمر ، القاهرة ، ٢٠١٠ ، الطبعة الأولي، ص ٧٨، د/ رشاد السيد ، حماية البيئة في المنازعات الدولية المسلحة، مجلة القانون والاقتصاد للبحوث القانونية والاقتصادية، العدد الثاني والستون، ١٩٩٢، ص ١٦ ، غراهام س. بيرسون، حظر الأسلحة. البيولوجية، الأنشطة الجارية وأفاق المستقبل، المجلة الدولية للصليب الأحمر، السنة العاشرة، العدد ٥٥ مايو ،١٩٩٧، ص ٢٧٨، ٢٧٩.

نحو آخر[١] ، كما تتعهد بتدمير جميع الوسائل الجرثومية أو البيولوجية التي بحوزتها أو خاضعة لولايتها أو رقابتها أو بتحويلها للاستعمال في الأغراض السلمية، ويكون التدمير أو التحويل خلال فترة لا تزيد عن تسعة أشهر بعد بدء نفاذ الاتفاقية[٢] . وتقضي بأن تتخذ الدول الأطراف تدابير تنفيذ وطنية، وتنص على حماية وتشجيع استخدام العلوم والتكنولوجيا البيولوجية للأغراض السلمية[٣].

كذلك نجد أن المادة ٣/ ٣٥ من **بروتوكول جنيف الأول عام** ١٩٧٧ حظرت استخدام وسائل أو أساليب القتال التي يقصد بها أو قد يتوقع منها أن تلحق بالبيئة الطبيعية أضرارا بالغة وواسعة الانتشار وطويلة الأمد، التي يمكن أن تتسبب في أضرار بالبيئة الطبيعية ومن ثم تشكل خطرا وتسبب أضرارا بصحة وبقاء السكان[٤]، ويفهم من هذه المادة حظر استخدام الأسلحة الجرثومية وغيرها من الأسلحة التي تلحق أضرارا بالبيئة، ومن هنا أصبحت الدول تلتزم بتعهدها بمنع استعمال العوامل الجرثومية في الحرب.

هذا وقد بذلت العديد من الجهود في التسعينيات لمعالجة القصور الموجودة في اتفاقية الأسلحة البيولوجية عام ١٩٧٢ ، ولكنها باءت بالفشل حينما سحبت الولايات المتحدة الأمريكية وقتها تأييدها مما أدي إلي نشوب خلافات بين الدول الأطراف بشأن مستقبل الاتفاقية، ومنذ ذلك الوقت، ينصب تركيز نشاط الدول الأطراف على تحسين وتنسيق تنفيذ

---

(١) راجع نص المادة ٣ من اتفاقية حظر استحداث وإنتاج وتخزين الأسلحة البيولوجية والمواد السامة وتدمير تلك الأسلحة لعام ١٩٧٢م

(٢) راجع نص المادة ٢ من اتفاقية حظر استحداث وإنتاج وتخزين الأسلحة البيولوجية والمواد السامة وتدمير تلك الأسلحة لعام ١٩٧٢م

(٣) ميليسا غيليس، نزع السلاح ، دليل أساسي، الأمم المتحدة ، نيويورك، ٢٠١٣، الطبعة الثالثة، ص ٤٧

(٤) بوعالم يوسف المساءلة عن الجرائم البيئية في القانون الدولي، مركز الدراسات العربية للنشر والتوزيع، الطبعة الأولي ٢٠١٥، ص ٧٤.

الاتفاقية على الصعيد الوطني، خاصة من خلال برنامج عمل سنوي يتناول مواضيع محددة وتبادل الخبرات التقنية بين طائفة من الأطراف الفاعلة والمنظمات المختلفة [١].

وعلي أثر ذلك، تم إنشاء اللجنة الخاصة للأمم المتحدة المعنية بالعراق عام ١٩٩١ لغرض تنفيذ القرار ٦٨٧ الذي يدعو إلى إزالة كافة أسلحة التدمير الشامل العراقية، هذا وقد عملت اللجنة بموجب ولاية لجمع المعلومات من أجل تقييم قدرات العراق في المجالات المتعلقة بالأسلحة البيولوجية والكيميائية والنووية والتخلص من كافة المخزونات العراقية من الأسلحة البيولوجية وغيرها من الأسلحة[٢]، كما تم إصدار إعلان مشترك بين الاتحاد الروسي وبريطانيا والولايات المتحدة بعد اجتماع عقد في موسكو في الفترة ما بين ١٠ ١١ أيلول/ سبتمبر ١٩٩٢، بهدف الامتثال لاتفاقية الأسلحة البيولوجية لعام ١٩٧٢، وأكدت الدول الثلاث التزامها بالامتثال التام لأحكام اتفاقية الأسلحة البيولوجية وتعهدت روسيا بإنهاء برنامج أسلحتها البيولوجية الهجومية الذي نفذه الاتحاد السوفيتي في الفترة ما بين ١٩٧١ و ١٩٩٢ متنافيا مع الاتفاقية، كما وافقت الأطراف الثلاثة علي إنشاء فرق عمل للبحث في التدابير المحتملة لرصد الامتثال للاتفاقية[٣] ، كما وضعت منظمة العمل الدولية اتفاقية رقم ١٥٥ عام ١٩٨١م التي أكدت علي ضرورة اعتماد تدابير وقائية خاصة بالمخاطر البيولوجية التي تؤثر علي صحة العمال [٤] . وهناك العديد من التوصيات شددت علي ضرورة الحماية ضد المخاطر البيولوجية والأمراض المعدية [٥]. ولكن يلاحظ في الوضع الراهن أن

---

(١) د. صفا عزام، الحماية الدولية للبيئة من التلوث البيولوجي مع دراسة للجهود الدولية المبذولة لمكافحة جائحة كوفيد ١٩، مرجع سابق، ص. ٣٨٣٠

(٢) راجع ستيف توليو وتوماس شمالبرغر ، معهد الأمم المتحدة لبحوث نزع السلاح، نحو الاتفاق علي مفاهيم الأمن: قاموس مصطلحات تحديد الأسلحة ونزع السلاح وبناء الثقة المرجع السابق، ص ٢١٨

(٣) راجع ستيف توليو وتوماس شمالبرغر ، معهد الأمم المتحدة لبحوث نزع السلاح، نحو الاتفاق علي مفاهيم الأمن : قاموس مصطلحات تحديد الأسلحة ونزع السلاح وبناء الثقة المرجع السابق، ص ٥١

(٤) انظر المواد ٥(أ) و ١١(و) و ١٢(ب) من الاتفاقية ١٥٥

(٥) راجع في ذلك توصية القواعد الصحية (التجارة والمكاتب لعام ١٩٤٦ رقم ١٢٠، وتوصية العاملين بالتمريض لسنة ١٩٧٧ رقم ١٥٧ ، واتفاقية السلامة والصحة في البناء لسنة ١٩٨٨ رقم ١٦٧ واتفاقية

مجموعة معايير العمل الدولية لا تتضمن أحكاما تؤكد بصورة واضحة علي حماية العمال أو بيئة العمل من المخاطر البيولوجية[١]، فكل ما تقوم به الآن هو وضع إرشادات توجيهية حول الأخطار البيولوجية[٢].

وجاء المؤتمر السادس لاستعراض اتفاقية الأسلحة البيولوجية المعقود في عام ٢٠٠٦ بالتعزيز علي تحسين وتنسيق تنفيذ الاتفاقية على الصعيد الوطني عن طريق إنشاء وحدة دعم التنفيذ لمساعدة الدول الأطراف على تنفيذ الاتفاقية، وتيسير الاتصال بالمنظمات ذات الصلة.وعلى الرغم من أن وحدة دعم التنفيذ تقدم الدعم الإداري لاتفاقية الأسلحة البيولوجية فإنها ليس لها ولاية لرصد تنفيذ الاتفاقية علي الوجه المطلوب أو التحقق من الانتهاكات[٣].

كما أكد المؤتمر الاستعراضي السابع للدول الأطراف في اتفاقية حظر استحداث وإنتاج وتكديس الأسلحة البكتريولوجية والتكسينية وتدمير الأسلحة عام ٢٠١١م، **والمؤتمر الاستعراضي الثامن عام** ٢٠١٦، "علي سبل ووسائل تعزيز التنفيذ علي المستوي الوطني بما في ذلك أعمال التشريعات الوطنية وتعزيز المؤسسات الوطنية والتنسيق فيما بينهم، وكذلك اتخاذ كافة التدابير الوطنية والإقليمية والدولية لتحسين السلامة البيولوجية والأمن البيولوجي بما في ذلك سلامة المختبرات وأمن مسببات الأمراض

السلامة والصحة في المناجم لسنة ١٩٩٥ رقم ١٧٦ واتفاقية السلامة والصحة في الزراعة لسنة ٢٠٠١ رقم ١٨٤ وتوصية السلامة والصحة في الزراعة لسنة ٢٠٠١ رقم ١٩٢ واتفاقية العمل البحري لعام ٢٠٠٦ (LC) ٢٠٠٦

(١) راجع معايير منظمة العمل الدولية وكوفيد - ١٩ مارس ٢٠٢٠، ص ١٥

(٢) تمت مراجعة توصية الوقاية من الجمرة الخبيثة لسنة ١٩١٩ رقم ٣، فيما عدا الجمرة الخبيثة التي تغطيها توصية الوقاية من الجمرة الخبيثة لسنة ١٩١٩ رقم ٣، تمت مراجعة المعيار في إطار مجموعة العمل الثلاثية بشأن آلية مراجعة المعايير واعتبر ضيق النطاق أن لناحية الحماية من الجمرة الخبيثة بصورة خاصة أو لناحية الحماية من الأخطار البيولوجية بصورة عامة وتقترح مراجعة التوصية ٣ من خلال أداة تعالج الأخطار البيولوجية.

(٣) ميليسا غيليس، نزع السلاح، دليل أساسي، المرجع السابق، ص ٤٧

والتكسينات، بالإضافة إلى توفير المساعدة والتنسيق مع المنظمات المختصة بناء على طلب أية دولة طرف في حالة زعم استخدام أسلحة بيولوجية أو تكسينية، بما في ذلك تحسين القدرات الوطنية لمراقبة الأمراض وكشفها وتشخيصها ونظم الصحة العامة [١] ، كما أكد المؤتمر علي نجاح وحدة دعم التنفيذ وقرر تجديد ولاية الوحدة مع إجراء بعض التعديلات للفترة من ٢٠١٢ حتى ٢٠١٦ وكذلك علي الدول الأطراف تقديم استمارات متعلقة بتدابير بناء الثقة التي اتفق عليها في المؤتمر الاستعراضي الثالث وتم تعديلها في المؤتمر السابع[٢].

ثانيا: التدابير الدولية لمكافحة البرمجيات الخبيثة Malware

يمكن تحديد تلك التدابير على النحو التالي:

١ـ تسليم المجرم المسئول عن البرمجيات الخبيثة Malware

يجب على الدول أن تتعاون بعضها مع البعض ومن خلال تطبيق المواثيق الدولية ذات الصلة بشأن التعاون الدولي في المسائل الجنائية وعلى وجه الخصوص في مجال تسليم المجرم المعلوماتي حيث يجب تسليم مرتكبيها وذلك وفقا لمعيار معين لتكييف الجريمة كجريمة يجوز تسليم مرتكبيها:

أ-أن يكون الدخول إلى النظام أو البيانات قد تم بدون وجه حق وبنية الإخلال بسرية البيانات أو إعاقة نظام الكمبيوتر .

ب- أن تبرم الدول فيما بينها اتفاقية تسليم مرتكبي الجرائم المعلوماتية .

ج- إذا ما رفض طلب التسليم الصادر في شأن مرتكبي إحدى الجرائم المعلوماتية بناء على جنسية الشخص المراد تسليمه نظرا لأن طرف المدعي يعتبر أنه يختص قضائيا

---

(١) نقلا عن الوثيقة الختامية للمؤتمر السابع للدول الأطراف في اتفاقية حظر استحداث وإنتاج وتكديس الأسلحة البكتريولوجية (البيولوجية) والتكسينية وتدمير تلك الأسلحة، الذي عقد في جنيف ٢٢٠٥ كانون الأول / ديسمبر ٢٠١١، BWC/CONF.VII/٧

(٢) راجع الوثيقة الختامية للمؤتمر السابع للدول الأطراف في اتفاقية حظر استحداث وإنتاج وتكديس الأسلحة البكتريولوجية (البيولوجية والتكسينية وتدمير تلك الأسلحة ، المرجع السابق ، BWC/CONF.VII /٧

بالجرمية محل الادعاء ،يقوم الطرف المدعى عليه بتقديم القضية إلى سلطاته بغرض السير في الدعوى الجنائية وعلى أن يبلغ الطرف المدعي بالنتائج المترتبة عليه

٢- تفعيل إجراءات التعاون الدولي في سبيل مكافحة البرمجيات الخبيثة Malware

وتتمثل المعونة المتبادلة في الإجراءات التالية :

أ- يجب على الدول أن تقدم لبعضها البعض المعونة المتبادلة وذلك بأكبر قدر ممكن لأغراض التحقيق والإجراءات الخاصة بالجرائم الجنائية المتعلقة بنظم وبيانات الحاسب الآلي .

ب- يجب على الدول أن تقبل وتستجيب إلى طلبات المعونة المتبادلة من خلال وسائل الاتصال السريعة كالفاكس والبريد الإلكتروني ،بالقدر الذي يوفر للطرف الطالب المستوى من الأمن والمصداقية.

ج- تخضع المعونة المتبادلة للاشتراطات المنصوص عليها في قوانين الدولة المدعية أو المنصوص عليها بموجب اتفاقيات المعونة المتبادلة .

د- في الأحوال التي يسمح فيها للطرف المدعى عليه بتعليق طلب المعونة المتبادلة على اشتراط وجود جريمة مزدوجة، يعتبر هذا الشرط محل اعتبار وبغض النظر عما إذا كانت قوانين هذه الدولة تضع الجريمة في نطاق ذي تصنيف آخر .

هـ- تحدد كل دولة سلطة مركزية تنهض بالمسئولين إرسال طلبات المعونة المتبادلة والرد عليها وتنفيذها أو نقلها للسلطات المعنية للتنفيذ.

و- تنفذ طلبات المعونة المتبادلة وفقا للإجراءات التي يحددها الطرف المدعي فيما عدا الأحوال التي لا تتصل فيها تلك الإجراءات مع أحكام القانون السائد بالدولة المعتدى عليها .

ز- يجوز للدولة المدعى عليها أن ترفض طلب المعونة إذا ما توافرت لديها القناعة بأن الالتزام بما ورد بالطلب قد يخل بسيادتها أو أمنها أو نظامها العام أو بأي من مصالحها الأساسية الأخرى.

ح- يجوز للدولة المدعى عليها تأجيل التصرف في الطلب إذا كان هذا التصرف سيخل بالتحقيقات أو إجراءات الادعاء أو الإجراءات الجنائية التي تباشر بمعرفة السلطات المعنية .

ط- يجب على الدول المدعى عليها أن تخطر الدولة المدعية بصورة فورية بنتائج تنفيذ طلب المعونة فإذا ما رفض الطلب أو تم تأجيله يجب تقديم أسباب الرفض أو التأجيل .

ى- يجوز للدولة المدعية أن تطلب من الدولة المدعى عليها أن تحتفظ بسرية الوقائع والمحتويات التي يتضمنها الطلب ،فإذا لم يكن بمقدور الدولة المدعى عليها الوفاء بمتطلبات سرية الطلب فيجب عليها إخطار الدولة المدعية بذلك وعلى الأخيرة في هذه الحالة تحديد ما إذا كان سينفذ الطلب من عدمه .

ك- يجوز في حالة الاستعجال إرسال طلبات المعونة المتبادلة مباشرة إلي السلطات القضائية بما فيها النيابة العامة لدى الدولة المدعى عليها وفي مثل الحالة يجب إرسال نسخة بالطلب نفسه إلى السلطة المركزية القائمة لدى الدولة المدعى عليها.

وترتيبا على ما سبق يمكن التأكيد أن العالم أصبح مترابطا إلكترونيا، فيجب الاهتمام على المستوى الدولي بمشكلة جرائم الكمبيوتر وخاصة في مجال التشريعات والتعاون المتبادل، ويعتقد مركز الأمم المتحدة للتطوير الاجتماعي والشؤون الإنسانية أن الوقاية من جرائم الكمبيوتر تعتمد على الأمن في إجراءات معالجة المعلومات، والبيانات الإلكترونية، وتعاون ضحايا جرائم الكمبيوتر،ومنفذي القانون،والتدريب القانوني، وتطور أخلاقيات استخدام الكمبيوتر.والأمن الدولي لأنظمة المعلومات. ففي المجال الدولي هناك حاجة للتعاون المتبادل بين الدول، والبحث الجنائي والقانوني عن بنوك المعلومات، ففي أوروبا قدمت لجنة جرائم الكمبيوتر توصيات تتعلق بجرائم الكمبيوتر تمحورت في النقاط التالية:

- المشكلات القانونية في استخدام بيانات الكمبيوتر والمعلومات المخزنة فيه في التحقيق الجنائي.
- الطبيعة العالمية لبعض جرائم الكمبيوتر.
- تحديد معايير لوسائل الأمن المعلوماتي وللوقاية من جرائم الكمبيوتر.
- مشكلة الخصوصية وخرقها في جرائم الكمبيوتر.
- موقف ضحايا جرائم الكمبيوتر.هذا وقد لخص التقرير الصادر عن اللجنة الأوروبية جرائم الكمبيوتر في التالي:

١. الاحتيال.

٢. حذف وتدمير البيانات أو المعلومات أو البرمجيات في الكمبيوتر.

٣. الدخول غير القانوني.

٤. الاعتراض غير القانوني للاتصال بين الكمبيوتر وخاصة في مجال التحويل المالي.

٥. الإنتاج غير القانوني لبيانات، أو معلومات أو برمجيات الكمبيوتر.

وقد أقر الوزراء الأوروبيون التوصيات التالية:

١. إدراك أهمية الاستجابة الدقيقة والسريعة للتحدي الجديد للجرائم المتصلة بالكمبيوتر.

٢. أن يؤخذ بالحسبان أن الجرائم المتصلة بالكمبيوتر ذات خاصية تحويلية.

٣. الوعي بالحاجة الناجمة للتناغم بين القانون والتطبيق وتحسين التعاون الدولي القانوني.

٣. أساليب الوقاية من البرمجيات الخبيثة Malware

تتعدد أساليب الوقاية من الفيروسات المعلوماتية، ومن ثم يجب تحميل برنامج مضاد للفيروسات داخل كافة الأنظمة المعرضة لخطر الإصابة بها ويمكن الأخذ بالاحتياطات التالية للحد من انتشار الفيروسات وذلك على النحو التالي : [(١)]

١) أن يتم إدخال البرامج المحملة عن طريق الإنترنت من المواقع الموثوق فيها فقط.

٢) ألا يتم استخدام أي من الأقراص المرنة داخل الكمبيوتر ما لم يجر عليه فحص دقيق للتأكد من خلوه من الفيروسات. مع وقف عمل وحدة (الماكرو) كلما أمكن ذلك.

٣) يمكن تطعيم الأقراص المرنة ضد الفيروسات التي تصيب قطاع التحميل.

٤) الإبقاء على شريط الحماية الموجود بالبرامج الجديدة المسجلة على الأقراص المرنة.

٥) يجب على مهندسي الكمبيوتر الذين ينتقلون من شبكة إلى أخرى كفالة حماية الأقراص المرنة التي يستخدمونها.

---

(١) راجع في ذلك :

Dr : Linda Volonino Cyber Jerrorism op. cit.

وعلى أية حال ، لم يعد الشخص المتعامل مع الحاسب الآلى بحاجة لبرنامج مكافحة الفيروسات؛ وذلك نظراً لأن معظم شركات إنتاج هذه البرامج، بدأت تحرص على توفير العلاج ضد أى فيروس يكون قد ضرب ضربته الضارة بالفعل، وذلك إما باستخدام برنامج لفحص محتوي رسائل البريد الإلكتروني فيمكن منع وقوع الضرر قبل حدوثه، كما يُمكن لبرنامج الحماية الذي يفحص مضمون الرسائل الإلكترونية، اعتراض أي رسائل أو ملحقاتها تعتمد على لغة برمجة مثل نصوص لغة "فيجوال بيسك" أو أية ملفات أخري ذات أوامر تنفيذية وذلك على مستوي الجهاز الرئيس (الخادم).

ومن المؤكد أن الطريقة الوحيدة للحصول على تأمين كامل ضد فيروسات البريد الإلكتروني وكافة النسخ المعدلة منه هو اعتراض وإيقاف كافة رسائل البريد الإلكتروني التي تحتوي نصوصاً خاصة بالبرمجة على مستوي الجهاز الرئيس (الخادم). وذلك بعزل هذه الرسائل وهذه هي أكثر الطرق أماناً لمنع الإصابة بهذه الفيروسات.

وختاما فإن الواقع أن المخربين على الإنترنت يختلفون من جهة الخطورة؛ فمنهم المستخدم العادي الذي يستطيع الوصول لأغراض تخريبية، ومنهم الهاوي الذي يتعلم بعض المهارات على حساب الآخرين، ومنهم المحترف الذي يقصد التخريب، ومنهم العصابات المنظمة. ولهذا فمن أنجع الوسائل أن يتم التعامل مع الأشخاص على الإنترنت بحذر شديد، وألا يتم التعامل إلا مع أشخاص أو مواقع معروفة، بحيث لا يتم تحميل ملفات إلا من المواقع الموثوقة، ويمكن الاستفادة من تقنية التوقيع الرقمي التي تعطى للمواقع عبر شركات كثيرة؛ إذ إن المواقع المعروفة لها توقيعات رقمية معترف بها. وهذه التقنية تدعمها برامج تشغيل الحاسبات المنتشرة في العالم مثل نظام التشغيل ويندوز من شركة مايكروسوفت، ولهذا يتم تحذيرك إذا كان الموقع غير معروف (ليس له توقيع رقمي معروف أو معترف به)، وأيضًا ينبغي التعامل بحذر مع رسائل البريد الإلكتروني بعدم فتح أي بريد يحوي مرفقات حتى لو كان من شخص نعرفه، إلا إذا كان المستخدم يتوقع وصول ذلك البريد، وذلك لاحتمال احتوائها على فيروسات أو ملفات تجسس.

الخاتمة

لاشك أن جريمة إرسال البرمجيات الخبيثة ، ليست حكرا على بعض الدول دون الأخرى؛ إذ إن الواقع الذى يفرضه التقدم التكنولوجى والمعلوماتي الذي أكده التطور المستمر فى وسائل معالجة ونقل المعلومات باعتبارها باتت المحدد الاستراتيجي للبناء الثقافي والإنجاز الاقتصادي، يؤكد أن هذه الجريمة الجديدة، آخذة فى الانتشار فى ربوع الأرض، فليس غريبا أن نجد مجرمي البرمجيات الخبيثة فى العالم العربى، كما أن الدول الأوربية والولايات المتحدة الأمريكية ظلت لفترة طويلة – وما زالت- مرتعا خصبا للإجرام الإلكتروني بل إن هذه الدول بما حققته من تقدم علمي وتكنولوجي كانت أحد الأسباب الرئيسة لانتشار الجريمة الإلكترونية فى ربوع العالم.

وأمام هذا الانتشار الكبير لهذا النوع من الجرائم اتجهت الدول إلى تضمين أنظمتها القانونية قوانين لمكافحة جريمة نشر الفيروسات الخبيثة من أجل إنزال حكم القانون على المجرم المعلوماتي أينما وجد وتوقيع العقاب عليه. فضلا عن اتجاه الكثير من الدول إلى تفعيل مبدأ التعاون الدولي فى مجال مكافحة الجريمة الإلكترونية.

ومما هو جدير بالذكر أن جرائم البرمجيات الخبيثة ، هى ظاهرة إجرامية جديدة ومستجدة تقرع في جنباتها أجراس الخطر لتنبه مجتمعات العصر الراهن لحجم المخاطر وهول الخسائر الناجمة عن جريمة الحاسب الآلي التي تستهدف الاعتداء على المعطيات بدلالتها التقنية الواسعة، فجريمة الحاسب الآلي جريمة تقنية تنشأ في الخفاء، يقترفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية، توجه للنيل من الحق في المعلومات، وتطال اعتداءاتها معطيات الحاسب المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات.

هذه المعطيات هي موضوع هذه الجريمة وما تستهدفه اعتداءات الجناة، وهذا وحده – عبر دلالته العامة – يظهر مدى خطورة الجرائم الإلكترونية، فهي تطال الحق في

المعلومات، وتمس الحياة الخاصة للأفراد، وتهدد الأمن القومي والسيادة الوطنية، وتشيع فقدان الثقة بالتقنية وتهدد إبداع العقل البشري، لذا فإن إدراك ماهية الجرائم الإلكترونية ، منوط بتحليل وجهة نظر الدارسين لتعريفها والاصطلاحات الدالة عليها واختيار أكثرها اتفاقًا مع الطبيعة الموضوعية لهذه الجرائم، واستظهار موضوعها وخصائصها ومخاطرها وحجم الخسائر الناجمة عنها وسمات مرتكبيها ودوافعهم.

نتائج الدراسة

٤. تعتبر جريمة إعاقة الوصول إلى الخدمات الإلكترونية من الجنح التي تتمثل بتعطيل الوصول أو إعاقة الوصول إلى الخدمات الإلكترونية أو الأجهزة أو البرامج أو المعلومات الإلكترونية على اختلاف أنواعها.

٥. إن محل الحماية في جريمة الاعتداء على البرامج الإلكترونية هو الأجهزة الإلكترونية والشبكة الإلكترونية والبرامج الملحقة بها، بالإضافة إلى البيانات والمعلومات الإلكترونية المخزنة، وأيضا الخدمات التي تقدمها، وهنا حاول المشرع الفلسطيني توفير هذه الحماية انطلاقاً من حق المستخدم في الوصول إلى الجهاز الالكتروني الخاص به، وأن تعطيل أو إعاقة الوصول للأجهزة الإلكترونية والشبكة الإلكترونية والبرامج الملحقة يشكل اعتداء على هذا الحق.

٦. هناك العديد من البرمجيات الخبيثة Malware التي تستهدف تعطيل الأجهزة الإلكترونية أو الحواسيب، وجميع أشكالها وأنواعها تقع بها الجريمة.

٧. جرائم الاعتداء على البرامج الإلكترونية لا تقوم إلا عمدية، وهو ما أشار إليه المشرع الفلسطيني، حيث تقوم على القصدين العام والخاص، حيث يتمثل القصد العام في توجه نية وإرادة المستخدم لإنتاج مثل تلك الفيروسات وإدخالها عبر الشبكة الإلكترونية، أو أي وسيلة إلكترونية أخرى، مع علمه بضررها، أما القصد الخاص فيتمثل في هذه الجريمة بنية الفاعل أن تؤدي هذه البرمجيات إلى إيقاف أو إتلاف البرامج الإلكترونية أو حذفها أو التعديل عليها.

٨. حاول المشرع توفير هذه الحماية للبرامج الإلكترونية انطلاقًا من حق المستخدم في الوصول إلى الجهاز الإلكتروني الخاص أو الخدمات الإلكترونية، وأن تعطيل أو إعاقة الوصول للأجهزة الإلكترونية والشبكة الإلكترونية والبرامج الملحقة يشكل اعتداء على هذا الحق.

٩. إن محل جرائم الاعتداء على المعلومات هو نظام المعلوماتية بمكوناته غير المادية، أما مكوناته المادية فالاعتداء عليها مجرم بنصوص التجريم التقليدية. كما أن غياب نصوص

دولية موحدة تواجه جرائم العالم الافتراضي، وغياب نصوص دولية موحدة تكفل الحماية الجنائية على شبكة الإنترنت.

١٠. إن فكرة تطويع النصوص التقليدية وتعديلها بما يتلاءم وطبيعة البيئة المعلوماتية لا يحقق الحماية الكافية لأمن المعلومات للطبيعة المتطورة لهذه الجرائم ومن ثم يصبح البحث عن سبيل آخر أمرا لا مفر منه.

١١. إن من أهم الدواعي هو تدخل المشرع لإصدار نصوص تحظر الاعتداء على نظم المعلوماتية في التشريع المصري القائمة على الإحاطة بكافة أشكال الاعتداءات التي تقع على مكوناتها غير المادية، خاصة مع العجز الذي كان يشوب التشريع في مواجهتها للجرائم التي كانت ستترتب عليها آثار خطيرة، نتيجة ارتكاب أفعال غير مشروعة ويفلت أصحابها من العقاب بسبب عدم وجود نصوص تجرمها ، وحسنا فعل المشرع المصري عندما أقر مشروع القانون الأخير لمكافحة هذه الجرائم.

١٢. هناك بعض من العوائق التي تعيق مكافحة الاعتداءات الواقعة على أمن المعلومات في إطار البيئة الإليكترونية بعضها تشريعي وبعضها إجرائي هذه التعقيدات ناتجة عن طبيعة هذه الجريمة سواء من ناحية تطورها التقني ،أم من ناحية طبيعتها العابرة للحدود والآثار الخطيرة الناجمة عنها التي قد تصيب العديد من البلدان في آن واحد.

توصيات الدراسة

١. حماية البرامج من البرمجيات الخبيثة Malware لدى المستخدمين من خلال رفع مستويات الأمان في الحواسيب على اختلاف أنواعها، وتتمثل بتجنب زيارة المواقع الإلكترونية غير الآمنة، والتأكد من تحديثات برامج مضاد الفيروسات وأنظمة التشغيل والتأكد من تشغيل الجدران النارية، وعدم فتح بريد إليكتروني أو مرفق من أشخاص غير معروفين، تفعيل أنظمة كشف التسلل IDS وأنظمة الحماية من التسلل IPS وذلك على مستوى الشبكات، وتفعيل تطبيقات مانع الإعلانات التجارية.

٢. ضرورة المراجعة الدورية للتشريعات الجزائية القائمة وإزالة أي غموض أو ثغرات من الممكن أن يستغلها الجناة للإفلات من العقاب.

٣. تعزيز التعاون الدولي في مكافحة الجرائم المعلوماتية ، بهدف التقريب بين القوانين الوطنية الجزائية ، وجمع الأدلة وتسليم المجرمين ، وتبادل الخبرات والمعلومات المتعلقة بهذا الأمر.

٤. إنشاء وحدات خاصة يناط بها مهمة التحري والتعمق في البيئة الإليكترونية سواء على المستوى الوطني أو الدولي على أن يتم بالتوازي الاهتمام بتدريب وإعداد الكوادر الشرطية المؤهلة للتعامل مع جرائم الاعتداء على المعلومات ذات الطبيعة التقنية المعقدة ، وتعزيز قدراتهم على التحقيق فيها وتأمين الأدلة التقنية. تمكين القضاة وأعضاء النيابة وإعدادهم لملاحقة ومقاضاة مرتكبي جرائم تقنية المعلومات والاستفادة من الأدلة التقنية من خلال التدريب والتخطيط.

٥. تدريس الجرائم التقنية وكل ما يخصها واعتبارها مادة أساسية في المعاهد الأمنية ومؤسسات إعداد القضاة ومناهج الدراسة الخاصة بالقانون الجنائي لتخريج كوادر قادرة على التعامل مع مثل هذه الاعتداءات والجرائم.

٦. يجب أن تتضمن مقومات واستراتيجيات مواجهة جرائم الاعتداء على المعلومات ومحاربتها بجانب القوانين الجنائية الموضوعية قوانين إجرائية تتماشى وطبيعة البيئة الرقمية ، وبخاصة مسألة استخلاص الدليل الرقمي بدون المساس بحقوق الإنسان

وحرياته الأساسية وتعريضها للخطر ولذلك قيل بأن من يتقن وضع قانون عقوبات ثم يترك قانون الإجراءات الجنائية بدون إتقان كمن يبني قصرا في الهواء.

٧. ضرورة الاتفاق من خلال تعزيز التعاون الدولي بالاتفاقيات الثنائية والمتعددة لمواجهة هذه الظاهرة الإجرامية ذات الطبيعة العابرة للحدود على حل جميع العقبات التي تحول دون ملاحقة مرتكبي هذه الجرائم ، وبخاصة مشاكل تنازع الاختصاص وتسليم المجرمين، والنص في القانون المصري الجديد على تقادم العقوبة في هذه النوعية من الجرائم واعتبارها من الجرائم المستمرة في سريان مدة التقادم للتقليل من الإفلات من العقاب، واستحداث نص خاص بالتزوير المعلوماتي ، وتوسيع مفهوم المحرر ليشمل أية دعامة أخرى.

قائمة المراجع

المراجع العربية

الكتب القانونية:

١. باسل مصطفى الخطيب وآخرون. (٢٠١٦)، الحاسوب والبرمجيات الجاهزة، الطبعة الأولى، دار الاعصار العلمي، الأردن.

٢. توفيق نظام المجالي. (٢٠١٢) ، شرح قانون العقوبات القسم العام، الطبعة الثالثة، دار الثقافة للنشر والتوزيع، الأردن.

٣. جبريل بن حسن العريشي، سلمى بنت عبد الرحمن محمد الدوسري (٢٠١٨)، الشبكات الاجتماعية والقيم، الطبعة الأولى الدار المنهجية للنشر، الأردن.

٤. جبريل بن حسن العريشي، محمد حسن الشلهوب (٢٠١٦) ، أمن المعلومات، الطبعة الأولى، دار المنهجية للنشر والتوزيع، الأردن.

٥. زياد القاضي. (٢٠٠٧)، انظمة التشغيل، الطبعة الخامسة، دار المسيره، الأردن.

٦. عبد الله ذيب محمود، وأسامة اسماعيل دراج (٢٠٢٢) الوجيز في الجرائم الإلكترونية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن.

٧. علاء حسين الحمامي، سعد عبد العزيز العاني. (٢٠٠٧) ، تكنولوجيا امنية المعلومات وانظمة الحماية، الطبعة الأولى، دار وائل للنشر، الأردن.

٨. علاء حسين الحمامي مازن سمير الحكيم (٢٠١٧) ، كل شيء عن إنترنت الاشياء وتطبيقات المدن الذكية دار الراية للنشر والتوزيع، الطبعة الأولى، الأردن.

٩. علي جبار الحسيناوي. (٢٠٠٩)، جرائم الحاسوب والإنترنت، الطبعة الأولى، دار اليازوري العلمية، الأردن.

١٠. عيدي سليمة. (٢٠١٧) ، أمن المعلومات وأنظمتها في العصر الرقمي، الطبعة الأولى، دار الفكر الجامعي، مصر.

١١. غنية باطلي. (٢٠١٥)، الجريمة الإلكترونية، الطبعة الأولى منشورات الدار الجزائرية، الجزائر.

١٢. فايز مصطفى الحمودي، عدنان هادي الهلالي (٢٠٠٩)، نظم التشغيل، الطبعة الأولى، دار صفاء، الأردن.

١٣. فخري الحديثي، وخالد الزعبي. (٢٠١٠)، شرح قانون العقوبات (القسم العام)، الطبعة الثانية، دار الثقافة، الأردن.

١٤. مجدي أبو العطا. (٢٠١٦)، أمن المعلومات والإنترنت، الطبعة الأولى، شركة علوم الحاسبة (كمبيوسانيس)، مصر.

١٥. محمد بلال الزعبي، أحمد الشرايعة سهير عبد الله خالد محمد الزعبي (٢٠٠٩)، الحاسوب والبرمجيات الجاهزة: مهارات الحاسوب الطبعة التاسعة، دار وائل، الأردن.

١٦. محمد صبحي نجم. (٢٠١٠)، قانون العقوبات القسم العام، الطبعة الثالثة، دار الثقافة للنشر والتوزيع، الأردن.

١٧. منال البلقاسي . (٢٠١٩)، مفاهيم مستحدثة في نظام التشغيل، الطبعة الأولى، دار القلم الجامعي، مصر.

١٨. يوسف المصري. (٢٠١١) ، الجرائم المعلوماتية والرقمية للحاسوب والإنترنت، الطبعة الأولى، دار العدالة، مصر.

ثانيا: الكتب العامة

١) أحمد فتحي سرور : الحق في الحياة الخاصة ، مجلة القانون والاقتصاد للبحوث القانونية والاقتصادية ، مطبعة جامعة القاهرة ، العدد ٥٤، ١٩٨٦م.

٢) آدم عبد البديع آدم حسين : الحق في حرمة الحياة الخاصة ومدى الحماية التي يكفلها له القانون الجنائي ، رسالة دكتوراه ، كلية الحقوق ، جامعة القاهرة ، ٢٠٠٠م .

٣) أسامة عبد الله قايد :- الحماية الجنائية للحياة الخاصة وبنوك المعلومات ، بدون دار نشر ورقم طبعة ، ١٩٨٠م.

٤) أشرف شمس الدين ، الحماية الجنائية للمستند الإليكتروني ، ط ا ، دار النهضة العربية، القاهرة،٢٠٠٦م.

٥) أشرف صلاح الدين ، طرق الحماية التكنولوجية بأنواعها وأشكالها المختلفة ، ورشة عمل بعنوان أمن وحماية نظم المعلومات في المؤسسات العربية ، القاهرة ، ٢٠٠٧.

٦) إيهاب ماهر السمباطي : - الجرائم الإليكترونية والجرائم السيبرية وظيفة جديدة ، فئة مختلفة ، التناغم القانوني هو السبيل الوحيد ، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر ، المغرب ١٩-٢٠ يونيه ،٢٠٠٧م.

٧) جلاد سليم: الحق في الخصوصية بين الضمانات والضوابط في التشريع الجزائري والفقه الإسلامي، رسالة ماجستير ، كلية العلوم الإنسانية والحضارة الإسلامية ، جامعة وهران ، الجزائر ٢٠١٣-٢٠١٤م.

٨) جميل زكريا محمود ، الفيروسات وطرق الوقاية منها كوسيلة لأمن البيانات ، المؤتمر الدولي الأول حول أمن المعلومات ، نحو تكامل رقمي آمن ،١٨ - ٢٠ ديسمبر ٢٠٠٥م ، مسقط عمان .

٩) حسن طاهر داوود ، الحاسب وأمن المعلومات ، مركز الدراسات والبحوث ، المملكة العربية السعودية ، ٢٠٠٠م.

١٠) خالد ممدوح إبراهيم، الجرائم المعلوماتية ، دار الفكر الجامعي ، الإسكندرية ، ط١ ، ٢٠٠٩م. أمن المعلومات الالكترونية ، الدار الجامعية ، القاهرة ،٢٠٠٨م.

١١) ذيب بن عايض القحطاني ، أمن المعلومات ، مدينة الملك عبد العزيز للعلوم التقنية ، الرياض ١٤٣٦هـ- ٢٠١٥م.

١٢) سعد غالب ياسين ، نظم المعلومات الإدارية الطبعة العربية دار اليازوري العلمية للنشر والتوزيع، عمان الأردن ،٢٠٠٩م.

١٣) عائشة بن قارة مصطفي :- حجية الدليل الإليكتروني في مجال الإثبات الجنائي ، دار الجامعة الجديدة الإسكندرية ،٢٠٠٩م.

١٤) عبد الجبار الحنيص:- الاستخدام غير المشروع لنظام الحاسوب من وجهة نظر القانون الجزائي " دراسة مقارنة" ، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية ، المجلد ٢٧ ، العدد الأول ، ٢٠١١م.

١٥) عبد العظيم مرسي وزير شرح قانون العقوبات ، دار النهضة العربية.

١٦) عبد الفتاح بيومي حجازي التجارة الإليكترونية وحمايتها القانونية ، دار الفكر الجامعي ، الإسكندرية ، ٢٠٠٤م.

١٧) عبد المحسن بدوي محمد أحمد: استراتيجيات ونظريات معالجة قضايا الجريمة والانحراف في وسائل الإعلام الجماهيرية ، الندوة العلمية حول الإعلام والأمن ، مركز الدراسات والبحوث ، قسم الندوات واللقاءات العلمية ، أكاديمية نايف العربية للعلوم الأمنية ،١١-١٣ / ٥ / ٢٠٠٥م.

١٨) عفيفي كامل عفيفي ، جرائم الكمبيوتر ودور الشرطة والقضاء ، رسالة دكتوراه ، كلية الحقوق ، جامعة الإسكندرية ، ١٩٩٩م.

١٩) علي محمود علي حمودة :- الأدلة المتحصلة من الوسائل الإليكترونية في إطار نظرية الإثبات الجنائي، مقدم للمؤتمر العلمي الأول حول الجوانب القانونية الأمنية للعمليات الإليكترونية، أكاديمية شرطة دبي ٢٨-٢٠٠٣/ ٤/ ٢٩م.

٢٠) عوض الحاج على أحمد ، عبد الأمير خلف حسين ، أمنية المعلومات وتقنيات التشفير، دار الحامد للنشر والتوزيع ، الأردن ، ٢٠٠٠م.

٢١) غنام محمد غنام ، عدم ملاءمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر مقدم لمؤتمر القانون والكمبيوتر والإنترنت ، الإمارات العربية المتحدة ، كلية الشريعة والقانون ، ١-٣مايو، ٢٠٠٣م ، المجلد الثاني.

٢٢) فاطمة مرينز : الاعتداء على الحق في الحياة الخاصة عبر شبكة الإنترنت ، رسالة دكتوراه ، جامعة أبو بكر بلقان ، تلمسان ، الجزائر ،٢٠١٢ - ٢٠١٣م .

٢٣) قانون الأونيسترال النموذجي للتوثيق التجاري الدولي مع دليل الاشتراع استعماله ، منشورات الأمم المتحدة .A05.V4. Y..E

٢٤) القانون رقم ١٧٥ لسنة ٢٠١٨م في شأن مكافحة جرائم تقنية المعلومات المنشور بالجريدة الرسمية العدد ٣٢ مكرر في١٥ أغسطس ٢٠١٨.

٢٥) قرار مجلس وزراء العدل العرب الدورة التاسعة القرار رقم ٤٩٥ - ١٩ - ٢٠٠٣/ ١٠/ ٨م.

٢٦) محمد أبوبكر يونس ، الجرائم الناشئة عن استخدام الإنترنت (الأحكام الموضوعية والجوانب الإجرائية ، دار الثقافة العربية للنشر ، ٢٠٠٤م.

٢٧) محمد بن عبد الله القحطاني ، أمن المعلومات ، جامعة الملك عبد العزيز للعلوم والتقنية، الرياض، ٢٠٠٩م.

٢٨) محمد حماد مرهج الهيتي، "جرائم الحاسوب ، ط ، إدارة المناهج للنشر والتوزيع، عمان، ٢٠٠٦م

٢٩) محمد شوابكة ، جرائم الحاسوب والإنترنت ، دار الثقافة عمان ، ط ١، ٢٠٠٤ . ص ١٣ .، وقد تلافي المشرع المصري في القانون رقم ١٧٥ لسنة ٢٠١٨م.

٣٠) محمد فهمي طلبة ، فيروسات الحاسب وأمن البيانات ، مجموعة النيل العربية للطباعة والنشر، ١٩٩١م.

٣١) محمد محمد الألفي ، ورقة عمل مقدمة في ندوة حماية نظم المعلومات في المؤسسات العربية ، القاهرة ،٢٠٠٧م.

٣٢) مدحت رمضان : - جرائم الاعتداء على الأشخاص والإنترنت ، دار النهضة العربية ن القاهرة ،٢٠٠٧م.

٣٣) مفتاح بو بكر المطردي ، الجريمة الإليكترونية ، ورقة عمل مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية ، السودان ٢٣-٢٥ أيلول ٢٠٠١م.

٣٤) ممدوح خليل بحر :- نطاق حماية الحياة الخاصة في القانون الجنائي ، دار الثقافة للنشر والتوزيع ، الأردن ، ٢٠٠٦م.

٣٥) ممدوح عبد الحميد عبد المطلب، زبيدة محمد قاسم، عبد الله عبد العزيز، أنموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في جرائم الكمبيوتر، مؤتمر الأعمال المصرفية الإليكترونية، كلية الشريعة والقانون، الإمارات، غرفة تجارة وصناعة ، دبي، ٥- ١٠/ ١٢/ ٢٠٠٣م.

٣٦) نادية أمين محمد علي ، الفيروسات وطرق الوقاية منها كوسيلة لأمن البيانات ، المؤتمر الدولي الأول حول أمن المعلومات ، نحو تكامل رقمي آمن ديسمبر ٢٠٠٥ ، مسقط عمان.

٣٧) نائل عبد الرحمان صالح، واقع، جرائم الحاسب في التشريع الأردني ، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت الذي نظمته كلية الشريعة والقانون – جامعة الإمارات العربية المتحدة (٢٠٠٠) بحوث مؤتمر القانون والكمبيوتر والإنترنت ، المجلد الأول ، الطبعة الثالثة ، كلية الشريعة والقانون جامعة الإمارات العربية المتحدة ، ٢٠٠٤م.

٣٨) نائلة عادل محمد فريد قورة، جرائم الحاسب الاقتصادية رسالة دكتوراه جامعة القاهرة، كلية الحقوق، طبعة ٢٠٠٣م.

٣٩) نجم عبد الله الحميدي ، نظم المعلومات الإدارية مدخل معاصر ، الطبعة الثانية ، دار اليازوري للنشر والتوزيع، عمان ، الأردن ، ٢٠٠٩م.

٤٠) نظام مكافحة جرائم المعلوماتية ، هيئة الاتصالات وتقنية المعلومات، المملكة العربية السعودية.

٤١) هدى حامد قشقوش : حماية الحاسب الإليكتروني ، في التشريع المقارن، دار النهضة العربية، القاهرة ١٩٩٢م.

٤٢) هشام فريد رستم ، قانون العقوبات و مخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، ١٩٩٢ .

٤٣) الحماية الجنائية للإنسان في صورته ، مكتبة الآلات الحديثة ، أسيوط.

٤٤) هيثم حمود الشبلي ، إدارة مخاطر الاحتيال في قطاع الاتصالات ، دار صفاء للنشر والتوزيع ، ط ١ ، عمان ، الأردن ٢٠٠٩م.

٤٥) هيثم محمد الزعبي ، إيمان فاضل السامرائي ، نظم المعلومات الإدارية، الطبعة الأولى، دار صفاء للنشر والتوزيع ، عمان ، ٢٠٠٤م .

٤٦) وائل بندق ، موسوعة القانون الإليكتروني وتكنولوجيا الاتصال والمعلومات ، دار المطبوعات الجامعية ، الإسكندرية ، ط١ ، ٢٠٠٧م. يوسف خليل يوسف عبد الجابر ،

مدى فاعلية إجراءات الرقابة الداخلية في توفير أمن المعلومات الإليكترونية في الشركات الصناعية الأردنية ، رسالة ماجستير ، جامعة الشرق الأوسط ،٢٠١٣م.

٤٧) يونس عرب: قراءة في الاتجاهات التشريعية للجرائم الإليكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان ، ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الإليكترونية ، مسقط ، ٢-٤ أبريل ٢٠٠١م.

٤٨) يونس عرب ، جرائم الكومبيوتر والانترنت ، إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات، ورقة عمل مقدمة إلى مؤتمر الأمن العربي ٢٠٠٢م تنظيم المركز العربي للدراسات والبحوث الجنائية ، أبو ظبي ، ص ١١ ، ١٠ – ١٢/ ٢ ٢٠٠م.

المراجع الاجنبية

1) Basil Mustafa Al-Khatib et al. (2016), Computer and ready-made software, first edition, Dar Al-Assar Alami, Jordan.

2) Tawfiq Al-Majali System. (2012), Explanation of the Penal Code, General Section, third edi- tion, House of Culture for Publishing and Distribution, Jordan.

3) Jibril bin Hassan Al-Areshi, Salma bint Abdul Rahman Muhammad Al-Dosari. (2018), So- cial Networks and Values, First Edition, Methodology House for Publishing, Jordan.

4) Jibril bin Hassan Al-Areshi, Mohammed Hassan Al-Shalhoub. (2016), Information Security, First Edition, House of Methodology for Publishing and Distribution, Jordan.

5) Ziad Al-Qadi. (2007), Operating Systems, Fifth Edition, Dar Al Masirah, Jordan .5

6) Abdallah (Theeb Mahmoud, and Osama Ismail Darrag. (2022) Al-Wajeez in Electronic .6 .Crimes, first edition, House of Culture for Publishing and Distribution, Jordan

7) Alaa Hussein Al-Hamami, Saad Abdul Aziz Al-Ani. (2007), Information Security Technolo- .7 .gy and Protection Systems, First Edition, Wael Publishing House, Jordan

8) Alaa Hussein Al-Hamami, Mazen Samir Al-Hakim. (2017), All about the Internet of Things .8 .and smart city applications: Dar Al-Raya for Publishing and Distribution, first edition, Jordan

9) Ali Jabbar Al-Husseinawi. (2009), Computer and Internet Crimes, first edition, Al-Yazuri .9 .Scientific House, Jordan

10) Idi sound. (2017), Information security and systems in the digital age, first edition, Dar Al- .10 Fikr Al-Jamii, Egypt

11) Rich my void. (2015), Cybercrime, first edition, Algerian House Publications, Algeria .11

12) Fayez Mustafa Al-Hamoudi, Adnan Hadi Al-Hilali. (2009), Operating Systems, First Edi- .12 .tion, Dar Safaa, Jordan

13) Fakhri Al-Hadithi, and Khaled Al-Zoubi. (2010), Explanation of the Penal Code (General .13 .Section), second edition, House of Culture, Jordan

14) Magdy Abu Al-Atta. (2016), Information and Internet Security, first edition, Computer Sci- .14 .ence Company (CompuSanis), Egypt

15) Muhammad Bilal Al-Zoubi, Ahmed Al-Sharia, Suhair Abdullah, Khaled Muhammad .15 Al-Zoubi. (2009), Computer

and Ready-made Software: Computer Skills, Ninth Edition, Dar Wael, Jordan

16) Mohamed Sobhi Negm. (2010), Penal Code, General Section, third edition, House of Cul- .16 .ture for Publishing and Distribution, Jordan

17) Manal Belkassi. (2019), New concepts in the operating system, first edition, Dar Al-Qalam .17 .University, Egypt

18) Youssef Al-Masry. (2011), Computer and Internet Information and Digital Crimes, First .18 .Edition, House of Justice, Egypt

19) Charles P. Pfleeger, (2015)Shari Lawrence Pfleeger, Jonathan Margulies, Securityin Com- .19 .puting5th ed, Pearson Education, Inc

20) Kim, D., & Solomon, M. G. (2018). Fundamentals of information systems security. Jones .20 .& Bartlett Publishers

21) Thakur, K., & Pathan, A. S. K. (2020). Cybersecurity Fundamentals: A Real-World Perspec- .21 .tive. CRC Press

22) Manish Gupta and Raj Sharman, Social and Organizational Liabilities in Information Security, publishing Information Science Reference, Hershey, New York, 2009 .P.296

23) Micki Krause; Harold F. Tipton, Information Security Management Hand book, Sixth Edition, Auerbach Publication, New York, 2008.

24) Romney, M& Steinbart ,P., Accounting information's system ,12ed., ENGLAND. Pearson education,2012.

25) Samuel D. Warren &Louis D. Brandeis, The right of piracy , Harvard law review, Vol. IV., Dec. 15, 183-220

26) Todd G. Shipley, Henory R. Reeve, Collecting evidence from a running computer, The national consortium for justice information and statistic,2006

References:

alkutub alqanunia:

• basil mustafaa alkhatib wakhrun. (2016), alhasub walbarmajiaat aljahizatu, altabeat al'uwlaa, dar aliaesar alealami, al'urdunn.

• tufiq nizam almajali. (2012) , sharh qanun aleuqubat alqism aleama, altabeat althaalithata, dar althaqafat lilnashr waltawziei, al'urduni.

• jbril bin hasan alearishi, salmaa bint eabd alrahman muhamad alduwsarii (2018), alshabakat aliajtimaeiat walqiimu, altabeat al'uwlaa aldaar almanhajiat lilnashri, al'urduni.

• jbril bin hasan alearishi, muhamad hasan alshalhub (2016) , 'amn almaelumati, altabeat al'uwlaa, dar almanhajiat lilnashr waltawziei, al'urdun.

• zyad alqadi. (2007), anzimat altashghili, altabeat alkhamisatu, dar almasirihi, al'urdun.

• eabd allah dhib mahmud, wa'usamat asmaeil daraaj (2022) alwajiz fi aljarayim al'iiliktruniati, altabeat al'uwlaa, dar althaqafat lilnashr waltawziei, al'urduni.

• eala' husayn alhamaami, saed eabd aleaziz aleani. (2007) , tiknulujia aminiat almaelumat wanzimat alhimayati, altabeat al'uwlaa, dar wayil lilnashri, al'urduni.

• eala' husayn alhamaami mazin samir alhakim (2017) , kulu shay' ean 'iintirnit alashia' watatbiqat almudun aldhakiat dar alraayat lilnashr waltawziei, altabeat al'uwlaa, al'urdunn.

• eali jabaar alhusaynawi. (2009), jarayim alhasub wal'iintirnti, altabeat al'uwlaa, dar alyazuri aleilmiati, al'urdun.

• eidi salimat. (2017) , 'amn almaelumat wa'anzimatiha fi aleasr alraqmii, altabeat al'uwlaa, dar alfikr aljamieii, masru.

• ghaniat batili. (2015), aljarimat al'iiliktiruniatu, altabeat al'uwlaa manshurat aldaar aljazayiriati, aljazayir.

• fayiz mustafaa alhamuwdi, eadnan hadi alhalali (2009), nazam altashghili, altabeat al'uwlaa, dar safa', al'urdun.

• fakhiri alhadithi, wakhalid alzuebi. (2010), sharh qanun aleuqubat (alqism aleama), altabeat althaaniatu, dar althaqafati, al'urdun.

• majdi 'abu aleataa. (2016), 'amn almaelumat wal'iintirnti, altabeat al'uwlaa, sharikat eulum alhasiba (kumbiusanis), musr.

• muhamad bilal alzuebi, 'ahmad alsharayieat suhayr eabd allh khalid muhamad alzuebi (2009), alhasub walbarmajiaat aljahizatu: maharat alhasub altabeat altaasieata, dar wayil, al'urdun.
• muhamad subhi najma. (2010), qanun aleuqubat alqism aleama, altabeat althaalithata, dar althaqafat lilnashr waltawziei, al'urdun.
• manal albalqasi . (2019), mafahim mustahdithat fi nizam altashghili, altabeat al'uwlaa, dar alqalam aljamieii, masr.
• yusuf almisri. (2011) , aljarayim almaelumatiat walraqmiat lilhasub wal'iintirnti, altabeat al'uwlaa, dar aleadalati, masr.

alkutub alama

• 'ahmad fathi surur : alhaqu fi alhayat alkhasat , majalat alqanun waliaqtisad lilbuhuth alqanuniat waliaqtisadiat , matbaeat jamieat alqahirat , aleadad 54, 1986m.
• adim eabd albadie adam husayn : alhaqu fi hurmat alhayaat alkhasat wamadaa alhimayat alati yakfiluha lah alqanun aljinayiyu , risalat dukturah , kuliyat alhuquq , jamieat alqahirat ,2000m .
• 'usamat eabd allah qayid :- alhimayat aljinayiyat lilhayat alkhasat wabanuk almaelumat , bidun dar nashr waraqm tabeat , 1980m.
• 'ashraf shams aldiyn , alhimayat aljinayiyat lilmustanad al'iilikturuni , t a , dar alnahdat alearabiati, alqahirati,2006m.
• 'ashraf salah aldiyn , taruq alhimayat altiknulujiat bi'anwaeiha wa'ashkaliha almukhtalifat , warshat eamal bieunwan 'amn wahimayat nazum almaelumat fi almuasasat alearabiat , alqahirat , 2007.
• 'iihab mahir alsambatii : - aljarayim al'iilikturuniat waljarayim alsaybariat wazifat jadidat , fiat mukhtalifat , altanaghum alqanuniu hu alsabil alwahid , alnadwat al'iiqlimiat hawl aljarayim almutasilat bialkumbiutar , almaghrib 19-20 yunih ,2007m.
• jalad salim: alhaqu fi alkhususiat bayn aldamanat waldawabit fi altashrie aljazayirii walfiqh al'iislamii, risalat majistir , kuliyat aleulum al'iinsaniat walhadarat al'iislamiat , jamieat wahran , aljazayir 2013-2014m.
• jamil zakariaa mahmud , alfayrusat waturuq alwiqayat minha kawasilat li'amn albayanat , almutamar alduwaliu al'awal hawl 'amn almaelumat , nahw takamul raqamay aman ,18 - 20 disambir 2005m , masqat eamaan .

• hasan tahir dawwud , alhasib wa'amn almaelumat , markaz aldirasat walbuhuth , almamlakat alearabiat alsueudiat , 2000m.
• khalid mamduh 'iibrahim, aljarayim almaelumatiat , dar alfikr aljamieii , al'iiskandariat , ta1 , 2009ma. 'amn almaelumat alalkitruniat , aldaar aljamieiat , alqahirat ,2008m.
• dhib bin eayid alqahtanii , 'amn almaelumat , madinat almalik eabd aleaziz lileulum altaqniat , alriyad 1436hi- 2015m.
• saed ghalib yasin , nazam almaelumat al'iidariat altabeat alearabiat dar alyazurii aleilmiat lilnashr waltawziei, eamaan al'urduni ,2009m.
• eayishat bin qarat mustafi :- hajiat aldalil al'iilikturuni fi majal al'iithbat aljinayiyi , dar aljamieat aljadidat al'iiskandariat ,2009m.
• eabd aljabaar alhunisi:- alaistikhdam ghayr almashrue linizam alhasub min wijhat nazar alqanun aljazayiyi " dirasat muqaranati" , majalat jamieat dimashq lileulum alaiqtisadiat walqanuniat , almujalad 27 , aleadad al'awal , 2011m.
• eabd aleazim mursi wazir sharh qanun aleuqubat , dar alnahdat alearabiati.
• eabd alfataah biumi hijazii altijarat al'iilikturuniat wahimayatiha alqanuniat , dar alfikr aljamieii , al'iiskandariat , 2004m.
• eabd almuhsin badawi muhamad 'ahmad: astiratijiaat wanazariaat muealajat qadaya aljarimat walainhiraf fi wasayil al'iielam aljamahiriat , alnadwat aleilmiat hawl al'iielam wal'amn , markaz aldirasat walbuhuth , qism alnadawat walliqa'at aleilmiat , 'akadimiat nayif alearabiat lileulum al'amniat ,11-13 / 5 / 2005m.
• efifi kamil eafifi , jarayim alkumbuyutar wadawr alshurtat walqada' , risalat dukturah , kuliyat alhuquq , jamieat al'iiskandariat , 1999m.
• eali mahmud eali hamuwdat :- al'adilat almutahasilat min alwasayil al'iilikturuniat fi 'iitar nazariat al'iithbat aljinayiy, muqadim lilmutamar aleilmii al'awal hawl aljawanib alqanuniat al'amniat lileamaliaat al'iilikturuniati, 'akadimiat shurtat dubay 28-2003/4/29m.
• eawad alhaji ealaa 'ahmad , eabd al'amir khalaf husayn , 'amniat almaelumat watiqniaat altashfiri, dar alhamid lilnashr waltawzie , al'urdunu ,2000m.

• ghnam muhamad ghanaam , eadam mula'amat alqawaeid altaqlidiat fi qanun aleuqubat limukafahat jarayim alkumbuyutir muqadam limutamar alqanun walkumbuyutir wal'iintirnit , al'iimarat alearabiat almutahidat , kuliyat alsharieat walqanun , 1-3mayu, 2003m , almujalad althaani.
• fatimat mrinz : aliaietida' ealaa alhaqi fi alhayaat alkhasat eabr shabakat al'iintirnit , risalat dukturah , jamieat 'abu bakr balqan , talmisan , aljazayir ,2012 - 2013m .
• qanun al'uwnistiral alnamudhajiu liltawthiq altijarii alduwalii mae dalil aliaishtirae aistiemaluh , manshurat al'umam almutahida .A05.V4. Y..E
• alqanun raqm 175 lisanat 2018m fi shan mukafahat jarayim taqniat almaelumat almanshur bialjaridat alrasmiat aleadad 32 mukarir fi15 'aghustus 2018.
• qarar majlis wuzara' aleadl alearab aldawrat altaasieat alqarar raqm 495 - 19 - 2003/10/8m.
• muhamad 'abubakr yunis , aljarayim alnaashiat ean astikhdam al'iintirnit (al'ahkam almawdueiat waljawanib al'iijrayiyat , dar althaqafat alearabiat lilnashr , 2004m.
• muhamad bin eabd allah alqahtanii , 'amn almaelumat , jamieat almalik eabd aleaziz lileulum waltiqniati, alriyadi,2009m.
• muhamad hamaad mirhij alhiti, "jarayim alhasub , t , 'iidarat almanahij lilnashr waltawziei, eaman, 2006m
• muhamad shawaabikat , jarayim alhasub wal'iintarnit , dar althaqafat eamaan , t 1, 2004 . s 13., waqad talafi almusharie almisriu fi alqanun raqm 175 lisanat 2018m.
• muhamad fahmi talabat , fayrusat alhasib wa'amn albayanat , majmueat alniyl alearabiat liltibaeat walnashri, 1991m.
• muhamad muhamad al'alfi , waraqat eamal muqadimat fi nadwat himayat nazam almaelumat fi almuasasat alearabiat , alqahirat ,2007m.
• mdahat ramadan : - jarayim aliaetida' ealaa al'ashkhas wal'iintarnit , dar alnahdat alearabiat n alqahirat ,2007m.
• miftah bu bakr almutaridiu , aljarimat al'iiliktruniat , waraqat eamal muqadimat 'iilaa almutamar althaalith liruasa' almahakim aleulya fi alduwal alearabiat , alsuwdan 23-25 'aylul 2001m.

• mamduh khalil bahr :- nitaq himayat alhayat alkhasat fi alqanun aljinayiyi , dar althaqafat lilnashr waltawzie , al'urduni , 2006m.
• mamduh eabd alhamid eabd almutalabi, zubaydat muhamad qasama, eabd allah eabd aleaziza, 'unmudhaj muqtarah liqawaeid aietimad aldalil alraqmii lil'iithbat fi jarayim alkumbiutar, mutamar al'aemal almasrifiat al'iilikturuniat, kuliyat alsharieat walqanuni, al'iimaratu, ghurfat tijarat wasinaeat , dibi, 5-10/12/2003m.
• nadiat 'amin muhamad eali , alfayrusat waturuq alwiqayat minha kawasilat li'amn albayanat , almutamar alduwaliu al'awal hawl 'amn almaelumat , nahw takamul raqamay amn disambir 2005 , masqat eaman.
• nayil eabd alrahman salihi, waqie, jarayim alhasib fi altashrie al'urduniyi , bahath muqadim limutamar alqanun walkumbuyutir wal'iintirnit aladhi nazamath kuliyat alsharieat walqanun - jamieat al'iimarat alearabiat almutahida (2000) buhuth mutamar alqanun walkumbuyutir wal'iintirnit , almujalad al'awal , altabeat althaalithat , kuliyat alsharieat walqanun jamieat al'iimarat alearabiat almutahidat , 2004m.
• nayilat eadil muhamad farid qurat, jarayim alhasib alaiqtisadiat risalat dukturah jamieat alqahirati, kuliyat alhuquqi, tabeat 2003m.
• najam eabd allah alhumaydii , nazam almaelumat al'iidariat madkhal mueasir , altabeat althaaniat , dar alyazurii lilnashr waltawziei, eamaan , al'urduni , 2009m.
• nizam mukafahat jarayim almaelumatiat , hayyat alaitisalat watiqniat almaelumati, almamlakat alearabiat alsueudiati.
• hady hamid qashqush : himayat alhasib al'iilikturuni , fi altashrie almuqarani, dar alnahdat alearabiati, alqahirat 1992m.
• hisham farid rustum , qanun aleuqubat wamakhatir tiqniat almaelumati, maktabat alalat alhadithati, 'asyut, 1992.
• alhimayat aljinayiyat lil'iinsan fi suratih , maktabat alalat alhadithat , 'asyuta.
• haytham hamuwd alshabli , 'iidarat makhatir alaihtial fi qitae alaitisalat , dar safa' lilnashr waltawzie , t 1 , eamaan , al'urduni 2009m.
• haytham muhamad alzuebi , 'iiman fadil alsaamaraayiyu , nazam almaelumat al'iidariata, altabeat al'uwlaa, dar safa' lilnashr waltawzie , eamaan , 2004m .

• wayil bunduq , mawsueat alqanun al'iilikturuni watiknulujia aliaitisal walmaelumat , dar almatbueat aljamieiat , al'iiskandariat , ta1 , 2007m. yusif khalil yusif eabd aljabir , madaa faeiliat 'iijra'at alraqabat aldaakhiliat fi tawfir 'amn almaelumat al'iiliktruniat fi alsharikat alsinaeiat al'urduniyat , risalat majistir , jamieat alsharq al'awsat ,2013m.
• yunis earab: qira'at fi aliaitijahat altashrieiat liljarayim al'iilikturuniat mae bayan mawqif alduwal alearabiat watajribat saltanat euman , warshat eamal tatwir altashrieat fi majal mukafahat aljarayim al'iilikturuniat , masqat , 2-4 'abril 2001m.
• yunis earab , jarayim alkumbiutir walantirnit , 'iijaz fi almafhum walnitaq walkhasayis walsuwar walqawaeid al'iijrayiyat lilmulahaqat wal'iithbati, waraqat eamal muqadimat 'iilaa mutamar al'amn alearabii 2002m tanzim almarkaz alearabii lildirasat walbuhuth aljinayiyat , 'abu zabi , s 11 , 10 - 12/2 20m.

فهـــرس الموضوعـــات

الموضـــوع الصفحة