الإرشاد الخامس

الجرائم السيبرانية

٥

الورقة البحثية الخلفية لإرشاد الجرائم السيبرانية

١- هدف البحث

تتناول الورقة الشرحية الخلفية لموضوع الجرائم السيبرانية في الدول العربية، رصد وتحليل التشريعات العربية التي عالجت هذا الموضوع ومقارنتها مع الاتفاقيات الدولية المرتبطة، لتسليط الضوء على الثغرات والنقاط التي أغفلتها التشريعات العربية بهدف مساعدة الحكومات العربية على معالجتها وتنظيمها من خلال سن أو تعديل تشريعاتها الموجودة أو إصدار قرارات أو تنظيمات خاصة تتعلق بالجرائم السيبرانية بشكل يتناسب مع التشريعات والتنظيمات الدولية.

٢- موضوع وأقسام البحث

ينص مشروع إعداد "إرشادات الإسكوا للتشريعات السيبرانية" على أن تؤخذ بعين الاعتبار الخبرات الدولية والإقليمية المتراكمة مع تركيز خاص على "توجيهات الاتحاد الأوروبي" في هذا المجال لأجل صياغة الإرشاد الخاص بالجرائم السيبرانية.

تناولت أعمال البحث بشكل رئيسي الجرائم التالية:

١) **جرائم التعدي على البيانات المعلوماتية:** شملت الجرائم التي يكون موضوعها البيانات المعلوماتية أي التي تقع على بيانات معلوماتية، وهي جرائم التعرض للبيانات المعلوماتية وجرم اعتراض بيانات معلوماتية.

٢) **جرائم التعدي على الأنظمة المعلوماتية:** وتتناول جرائم الولوج غير المشروع إلى نظام معلوماتي أو المكوث فيه وجرائم الولوج غير المشروع إلى نظام معلوماتي أو المكوث فيه مع التعرض للبيانات المعلوماتية وجرائم إعاقة عمل نظام معلوماتي.

٣) **إساءة استعمال الأجهزة أو البرامج المعلوماتية:** تتناول جرائم إساءة إستعمال الأجهزة أو البرامج المعلوماتية وجرائم كل من قدّم أو أنتج أو وزّع أو حاز بغرض الاستخدام جهازاً أو برنامجاً معلوماتياً أو أية بيانات معلوماتية معدّة أو كلمات سر أو كودات دخول، وذلك بغرض اقتراف أي من الجرائم المنصوص عليها سابقاً.

٤) **الجرائم على الأموال:** تشمل جرم الاحتيال أو الغش بوسيلة معلوماتية وجرم التزوير المعلوماتي وجرم الاختلاس أو سرقة أموال بوسيلة معلوماتية وجرم أعمال التسويق والترويج غير المرغوب فيها وجرم الاستيلاء على أدوات التعريف والهوية المستخدمة في نظام معلوماتي والاستخدام غير المشروع لها وجرم الإطلاع على معلومات سرية أو حساسة أو إفشائها.

٥) **جرائم الاستغلال الجنسي للقاصرين:** وهي الأفعال التي تتعلق باستغلال القاصرين في أعمال جنسية، وتشمل الرسوم أو الصور أو الكتابات أو الأفلام أو الإشارات أو أية أعمال إباحية يشارك فيها قاصرون أو تتعلق باستغلال القاصرين في المواد الإباحية. وتشمل أيضاً إنتاج مواد إباحية للقاصرين بقصد بثها بواسطة نظام معلوماتي.

٦) **جرائم التعدي على الملكية الفكرية للأعمال الرقمية:** تشمل الجرائم التالية: جرم وضع اسم مختلس على عمل، وجرم تقليد إمضاء المؤلف أو ختمه، وجرم تقليد عمل رقمي أو قرصنة البرمجيات، وجرم بيع أو عرض عمل مقلّد أو وضعه في التداول، وجرم الاعتداء على أي حق من حقوق المؤلف أو الحقوق المجاورة.

٧) **جرائم البطاقات المصرفية والنقود الإلكترونية:** تشمل أعمال تقليد بطاقة مصرفية عن قصد بصورة غير مشروعة واستعمالها عن قصد، وتزوير نقود إلكترونية بصورة غير مشروعة وعن قصد، لما لذلك من إخلال بالاقتصاد الوطني وتأثير سلبي على العمليات المصرفية.

٨) **الجرائم التي تمسّ المعلومات الشخصية:** تشمل الأفعال الجرمية التي تتعلق بمعالجة البيانات ذات الطابع الشخصي دون حيازة تصريح أو ترخيص مسبق يتيح القيام بالمعالجة، وإفشاء معلومات ذات طابع شخصي لأشخاص لا يحق لهم الإطلاع عليها.

٩) **جرائم العنصرية والجرائم ضد الإنسانية بوسائل معلوماتية:** وتشمل جرم نشر وتوزيع المعلومات العنصرية بوسائل معلوماتية، وجرم تهديد أشخاص أو التعدي عليهم بسبب انتمائهم العرقي أو المذهبي أو لونهم وذلك بوسائل معلوماتية، وجرم توزيع معلومات بوسيلة إلكترونية

من شأنها إنكار أو تشويه أو تبرير أعمال إبادة جماعية أو جرائم ضد الإنسانية، وجرم المساعدة أو التحريض بوسيلة إلكترونية على ارتكاب جرائم ضد الإنسانية.

١٠) جرائم المقامرة وترويج المواد المخدرة بوسائل معلوماتية: تشمل جرم تملك وإدارة مشروع مقامرة على الإنترنت، وجرم تسهيل وتشجيع مشروع مقامرة على الإنترنت، وجرم ترويج الكحول للقاصرين على الإنترنت، وجرم ترويج المواد المخدرة على الإنترنت.

١١) جرائم المعلوماتية ضد الدولة والسلامة العامة: تشمل الأفعال الجرمية الناشئة عن المعلوماتية التي تطال الدولة وسلامتها وأمنها واستقرارها ونظامها القانوني، وهي جرائم تعطيل الأعمال الحكومية أو أعمال السلطة العامة باستعمال وسيلة معلوماتية.كما وتشمل جرائم الإخفاق في الإبلاغ أو الإبلاغ عن قصد بشكل خاطئ عن جرائم المعلوماتية، والإطلاع أو الحصول على معلومات سرية تخص الدولة، وذلك من خلال شبكة الإنترنت أو باستعمال وسيلة معلوماتية. بالإضافة إلى فعل العبث بالأدلة القضائية المعلوماتية أو إتلافها أو تخبئتها، والأعمال الإرهابية التي ترتكب باستعمال شبكة الإنترنت أو أية وسيلة معلوماتية. وجرائم التحريض على القتل باستعمال شبكة الإنترنت أو أية وسيلة معلوماتية.

١٢) جرائم تشفير المعلومات: تشمل أفعال تسويق أو توزيع أو تصدير أو استيراد وسائل تشفير دون حيازة ترخيص أو تصريح من قبل المراجع الرسمية المختصة في الدولة، وأفعال تقديم وسائل تشفير تؤمن السرية دون حيازة تصريح أو ترخيص من قبل المراجع الرسمية المختصة في الدولة، بالإضافة إلى بيع أو تسويق أو تأجير وسائل تشفير ممنوعة.

وأبرز ما تناوله البحث الأعمال التالية:

١) الوثائق الرسمية الأساسية الصادرة عن الأمم المتحدة والمجلس الأوروبي المتعلقة بهذا المجال ومنها:

- Convention on Cybercrime, Budapest, 23.XI.2001

- Additional Protocol to the Convention on Cybercrime - Explanatory Report.

- Additional Protocol to the Convention on Cybercrime Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems (released 7 November 2002)

- European Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography.

- European Council Decision of 29 May 2000 to combat child pornography on the Internet, Official Journal L 138 , 09/06/2000 P. 0001 – 0004

- Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems

- Recommendation No. R (89) 9 Of the Committee of Ministers to Member States on Computer-related crime

٢) وتناولت أعمال البحث أيضاً مختارات من تشريعات وطنية من دول أجنبية[1] مختلفة تناولت تنظيم التجارة الإلكترونية، وبخاصة منها التشريعات الأميركية، الفرنسية، البلجيكية، السويسرية، البريطانية، الكندية، الاسترالية، بالإضافة إلى بعض التشريعات الخاصة من دول أسيا الوسطى.

٣) كما وقد تم الاسترشاد بالمراجع الفقهية العالمية والعربية الخاصة بالجرائم السيبرانية:

- Fraud in the Internet, by Computer Crime Research Center, April 11, 2005
http://www.crime-research.org/articles/Internet_fraud_0405/

- Cybercriminals Reinvent Methods of Malicious Attacks, by Trend Micro Incorporated, July 11, 2008,
http://www.crime-research.org/analytics/3451/

- Cyber-crimes - Analytical data compiled, by Vladimir Golubev, published on Computer Crime Research Center,
http://www.crime-research.org/analytics/cyber_crimes0108/

- Crime on The Net,
http://rogerdarlington.me.uk/crimeonthenet.html#Hacking

- What is Cyber-terrorism, by Serge Krasavin Ph.D. MBAv, published by Computer crime research center (CCRC)
http://www.crime-research.org/library/Cyber-terrorism.htm

- How Computer Viruses Work, by Marshall Brain
http://computer.howstuffworks.com/virus2.htm

- How Hackers Work, Microsoft,
http://technet.microsoft.com/en-us/library/cc505928.aspx

- Cybershock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists and Weapons of Mass Disruption, Winn Schwartau, John Draper, January 2010.
http://www.terrorism.com/content/cybershock-

- Cyber Terrorism Vulnerabilities and Policy Issues "Facts Behind The Myth", Dhanashree Nagre Priyanka Warade http://www.contrib.andrew.cmu.edu/~dnagre/Final_Report_dnagre_pwarade.pdf

- Tracking a Computer Hacker, by *Daniel A. Morris*, Assistant United States Attorney Computer and Telecommunications Coordinator, District of Nebraska; published on 2005. http://www.cybercrime.gov/usamay2001_2.htm

- Internet Blocking: Crimes Should Be Punished and Not Hidden, by *Joe McNamee* - EUROPEAN DIGITAL RIGHTS (EDRI), June 2010. http://www.soros.org/initiatives/information/focus/policy/articles_publications/publications/edri-blocking-100606/EDRI-blocking-100606.pdf

- Data Breaches: What the Underground World of "Carding" Reveals, by *Kimberly Kiefer Peretti*- U.S. Department of Justice-Computer Crime and Intellectual Property Section. http://www.cybercrime.gov/DataBreachesArticle.pdf

- IT security and crime prevention methods, Published by *Interpol*, http://www.interpol.int/Public/TechnologyCrime/CrimePrev/ITSecurity.asp

- Financial and high-tech crimes, http://www.interpol.int/Public/FinancialCrime/Default.asp

- The Globalization of Crime a Transnational Organized Crime Threat Assesment, UNODC, 2010, page 203- 209 http://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf

- الإطار التشريعي لجرائم المعلوماتية والإنترنت، الدكتور نضال الشاعر، مؤتمر "جرائم المعلوماتية والإنترنت – نظرة على دول الشرق الأوسط- شباط ٢٠٠٦ http://www.ijma3.org/Admin/Additionals/Cybercrime/Judge%20Nidal%20El%20Chaer%20Presentation.pdf

- جرائم الحاسوب الاقتصادية، دراسة نظرية وتطبيقية، دكتور نائلة عادل محمد فريد قورة، جامعة حلوان، مصر.

- مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية، تأليف د. ناصر بن محمد البقمي، سنة ٢٠٠٩.

- الجرائم المعلوماتية، ماهيتها وصورها، تأليف الدكتور محمود صالح العادلي أستاذ القانون الجنائي، ورشة العمل الإقليمية حول: تطوير التشريعات في مجال مكافحة surviving-hackers-phreakers-identity-thieves-internet-terrorists-and-weapons-mass

- Prosecuting Computer Crimes Manual, published February, 2007. http://www.justice.gov/criminal/cybercrime/ccmanual/index.html

- Fighting cyber terrorism, by Carol Ko, June 17, 2008, Source: Computerworld.com.my http://www.crime-research.org/news/17.06.2008/3416/

- Organized crime: from trafficking to terrorism, By Frank Shanty http://books.google.com.lb

- Intellectual Property crimes: are proceeds from counterfeited goods funding terrorism? Hearing before the committee on International relations House of Representatives, July 16, 2003, Serial No. 108–48 http://www.foreignaffairs.house.gov/archives/108/88392.pdf

- Prosecuting Intellectual Property Crimes manual, Third Edition September 2006, CCIPS Criminal Division http://www.justice.gov/criminal/cybercrime/ipmanual/index.html

- COMPUTER-RELATED OFFENCES. A presentation at the Octopus Interface 2004 - Conference on the Challenge of Cybercrime, 15-17 September 2004, Council of Europe, Strasbourg, France. http://www.cybercrimelaw.net/documents/Strasbourg.pdf

- Recommendation No. R (89) 9 Of the Committee of Ministers to Member States on Computer-related crime and final Report of the European Committee on Crime Problems. http://www.oas.org/juridico/english/89-9&final%20Report.pdf

- Cyber Crime has Surpassed Illegal Drug Trafficking as a Criminal Moneymaker1; 1 in 5 will become a Victim2; http://www.symantec.com/about/news/release/article.jsp?prid=20090910_01

- Internet Gambling: Overview of federal criminal law; http://books.google.com.lb/

- The Myth of Cyberterrorism: There are many ways terrorists can kill you-computers aren't one of them. Joshua Green, The Washington Quartlerly Online http://www.washingtonmonthly.com/features/2001/0211.green.html

الجرائم الإلكترونية" مسقط ٢-٤ ابريل ٢٠٠٦م.
www.ituarabic.org/coe/2006/E-Crime/.../Doc2-Text-ar.DOC

- الجرائم الإلكترونية تشكل تحديات أمام القانون.ونظام المكافحة في المملكة حماية للاقتصاد الوطني. تأليف عبدالله عبد العزيز العجلان. صحيفة الرياض.
http://www.alriyadh.com/2008/02/29/article321790.html

- التحديات القانونية في الجرائم الإلكترونية. تأليف سمية بنت عبد الرحمن بن سليمان الحمدا.
http://coeia.edu.sa/index.php/ar/asuurance-awarness/articles/51-forensic-and-computer-crimes/1075-legal-challenges-in-cyber-crime.html

٤) وتم الاسترشاد أيضاً بالدراسات التي أعدتها منظمة الإسكوا في هذا المجال وأهمها: ١- متابعة التطورات الحاصلة في التشريعات السيبيرانية في الأردن وسوريا ولبنان وفلسطين والعراق. ٢- وضع التشريعات السيبرانية في سلطنة عمان ، دولة الإمارات العربية المتحدة ، دولة قطر. ٣- وضع التشريعات السيبرانية في السعودية والكويت واليمن.

٥) بالإضافة إلى ذلك تناولت أعمال البحث مراكز مكافحة الجرائم السيبرانية. وأبرزها:

- Computer Crime & Intellectual Property Section United States Department of Justice
http://www.justice.gov/criminal/cybercrime/reporting.htm

- Internet Crime Complaint Center (IC3)
http://www.ic3.gov/default.aspx

- Department of Defence-United States of America Cyber Crime Center,
http://www.dc3.mil/

- Computer Crime Task Forces – USA,
http://www.ccmostwanted.com/CP/LEccuUS.htm

- Computer Crime Task Forces – Global,
http://www.ccmostwanted.com/CP/LEccuGL.htm

- موقع مكتب مكافحة غسيل الأموال التابع لوزارة التجارة والصناعة في الكويت
http://www.mlcoo.org

٦) كذلك تناولت أعمال البحث التشريعات ومشاريع القوانين التابعة للدول العربية؛ إضافة إلى القرارات والقوانين النموذجية الصادرة عن جامعة الدول العربية والأنشطة والتجارب التي قامت بها ضمن هذا النطاق.

تجدر الإشارة من ناحية أخرى إلى انه تم التركيز على تحليل التشريعات الوطنية العربية الخاصة بمكافحة الجرائم السيبرانية. ومقارنتها مع التشريعات الأجنبية لمعرفة مدى شموليتها للنقاط التي يجب أن يتناولها هذا الإرشاد.

وبالتالي سنعرض أهم مخرجات البحث لهذه الجهة.

أ- بالنسبة للتشريعات الوطنية العربية الخاصة بالجرائم السيبرانية

تبين أثناء أعمال البحث أن هناك أربع دول عربية فقط عملت على إصدار تنظيم الجرائم السيبرانية ضمن تشريعات خاصة بها وهي السعودية. والإمارات العربية المتحدة والأردن والسودان. أما الأردن فقد أصدر قانوناً مؤقتاً لسنة ٢٠١٠ لمكافحة جرائم أنظمة المعلومات[١]. تتناول هذه التشريعات تحديد الأفعال الجرمية المرتكبة عبر شبكة الإنترنت والتي تعتبر جرائم معلوماتية كما تناولت العقوبات المقررة لكل منها وذلك لتحقيق الأهداف التالية: تحقيق الأمن المعلوماتي. حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية. حماية المصلحة العامة. والآداب والأخلاق العامة. وحماية الاقتصاد الوطني.

وهذه التشريعات المتعلقة بالجرائم السيبرانية هي التالية:

الأردن:
قانون جرائم أنظمة المعلومات لسنة ٢٠١٠
http://www.watnnews.net/NewsDetails.aspx?NewsID=12801

الإمارات العربية المتحدة:
القانون الاتحادي رقم ٢ لسنة ٢٠٠٦ في شأن مكافحة جرائم تقنية المعلومات
http://www.theuaelaw.com/vb/showthread.php?t=1022

السودان:
قانون رقم ١٤ لسنة ٢٠٠٧

تجدر الإشارة إلى أن ثمة بلداناً عربية أخرى قد أطلقت ورشة إعداد مشاريع قوانين لإصدار قانون خاص بالجرائم المعلوماتية. مثال:

سوريا، التي قامت بإعداد مشروع قانون مكافحة الجرائم الإلكترونية وحماية البيانات الشخصية السوري[٣].

وقد عمدت بعض الدول العربية مثال سلطنة عمان إلى تعديل قانونها الجزائي ليشمل أحكاماً تتعلق بجرائم الحاسوب، وأصدرت دول أخرى قرارات أو مراسيم من شأنها مكافحة بعض جرائم المعلوماتية مثال لبنان، وهناك دول أخرى قامت بتشكيل هيئات مختصة لمكافحة جرائم الحاسوب:

سلطنة عمان:
مرسوم سلطاني رقم ٢٠٠١/٢٧، تعديل بعض أحكام قانون الجزاء العماني ، إضافة المادة ٢٧٦ مكرر حول جرائم الحاسوب
http://www.oman-net.net/vb/t443.html

الكويت:
مشروع قانون لمكافحة جرائم شبكة الإنترنت وتقنية المعلومات، أعدته النيابة العامة الكويتية[٤].

لبنان:
- تعميم رقم ٤ تاريخ ٢٠٠٦/٠٥/٢٥، حماية برامج المعلوماتية ومكافحة القرصنة.
- قرار رقم ٧٨١٨ تاريخ ٢٠٠١/٨/٥ نظام مراقبة العمليات المالية والمصرفية لمكافحة تبييض الأموال.

مصر:
قرار وزاري رقم ٣٢٧ لسنة ٢٠٠٥، إنشاء إدارة متخصصة لمكافحة جرائم الحاسبات والشبكات بوزارة الداخلية تسمى "إدارة مباحث مكافحة جرائم الحاسبات الإنترنت".

السعودية:
نظام مكافحة جرائم المعلوماتية
http://www.mcit.gov.sa/arabic/Regulations/CriminalLaws/

اليمن:
مشروع قانون لمكافحة الجرائم الإلكترونية[٥].

إلا أننا نلاحظ أن معظم التشريعات الصادرة في الدول العربية والمتعلقة بالمعاملات والتواقيع الإلكترونية والتجارة الإلكترونية وحماية المستهلك نصت على مواد تحدد الجرائم المعلوماتية التي ترتكب في معرض ممارسة المعاملات أو التجارة الإلكترونية ومواد تتضمن العقوبات المترتبة عليها، وهي:

الأردن:
القانون الصادر في ٢٠٠١/١٢/٣١ بشأن المعاملات الإلكترونية.

البحرين:
مرسوم قانون رقم ٢٨ لسنة ٢٠٠٢ بشأن المعاملات الإلكترونية.

سوريا:
قانون رقم ٤ الصادر في ٢٠٠٩/٠٢/٢٥ بشأن التوقيع الالكتروني وخدمات الشبكة.

سلطنة عمان:
مرسوم سلطاني رقم ٢٠٠٨/٦٩ بإصدار قانون المعاملات الإلكترونية.

فلسطين:
مشروع قانون المبادلات والتجارة الإلكترونية.

مصر: قانون رقم ١٥ لسنة ٢٠٠٤ بشأن التوقيع الالكتروني.

الكويت:
مشروع قانون المعاملات الإلكترونية.

السعودية:
نظام التعاملات الإلكترونية.

اليمن:
قانون رقم ٤٠ لسنة ٢٠٠٦ بشأن أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية.

من ناحية أخرى، نفيد ضمن هذا المجال أن جامعة الدول العربية قد قامت بتبني قانون الإمارات العربية المتحدة الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها، وهذا القانون تناول تحديد جرائم المعلوماتية وتحديد العقوبات عند ارتكاب هذه الجرائم، من حبس وفرض غرامات وإبعاد الأجنبي المخالف.

ب - شمولية التشريعات الوطنية الخاصة

كما ذكرنا أعلاه، نجد أن السعودية والإمارات العربية المتحدة والأردن والسودان فقط، قد أصدرتا تشريعات خاصة بمكافحة جرائم تقنية المعلومات في منطقة الإسكوا، حيث اكتفت الدول العربية الأخرى بتجريم الأفعال غير المشروعة التي

ترتكب أثناء القيام بالمعاملات والتجارة الإلكترونية وفرض العقوبات المترتبة عليها فقط. لذا نجد أن هذه العقوبات غير شاملة لجميع الجرائم المعلوماتية. وعلى سبيل المثال، إنّ جرائم تشفير المعلومات وجرائم الاستغلال الجنسي للقاصرين عبر الإنترنت أو جرائم ترويج المخدرات عبر الانترنت بقيت غير منظمة ضمن مواد قانونية خاصة وبالتالي لا يجرم مرتكبوها ولا يعاقبون في حال تم ارتكابها عملاً بالمبدأ الساري "لا عقوبة بدون نص".

أما التشريعات الخاصة بمكافحة جرائم المعلوماتية الصادرة عن السعودية والإمارات العربية المتحدة، فهي تتناول مواد عقابية حول الدخول غير المشروع إلى المواقع الإلكترونية والأنظمة المعلوماتية المملوكة من الغير، وانتهاك المعتقدات الدينية أو الحياة الخاصة، والدخول غير المشروع واللعب بالبيانات الشخصية، والتنصت أو التقاط أو اعتراض الرسائل الإلكترونية، والتهديد والابتزاز عبر الوسائط الإلكترونية، وجرائم البطاقات المصرفية والتحاويل والنقود الإلكترونية. وتناولت أيضاً الجرائم الماسة بالنظام العام والآداب العامة، وجرائم الاتجار بالجنس البشري وجرائم الإرهاب وجرائم غسل الأموال والمخدرات، بالإضافة إلى أنها شملت أيضاً الجرائم الماسة بالملكية الفكرية عبر شبكة الإنترنت.

وقد تصل العقوبات المترتبة على جرائم المعلوماتية إلى حد السجن لفترة خمس سنوات بالإضافة إلى فرض الغرامات وإبعاد الأجنبي عن البلد الذي ارتكبت فيه الجريمة.

وقد شمل قانون الجزاء العماني، بعد تعديله وإضافة المادة ٢٧٦ (مكرر) عليه، تحديد الجرائم التي تعتبر جرائم معلوماتية، فكان أن شملت المواد القانونية المذكورة أعلاه معظم جرائم المعلوماتية، إلا أنها لم تتطرق إلى جرائم التشفير وجرائم الاستغلال الجنسي للقاصرين عبر الانترنت، وجرائم المقامرة وترويج المواد المخدرة بوسائل معلوماتية، وجرائم المعلوماتية ضد الدولة والسلامة العامة. وقد نصّت هذه المادة على الآتي: "يعاقب بالسجن مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنتين....كل من تعمد استخدام الحاسوب في ارتكاب احد الأفعال التالية: ١- الالتقاط غير المشروع للمعلومات أو البيانات، ٢- الدخول غير المشروع على أنظمة الحاسوب، ٣- التجسس والتنصت على البيانات والمعلومات، ٤- انتهاك خصوصيات الغير أو التعدي على حقهم في الاحتفاظ بإسرارهم، ٥- تزوير بيانات أو وثائق مبرمجة أياً كان شكلها، ٦- إتلاف وتغيير ومحو البيانات والمعلومات، ٧- جمع المعلومات والبيانات وإعادة استخدامها، ٨- تسريب المعلومات والبيانات، ٩- التعدي على برامج الحاسوب سواء بالتعديل أو الاصطناع، ١٠- نشر واستخدام برامج الحاسوب بما يشكل انتهاكاً لقوانين حقوق الملكية والأسرار التجارية".

ونصت المادة ٢٧٦ (مكرر ٣) على انه " يعاقب بالسجن مدة لا تزيد على ٥ سنوات وبغرامة لا تتجاوز ألف ريال كل من: ١- قام بتقليد أو تزوير بطاقة من بطاقات الوفاء أو السحب، ٢- استعمل أو حاول استعمال البطاقة المقلدة أو المزورة مع العلم بذلك، ٣- قبل الدفع ببطاقة الوفاء المقلدة أو المزورة مع العلم بذلك". كما جاء في المادة ٢٧٦ (مكرر ٤) على انه " يعاقب بالسجن مدة لا تزيد على ٣ سنوات وبغرامة لا تتجاوز خمسمائة ريال كل من: ١- استخدم البطاقة كوسيلة للوفاء مع علمه بعدم وجود رصيد له، ٢- استعمل البطاقة بعد انتهاء صلاحيتها أو إلغائها وهو عالم بذلك، ٣- استعمل بطاقة الغير بدون علمه".

أما تعميم مصرف لبنان القاضي بحماية برامج المعلوماتية ومكافحة القرصنة فينص على "أن الحماية القانونية لبرامج الحاسوب مهما كانت لغاتها، بما في ذلك الأعمال التحضيرية، تخضع للتشريعات المتعلقة بحماية الملكية الفكرية في لبنان، لاسيما قانون الملكية الأدبية والفنية رقم ١٩٩٩/٧٥." بالإضافة إلى **نظام مراقبة العمليات المالية والمصرفية لمكافحة تبييض الأموال** القاضي بتجريم غسيل الأموال عبر التحاويل الإلكترونية.

إلا أننا نجد أن المشرع العربي قد حدد بعض الجرائم المعلوماتية وفرض على مرتكبيها العقوبات في تشريعات متفرقة كالتشريعات الخاصة بالمعاملات والتجارة الإلكترونية، والاتصالات وحقوق المؤلف والملكية الفكرية، وقانون العقوبات. فقد ورد مثلاً، في المرسوم بقانون رقم (٥) لسنة ١٩٩٩م بشأن حقوق الملكية الفكرية في الكويت، تحديد المخالفات المرتبطة مباشرة ببرامج الحاسوب والتي يمكن أن تنطبق على كل من برامج الحاسوب وقواعد البيانات، وأي إنتاج مرتبط بتقنية المعلومات. ونص التشريع ذاته على أن يعاقب بالحبس مدة لا تزيد على سنة واحدة وبغرامة لا تزيد عل خمسمائة دينار أو بإحدى هاتين العقوبتين: ١- كل من كشف أو سهّل كشف برامج الحاسوب قبل نشرها، ٢- كل من ساعد في إزالة حماية تنظيم أو تقييد إطلاع الجمهور على المصنف أو الأداء أو البث أو التسجيل. كذلك الأمر بالنسبة إلى سلطنة عمان حيث جرّم المشرع العماني من القانون رقم ٦٥ لسنة ٢٠٠٨ بشأن حماية حق المؤلف والحقوق المجاورة في المادة ٥٢ بيع وتداول البرامج الحاسوبية دون إذن صاحبها سواء تم ذلك بالطرق التقليدية أو بالطرق المستحدثة كاستخدام شبكة الإنترنت وفرض

عقوبة السجن سنتين كحدٍ أقصى فضلاً عن غرامة مالية لا تزيد عن عشرة آلاف ريال.

هوامش

١ – راجع لائحة تشريعات الدول الأجنبية – ملحق رقم ٣.

٢– راجع القانون المؤقت لمكافحة جرائم أنظمة المعلومات
http://www.watnnews.net/NewsDetails.aspx?NewsID=12801

٣– راجع مشروع قانون مكافحة الجرائم الإلكترونية وحماية البيانات الشخصية السوري المنشور على الموقع الالكتروني:
http://www.dp-news.com/pages/detail.aspx?l=1&articleId=58379

٤– راجع مشروع قانون لمكافحة جرائم شبكة الإنترنت وتقنية المعلومات:
http://www.kwtfuture.com/vb/t8495.html

٥– راجع مشروع قانون لمكافحة الجرائم الإلكترونية
http://sh22y.com/vb/t10623.html

مقدمة إرشاد الجرائم السيبرانية

أسهم التطور التقني المتلاحق في أجهزة وأنظمة وشبكات الحاسوب[1] والإمكانية المتاحة لأي فرد في أن يمتلك ويستعمل جهاز حاسوب أو هاتف محمول في المنزل أو في المقهى أو أي مكان عام إلى تغيير كبير في ارتكاب الفعل الإجرامي[2] وفي ابتداع أساليب جديدة لارتكاب الجرائم السيبرانية وتبعاً لذلك تطور المفهوم الجرمي[3]، حيث لم يعد المجرم بحاجة إلى أدوات إجرامية وأساليب غير تقليدية، بل يكفي أن يكون الشخص ملماً باستعمال الحاسوب وأنظمته لكي يقوم بارتكاب جريمة من جرائم الفضاء السيبراني، سواء كانت الوسائل المعلوماتية أداة الجريمة أو كانت ضحية الفعل الجرمي. ومثال ذلك التعدي على حقوق المؤلف عبر تحميل أغاني أو أفلام مجاناً عن شبكة الإنترنت أو مشاهدة وإرسال أفلام إباحية تشمل الأطفال أو من هم دون السن القانونية بواسطة البريد الالكتروني الخ.. أو وضع برنامج خبيث[4] يمكن من خلاله خرق شبكة حواسب أو تدمير نظام حمائي أو اختراق جهاز آخر.

يعتمد المبدأ العام في القانون الجزائي في مختلف التشريعات والأنظمة القانونية على عدم التوسع في تطبيق و تفسير القواعد الجزائية وذلك لأن هذه القواعد تنص على عقوبات وتدابير إكراهية تنال من حرية الشخص أو ماله أو حقه بالتمتع بحقوقه. لهذا السبب لا يسوغ التوسع في تفسير هذه القواعد عبر القياس أو التحليل الخاص بالقاضي إذ من شأن ذلك الخروج عن مبدأ: لا عقوبة ولا جريمة بدون نص، وبسبب عدم جواز تشويه الإرادة الفعلية للمشترع عند وضعه نص القانون الجزائي إذ من خلال التوسع في التفسير قد تجرم أفعال لم يقصد المشترع، المعبّر عن إرادة المجتمع، تجريمها أو لا تعتبر أفعال أخرى جريمة تستوجب العقوبة المنصوص عنها في نص القانون الذي جرى تفسيره ليطابق جريمة الحاسوب أو الفضاء السيبراني. إلا انه مع ذلك ثمة أنظمة قانونية تستخدم في صياغتها لوصف الفعل الجرمي عبارات قد تفتح المجال لتوسّع نسبي في التفسير، ومن قبيل ذلك استعمال عبارة آلي في نص من قانون العقوبات باللغة العربية مما يسمح بان تشمل الأدوات المعلوماتية كونها تعتبر من الأدوات الآلية أيضاً.

ومن جهة أخرى، يقوم قانون الجزاء أو العقوبات على ركيزتين أساسيتين هما التجريم (وصف فعل على أنه جرم) والعقاب، إذ أن إعطاء وصف جرمي لفعل ما وفرض عقوبات عليه يخضع عادةً لاعتبارات ثقافية واجتماعية وضرورات اقتصادية خاصة بالدولة. فما يعتبر جرماً يمس الآداب العامة في الوطن العربي قد يعتبر تعبيراً عن الرأي في أوروبا، طبعاً مع الأخذ بعين الاعتبار أن العولمة أوجبت على المشترع اعتماد تعاريف ووصف لبعض الجرائم متلائمة مع القوانين العالمية الأمر الذي يجعل المشرع العربي ملزماً باعتماد الوصف الذي أعطاه المشرع الدولي لهذه الجرائم. فقد تتجه إرادة الناس في بعض المجتمعات إلى تشديد العقوبة على الجرائم التي تتناول مقدسات دينية أو أعمالاً لها علاقة بالعمليات المصرفية، بينما لا نرى مثل هذا التوجه في مجتمعات أخرى.

تنقسم جريمة الحاسوب أو جريمة الفضاء السيبراني[5] إلى نوعين أساسيين: النوع الأول هو الذي يكون فيه الحاسوب أداة تنفذ بواسطتها الجريمة، كجرائم الاختلاس وانتحال الصفة والأفعال الإباحية. وهي جرائم عادية والحاسوب هو مجرد الوسيلة التي سمحت بارتكابها. والنوع الثاني هو الذي يكون فيه جهاز الحاسوب وشبكات الحواسيب وبرامجها موضوعاً للجريمة، أي أن الفعل الجرمي ارتكب على هذا الجهاز، مثل اختراق نظام أمان أو إرسال برنامج خبيث أو التعدي على اسم موقع على الإنترنت مما يشكل جرماً يطال حقاً من حقوق الملكية الفكرية.

لقد أصبحت البرامج والأدوات المعلوماتية تُستخدم كوسائل فعّالة لارتكاب الجرائم العادية، فهذه الجرائم لم يتغير مفهومها أو عناصرها الجرمية، كالاحتيال أو الاختلاس أو السرقة أو التخريب أو القدح أو التهديد. إنما أصبحت طرق تنفيذها تجري بوسائل معلوماتية بدل الوسائل التقليدية الشائعة، كأن يتم التهديد عبر رسالة بريد إلكتروني أو يتم الاختلاس عبر التلاعب في النظام المعلوماتي الذي يخزّن تفاصيل عمليات حسابات الزبائن. وقد يكون الضرر وحجم الجريمة عند استخدام وسائل معلوماتية أكبر بكثير من الحالات المعروفة سابقاً. كما يمكن أن تكون الوسائل المعلوماتية، كالبرامج والبيانات المعلوماتية، هي موضوع الجرائم ذاتها، كالتعدي على الأنظمة والبيانات المعلوماتية أو تعديل ومحو هذه البيانات أو اعتراضها. وهذه الطائفة من الجرائم هي جرائم استجدّت بظهور المعلوماتية[6]، ولم تكن معروفة قبل ذلك. وقد أسهم نمو التجارة الإلكترونية والتعاملات الإلكترونية وشيوعها بين أوساط العامة في ازدياد حالات حصول هذه الطائفة الجديدة من الجرائم[7]. وقد وجدت المحاكم صعوبة في تكييف النصوص القانونية العامة الواردة في قانون العقوبات لتجريم الأفعال التي موضوعها أدوات

المعلوماتية. فالنص الجزائي يُفسّر على سبيل الحصر، عملاً بقاعدة "لا جريمة ولا عقوبة بدون نص". وكان لا بد بالتالي من إقرار قوانين جديدة تجرّم الأفعال الواقعة على الأنظمة والبيانات المعلوماتية باعتبارها جرائم حديثة[٨]، وكذلك توسّع نطاق المفاهيم الراسخة للجرائم التقليدية لتشمل حالات استخدام المعلوماتية كوسيلة لتنفيذ الجرائم.

وبفعل الشبكات المعلوماتية وتخطيها للحدود الجغرافية، كشبكة الإنترنت التي لا تخضع لسيادة أي دولة وبالتالي لسيادة أي قانون صادر عن مشترع وطني معيّن، تجاوزت الجرائم المعلوماتية النطاق الوطني، فظهرت مثلاً العصابات التي تتلاعب بالبطاقات المصرفية على الصعيد الدولي وتنقل نشاطها من دولة إلى أخرى حتى لا تنكشف، وظهر المحتالون على شبكة الإنترنت ينتحلون شخصيات معينة عبر سرقة عناصر التعريف العائدة لأشخاص آخرين، وذلك للاستيلاء على الأموال بصورة غير مشروعة.

يتفاقم يوماً بعد يوم وضع جريمة الفضاء السيبراني، حيث بالإضافة إلى الجرائم التي ترتكب فردياً، أصبحت الجريمة السيبرانية منظمة[٩] إلى درجة أنها باتت تعتبر أحد أساليب الحرب الجديدة[١٠] وإحدى وسائل الهجوم الإرهابي[١١] مما دفع وزارة الدفاع الأميركية إلى إصدار بيان اعتبرت فيه أن على الحكومة الأميركية أن تتخذ الإجراءات الكفيلة برد أي اعتداء على أنظمة الحاسوب في إطار اي حرب أو نزاع مستقبلي.

لذلك، وبناءً على الوضع التشريعي القائم، كان من اللازم إيجاد حلول للثغرات في التشريعات السيبرانية لملاحقة الجريمة السيبرانية المتخطية للحدود الوطنية بغية تفعيل مكافحتها، ولتأمين انسجام التشريعات الوطنية معها حتى لا يفلت المجرم من العقاب بعد ارتكاب فعله وينتقل إلى بلد آخر. وبغية اتباع سياسة جنائية مشتركة، وتعزيز التعاون بين الدول، حاولت الجهات الدولية وضع تشريعات نموذجية في هذا المجال. ونذكر خصوصاً اتفاقية بودابست المتعلقة بالجريمة الإلكترونية تاريخ ٢٠٠١/١١/٢٣ والصادرة عن مجلس أوروبا، والتي تشكل نموذجاً جدياً يمكن الاسترشاد به عند إعداد التشريعات الوطنية في هذا المجال. وقد تم الاسترشاد باتفاقية بودابست المتعلقة بالجريمة الإلكترونية وبالقانون الفرنسي رقم ٢٠٠٤/٥٧٥ الصادر بتاريخ ٢٠٠٤/٦/٢١ وبقوانين وطنية مختلفة وبالأعمال الفقهية، في إعداد نصوص الإرشاد الحالي الموجه إلى الدول العربية حول جرائم المعلوماتية والفضاء السيبراني.

لقد تم تقسيم القانون الاسترشادي المُقترح على ثلاثة عشر باباً، تتناول مختلف الجرائم المعلوماتية والعقوبات العائدة لها. وهذه الأبواب هي:

الباب الأول: جرائم التعدي على البيانات المعلوماتية.
الباب الثاني: جرائم التعدي على الأنظمة المعلوماتية.
الباب الثالث: إساءة استعمال الأجهزة أو البرامج المعلوماتية.
الباب الرابع: الجرائم على الأموال.
الباب الخامس: جرائم الاستغلال الجنسي للقاصرين.
الباب السادس: جرائم التعدي على الملكية الفكرية للأعمال الرقمية.
الباب السابع: جرائم البطاقات المصرفية والنقود الإلكترونية.
الباب الثامن: الجرائم التي تمسّ المعلومات الشخصية.
الباب التاسع: جرائم العنصرية والجرائم ضد الإنسانية بوسائل معلوماتية.
الباب العاشر: جرائم المقامرة وترويج المواد المخدرة بوسائل معلوماتية.
الباب الحادي عشر: جرائم المعلوماتية ضد الدولة والسلامة العامة.
الباب الثاني عشر: جرائم تشفير المعلومات.
الباب الثالث عشر: العقوبات.

شروحات حول الإرشاد المتعلق بالجرائم السيبرانية

يتضمن **الباب الأول** المعنون "جرائم التعدي على البيانات المعلوماتية" الجرائم التي يكون موضوعها البيانات المعلوماتية[١٢] أي التي تقع على بيانات معلوماتية. وهي جرم التعرض للبيانات المعلوماتية وجرم اعتراض بيانات معلوماتية. تُعاقب المادة ١ كل من أقدم قصداً بصورة غير مشروعة على تعديل أو إلغاء أو محو أو إفساد أو تدمير البيانات الرقمية. يجوز اشتراط أن الفعل المذكور يجب أن يؤدي إلى إلحاق ضرر لتحقق الجرم . إن الفعل يجب أن يكون قصدياً لتمييزه عن أي فعل عرضي أي عن حصول تعديل البيانات المعلوماتية أو محوها عرضاً. كما أن الفعل يشمل كل أنواع التعرض والتغيير في البيانات المعلوماتية، سواء تم كلياً أم جزئياً. إن التجريم لا يرتبط بوقوع أضرار جسيمة بحق المجني عليه، لكن يمكن إضافة هذا الشرط على شروط التجريم. كما تُعاقب المادة ٢ كل من أقدم قصداً بصورة غير مشروعة على اعتراض بيانات معلوماتية بوسائل تقنية وذلك عند نقلها غير المُتاح للجمهور من أو إلى أو داخل نظام معلوماتي. ويجوز اشتراط أن يتم الفعل بنية جرمية أو بنية الربط مع أنظمة معلوماتية أخرى. إن اعتراض بيانات معلوماتية يعني التقاطها بوسائل تقنية معلوماتية وليس مادية، سواء تم استعمالها فيما بعد أم لا. فمثلاً إن الاستيلاء على الحاسوب الذي خزّنت عليه البيانات المعلوماتية لا يدخل ضمن نطاق هذا الجرم. كما يفترض هذا الفعل أن تكون البيانات المعلوماتية غير مفتوحة لاطلاع الجمهور، أي أن نقلها عبر الشبكات المعلوماتية أو الأنظمة المعلوماتية هو محمي ولا يمكن الدخول إلى هذه البيانات إلا من قبل الأشخاص المفوضين.

يشتمل **الباب الثاني** المعنون "جرائم التعدي على الأنظمة المعلوماتية[١٣]" على جرم الولوج غير المشروع إلى نظام معلوماتي، أو المكوث فيه، وجرم الولوج غير المشروع إلى نظام معلوماتي أو المكوث فيه مع التعرض للبيانات المعلوماتية، وجرم إعاقة عمل نظام معلوماتي[١٤]. تُعاقب المادة ٣ كل من أقدم قصداً على الولوج غير المشروع إلى نظام معلوماتي أو جزء منه أو المكوث غير المشروع فيه. ويجوز اشتراط أن يتم الفعل عن طريق مخالفة تدابير الحماية الجارية على النظام المعلوماتي وبنية الحصول على بيانات رقمية، أو بنيّة أخرى جرمية أو بنيّة جرمية تتعلق بالربط مع أنظمة معلوماتية أخرى. إن مفهوم الولوج إلى نظام معلوماتي يعني الدخول إلى النظام واختراقه[١٥] والوصول إلى ما يحتويه وإمكانية الاطلاع على هذا المحتوى. يُشترط أن يكون الولوج غير مشروع أي أنه قد تم من قبل شخص غير مخول بالولوج، أو من قبلَ شخص مخول ولكن خلافاً للصلاحيات الممنوحة له أو خارج الأوقات المُتاحة له. كما يعني المكوث غير المشروع في نظام معلوماتي، أن الشخص بعد دخوله المشروع إلى النظام قد بقي فيه بعد انتهاء الوقت المخصص له. ويعتبر الفعل جرمياً ولو كان النظام المعلوماتي غير محمي، أو لم يكن القصد الاطلاع على محتوى النظام المعلوماتي من بيانات معلوماتية، إلا أنه يمكن إضافة شرط كون النظام محمياً من ضمن عناصر الجرم أو أن قصد الدخول هو الاطلاع على بيانات معلوماتية. تضيف المادة ٤ كشرط للتجريم قيام الفاعل بتعديل البيانات الرقمية أو البرامج أو إلغائها أو محوها أو إفسادها أو تدميرها أو المساس بعمل النظام المعلوماتي وذلك بعد دخوله غير المشروع إلى النظام المعلوماتي. وبطبيعة الحال، تكون العقوبة المقررة في هذه الحالة للجريمة أشد لكون الضرر هو فعلي وجسيم. في نهاية هذا الباب، تُعاقب المادة ٥ كل من أقدم بنية الغش، وبأي وسيلة، على إعاقة عمل نظام معلوماتي أو على إفساده. إن إعاقة عمل نظام معلوماتي أو إفساده تعني تعطيل وظائف النظام كلياً أو جزئياً، كعدم تمكنه من إتمام عملياته بشكل كلي أو بشكل جزئي أو التأخر في إتمام هذه العمليات أو إتمام العمليات مع الحصول على نتائج خاطئة. ويمكن تصور الحالات الجرمية التالية: تلقيم فيروس لتخريب النظام المعلوماتي[١٦]، وإغراق النظام المعلوماتي بالأوامر أكثر من طاقته، محو البيانات المعلوماتية. تفترض المادة نيّة الغش لدى الفاعل، وبالتالي تُستبعد الحالات العرضية التي تحصل بطريق الخطأ غير المقصود.

يعالج **الباب الثالث** المعنون "إساءة استعمال الأجهزة[١٧] أو البرامج المعلوماتية" جرم إساءة استعمال الأجهزة أو البرامج المعلوماتية. فالمادة ٦ تطال كل من قدّم أو أنتج أو وزّع أو استورد أو صدر أو روّج أو حاز بغرض الاستخدام جهازاً أو برنامجاً معلوماتياً أو أي بيانات معلوماتية معّدة أو كلمات سر أو تراميز دخول، وذلك بغرض اقتراف أي من الجرائم المنصوص عليها سابقاً. تشترط هذه المادة وجود نية جرمية خاصة لدى الفاعل[١٨]، أي وجود نية لديه بالاستعمال لاقتراف أي من الجرائم المعيّنة سابقاً (جرائم الولوج أو التعدي على الأنظمة المعلوماتية والبيانات المعلوماتية.)، وليس فقط قيامه بالإنتاج أو الحيازة أو التوزيع، وذلك لو لم يحصل الاستعمال لاحقاً إذ يكفي وجود النية مسبقاً. وتخرج بالتالي عن نطاق تطبيق هذه المادة حالات استخدام الأدوات المعدّة لاختراق الأنظمة المعلوماتية والتعدي على البيانات المعلوماتية لاختبار سلامة هذه الأنظمة أو لإجراء الأبحاث، ففي هذه الحالة تكون الأهداف مشروعة.

يتضمن **الباب الرابع** المعنون "جرائم التعدي على الأموال والمعاملات" جرم الاحتيال[١٩] أو الغش بوسيلة معلوماتية وجرم التزوير المعلوماتي وجرم الاختلاس أو سرقة أموال بوسيلة معلوماتية[٢٠] وجرم أعمال التسويق والترويج غير المرغوب فيها[٢١] وجرم الاستيلاء على أدوات التعريف والهوية[٢٢] المستخدمة في نظام معلوماتي والاستخدام غير المشروع لها وجرم الاطلاع على معلومات سرية أو حساسة أو إفشائها. تحدد المادة ٧ جرم الاحتيال أو الغش بوسيلة معلوماتية، فهو فعل من أقدم عن قصد بصورة غير مشروعة على إلحاق ضرر مالي بالغير عن طريق: إدخال أو تبديل أو محو أو تدمير بيانات معلوماتية أو بكل شكل من أشكال التعدي على عمل نظام معلوماتي، وذلك بنيّة الغش للحصول دون حق على منفعة مادية لنفسه أو للغير. فهذا النص لا يخرج عن المفهوم التقليدي لجرم الاحتيال المعروف، لكنه يحدد الوسائل الاحتيالية المستخدمة للاستيلاء على أموال الغير أو للحصول على المنفعة غير المشروعة بالتعرض للبيانات المعلوماتية أو الأنظمة المعلوماتية. أي أن البيانات المعلوماتية والأنظمة المعلوماتية تكون هي الوسائل المستخدمة لارتكاب الجرم ولا تكون موضوع الجرم. تعرّف المادة ٨ جرم التزوير المعلوماتي، فهو فعل كل من أقدم عن قصد وبصورة غير مشروعة على إدخال أو تبديل أو محو أو تدمير بيانات معلوماتية، نتج عنها بيانات غير صحيحة بقصد استخدامها أو التعويل عليها في أغراض قانونية كما لو كانت صحيحة، بصرف النظر عما إذا كانت هذه البيانات مقروءة ومفهومة بشكل مباشر من عدمه. فموضوع التزوير هنا هو البيانات المعلوماتية وليس المخطوطات الورقية، إنما القصد يبقى ذاته وهو التحوير المتعمد للحقائق لاستعمالها في نطاق القانون. فمفهوم التزوير التقليدي يبقى هو نفسه إنما ينصب هنا على البيانات المعلوماتية. ولا يتطلب تحقق الجرم كون البيانات المعلوماتية تفهم مباشرةً من قبل الإنسان ويكفي بالتالي إمكانية فك رموزها واستعراضها بشكل مفهوم للإنسان عبر الاستعانة بأجهزة حواسب. وجرم التزوير المعلوماتي ينطبق على فعل كل من أقدم عن قصد على استعمال البيانات المعلوماتية غير الصحيحة المذكورة في الفقرة الأولى. تُعاقب المادة ٩ على اختلاس الأموال أو سرقتها باستعمال وسيلة معلوماتية. ويُشترط في هذه الحالة أن تُستعمل الوسيلة المعلوماتية لاختلاس المال أو سرقته، لا لغرض آخر. ويبقى تعريف جرم السرقة والاختلاس منطبقاً على ذلك المعروف في قانون العقوبات العام. تعرّف المادة ١٠ جرم أعمال التسويق والترويج غير المرغوب بها[٢٣] بأنه فعل كل من أقدم على إرسال رسائل ترويج أو تسويق غير مرغوب بها دون تمكين المُرسل إليهم من إيقاف ورود هذه الرسائل، في حال رغبوا بذلك، ومع عدم تحمل أي نفقات إضافية. فقد أصبح إرسال رسائل الترويج للمنتجات والخدمات من قبل التجار للمستهلكين وللمتعاملين شائعاً جداً إلى درجة أصبح مرهقاً لهؤلاء المتعاملين وللأنظمة المعلوماتية بذاتها، ويقتضي بالتالي إتاحة المجال أمام كل متعامل لإيقاف إرسال هذه الرسائل له، وذلك تحت طائلة تجريم الفعل[٢٤]. تُعرّف المادة ١١ فعل الاستيلاء على أدوات التعريف والهوية العائدة لشخص آخر، والمستخدمة في نظام معلوماتي، والاستخدام غير المشروع لها[٢٥]. فقد أضحت هذه الأفعال من النشاطات الجرمية التي تُمارس على نطاق واسع على شبكة الإنترنت بانتحال هوية أو صفة شخص آخر توسلاً للاحتيال أو لسرقة الأموال. ففي التعامل عن قرب، يستطيع الشخص التعرف على الشخص الآخر من خلال ملامحه وصوته وشكله. أما في التعامل عن بعد، فالتعريف عن الشخص يتم من خلال أدوات تعريف تقنية وبرامج معلوماتية قد تكون عرضة للتلاعب، مما يحتّم توفير الحمأي القانونية الرادعة لمثل هذه التصرّفات. في نهأي هذا الباب، تعالج المادة ١٢ فعل الاطلاع بوسائل معلوماتية عن قصد ودون سبب مشروع على معلومات سرية أو حساسة أو على إفشاء مثل هذه المعلومات بوسائل معلوماتية. ويجوز اشتراط أن يؤدي الفعل إلى إلحاق الضرر بالغير أو بصاحب العلاقة. فالسرية على الشبكات والأنظمة المعلوماتية، حتى المحميّة منها تقنياً، هي دوماً عرضة للانتهاك من قبل مرتكبين يملكون مؤهلات تقنية متقدمة. ويجب بالتالي تجريم هذه الأفعال لردع هؤلاء المنتهكين. وإن تطبيق هذه المادة يرتبط بطبيعة المعلومات، السرية أو الحساسة، كما يرتبط بوسيلة الإفشاء أو الاطلاع التي يجب أن تكون معلوماتية.

يتناول **الباب الخامس** المعنون "جرائم الاستغلال الجنسي للقاصرين" الأفعال التي تتعلق باستغلال القاصرين في أعمال جنسية[٢٦]. وتعطي المادة ١٣ تعريفاً للمواد الإباحية[٢٧]، بمفهوم هذا القانون، معتبرةً أنها الرسوم أو الصور أو الكتابات أو الأفلام أو الإشارات أو أي أعمال إباحية يشارك فيها قاصرون أو تتعلق باستغلال القاصرين في المواد الإباحية، والتي تُظهر للعيان: قاصراً يقوم بفعل جنسي صريح، شخصاً يبدو كقاصر يقوم بفعل جنسي صريح، صوراً واقعية أو مصطنعة بالمحاكاة تظهر قاصراً يقوم بفعل جنسي صريح. هذا التعريف هو واسع يشمل كل الأشكال الممكن تصورها لاستغلال القاصرين جنسياً، بحيث تمنع تفلت المنتهكين من العقوبة. ويحتمل هذا التعريف قيام قاصر فعلياً بالمشاركة في أعمال إباحية، كما يحتمل قيام الراشد الذي له مظهر القاصر بها، أو حتى الصور المصنّعة بالمحاكاة دون اشتراك فعلي لإنسان ما فيها[٢٨]. كما تعرّف المادة ١٣ القاصر بأنه كل من لم يتم الثامنة عشرة من عمره[٢٩]. ويجوز لدولة عضو أن

تخفضّ السن إلى حدود أدنى، لا تقل عن السادسة عشرة. تجرّم المادة ١٤ فعل إنتاج مواد إباحية لقاصرين عن قصد وبصورة غير مشروعة بهدف بثها بواسطة نظام معلوماتي. فالإنتاج لوحده دون قصد البث غير معاقب عليه، ولا يدخل ضمن نطاق هذه المادة، باعتبار أن ضرر المواد الإباحية لا يتحقق إلا ببثها على نطاق واسع. تتناول المادة ١٥ جرم عرض أو توفير أو تقديم بواسطة نظام معلوماتي عن قصد وبصورة غير مشروعة. ويكفي في هذه الحالة قيام المرتكب بعرض المواد الإباحية ولو لم يقم هو نفسه بإنتاجها. تجرّم المادة ١٦ فعل توزيع أو بث أو نقل مواد إباحية قصداً بصورة غير مشروعة لقاصرين بواسطة نظام معلوماتي. فالغأي من هذه المادة المساهمة في منع وضع المواد الإباحية قيد اطلاع الجمهور، الأمر الذي يؤدي إلى انتهاك الآداب العامة وخدش الشعور العام للمواطنين. وتختلف هذه المادة عن المادة التي تسبقها بأن نطاق الأفعال المذكورة فيها أوسع بحيث تطال الجمهور أو فئات كبيرة منه، بخلاف المادة الأولى التي يمكن أن تطال أفعالها شخصاً واحداً فقط. هذا الأمر يحتم أن تكون عقوبة هذه المادة أشد من عقوبة المادة السابقة. تتعلق المادة ١٧ بجرم التزود أو تزويد الغير قصداً بمواد إباحية لقاصرين بواسطة نظام معلوماتي. هذه المادة تطبق على الأفعال الفردية، حيث يقوم شخص بالاستحصال عبر نظام معلوماتي على مواد إباحية لنفسه أو لغيره، ولا يتعدى ذلك إلى الجمهور. إن عقوبة هذا الجرم يجب أن تكون متناسبة مع الضرر المحدود الناتج عنها. تتطرق المادة ١٨ إلى جرم حيازة مواد إباحية لقاصرين على وسيطة إلكترونية أو نظام معلوماتي قصداً أو بصورة غير مشروعة. إن قيام شخص بحيازة هذه المواد الإباحية عن قصد يدل عن اتجاه منحرف لديه، ويبرر معاقبته. ولكن لا تدخل الحيازة العرضية أو المؤقتة غير المقصودة، كأن يقوم شخص بسحب صور عن الإنترنت، ثم يكتشف لاحقاً أنها مواد إباحية لقاصرين بعد الاطلاع عليها، ويقوم بالتالي بمحوها عن حاسوبه الشخصي. تجرّم المادة ١٩ فعل تحريض أو تشجيع القاصرين على القيام بأنشطة جنسية غير مشروعة أو إعدادهم لذلك بوسيلة معلوماتية وذلك سواء مجاناً أو لقاء عوض. كأن يستدرج الجاني أحد القاصرين عبر منتديات الحوار على الإنترنت أو عبر مخاطبته برسائل بريدية إلكترونية، ويقنعه بتنفيذ أعمال جنسية واعداً إياه بمكافأة أو غيرها. هذا الفعل يدل على وجود تفكير خلقي متدنٍ ومتمادٍ جرمياً لدى الفاعل، ويعمل على إفساد المجتمع، مما يحتم تشديد عقوبته. تتناول المادة ٢٠ جرم التحرش الجنسي بالقاصرين على شبكة الإنترنت أو بأي وسيلة معلوماتية أخرى، وذلك من أجل إشباع الرغبة الجنسية أو من أجل إقناعهم بالقيام بأنشطة جنسية سواء مجاناً أو بعوض. تختلف هذه المادة عن سابقتها في أن الفعل الجنسي الذي يجري إقناع القاصر بتنفيذه يتم في الحالة الأولى مع الغير إلا أنه في الحالة الثانية يتم مع الجاني.

يتضمن **الباب السادس** المعنون "جرائم التعدي على الملكية الفكرية للأعمال الرقمية[٣٠]" الجرائم التالية: جرم وضع اسم مختلس على عمل، وجرم تقليد إمضاء المؤلف أو ختمه، وجرم تقليد عمل رقمي أو قرصنة البرمجيات[٣١]، وجرم بيع أو عرض عمل مقلّد أو وضعه في التداول، وجرم الاعتداء على أي حق من حقوق المؤلف أو الحقوق المجاورة. ومن المتعارف عليه أن الأعمال الرقمية هي محمية بموجب حق المؤلف على الأعمال الفكرية إذا كانت تلبي شروط الابتكار. تجرّم المادة ٢١ فعل التعدي الحاصل على حق المؤلف بِنِسبَة العمل إلى الفاعل عبر وضع اسمه عليه، فتعاقب بالتالي كل من أقدم بقصد الغش على وضع اسم مختلس على عمل أدبي رقمي أو كلّف الغير بذلك. تتناول المادة ٢٢ جرم تقليد إمضاء المؤلف أو ختمه بقصد الغش. وفي ذلك أيضاً حمأي لحق المؤلف بِنِسبَة العمل إليه عبر تمكينه من وضع إمضائه أو ختمه على عمله، مما يثبت أبوته لهذا العمل. تتعلق المادة ٢٣ بجرم تقليد عمل أدبي وفني رقمي أو قرصنة البرمجيات، فهي تحدّد أعمال التقليد الواقعة على العمل الرقمي وكذلك قرصنة البرمجيات. ويشمل التقليد نسخ أو إعادة إنتاج أو طبع أو تصوير العمل الرقمي أو نقله إلى الغير وذلك دون حق. تجرم المادة ٢٤ الاعتداء على الحقوق المادية لصاحب حق المؤلف، فهي تعاقب كل من أقدم على بيع أو عرض للبيع أو وضع بالتداول أو قدّم قصداً عملاً أدبياً فنيا رقمياً مقلداً. تتوسع المادة ٢٥ في الحمأي القانونية الجزائية حتى لا يفلت أي فعل اعتداء على العمل الرقمي من العقاب، وتعاقب كل فعل اعتداء قصداً على أي حق من حقوق المؤلف أو الحقوق المجاورة المتعلقة بالأعمال الرقمية[٣٢].

يتناول **الباب السابع** المعنون "جرائم البطاقات المصرفية والنقود الإلكترونية"[٣٣] الأفعال الجرمية الواقعة على البطاقات المصرفية[٣٤] والنقود الإلكترونية. فالمادة ٢٦ تجرّم فعل تقليد بطاقة مصرفية عن قصد بصورة غير مشروعة. ويعني التقليد صنع أو إنتاج بطاقة مصرفية مزيفة تستعمل للوصول إلى حسابات الغير بصورة غير مشروعة. وتتعلق المادة ٢٧ بجرم استعمال بطاقة مصرفية مقلّدة عن قصد مع العلم بحقيقة البطاقة. فالضرر الحقيقي اللاحق بمصالح الآخرين بالاستيلاء على أموالهم يتحقق فعلياً باستعمال البطاقة المصرفية المزيفة، ولذلك جاءت هذه المادة لتوفر الحمأي القانونية المطلوبة في هذا المجال. ولا يهم طريقة حصول الجاني على البطاقة المصرفية المزيفة، سواء

صنعها بنفسه أو اشتراها أو استولى عليها أو استعارها. كما لا تأثير لنتيجة الاستعمال أي أن الجرم يعتبر واقعاً سواء أدى استعمال البطاقة المزيفة إلى الاستيلاء على أموال أو لا لسبب لا يعود للجاني، كأن يقوم المجرم بمحاولة سحب أموال عبر البطاقة فيتبيّن أن الحساب المجرى منه السحب فارغ. كما حددت المادة ٢٧ في فقرتها الثانية حالات تجريم استعمال أرقام البطاقات المصرفية المسروقة أو الاستيلاء عليها عن قصد. تجرّم المادة ٢٨ الطرف الآخر الذي يُشارك في الجرم ولو بصورة غير مباشرة عبر قبول الإيفاء ببطاقة مصرفية مقلّدة مع علمه بحقيقتها. فمن شأن التغاضي عن تجريم هذا الفعل تشجيع الجاني على التمادي في استعمال البطاقات المصرفية المزورة، ولو تنبه الآخرون إلى وجوب التدقيق في حقيقة البطاقات المصرفية وامتنعوا عن قبول الإيفاء بواسطة بطاقات مقلدة لساهم هذا الأمر في انحصار جرائم تزييف البطاقات واستعمالها. في نهاية هذا الباب، تجرّم المادة ٢٩ كل من أقدم عن قصد بصورة غير مشروعة على تزوير نقود إلكترونية، لما لذلك من إخلال بالاقتصاد الوطني وتأثير سلبي على العمليات المصرفية.

يتضمن **الباب الثامن** المعنون "الجرائم التي تمسّ المعلومات الشخصية" الأفعال الجرمية التي تتعلق بمعالجة البيانات ذات الطابع الشخصي. تجرّم المادة ٣٠ معالجة المعلومات ذات الطابع الشخصي عن قصد وبدون حيازة تصريح أو ترخيص مسبق يتيح القيام بالمعالجة، إذ إن معالجة المعلومات ذات الطابع الشخصي تخضع لقواعد خاصة لناحية ضرورة الحصول على ترخيص من المراجع الرسمية المختصة أو تقديم تصريح لها حول المعالجة وخصائصها، ولاسيما إذا كانت المعالجة تهدد الحياة الخاصة أو الحريات الشخصية. كما تتضمن هذه القواعد أيضاً قواعد تتعلق بجمع المعلومات وموجب الإعلام وأصول شكلية إجرائية وقواعد تضمن حق الشخص المعني بالاطلاع على المعلومات المُعالجة الخاصة به وطلب إجراء التصحيح اللازم بشأنها. وهذه القواعد هي آمرة ويقتضي فرض احترامها عبر تجريم أي مخالفة لأحكامها لردع المخالفين. ويقتضي بالتالي، وفقاً للمادة ٣١، تجريم معالجة المعلومات ذات الطابع الشخصي التي تتم دون احترام القواعد القانونية المقررة لذلك وفق القانون. كما يجب على المسؤول عن المعالجة المحافظة على سرية معلومات جمعها وهو بصدد معالجتها، حفاظاً على خصوصية الأفراد وحياتهم الخاصة. لذلك تجرّم المادة ٣٢ كل من أقدم، عن قصد أو عن إهمال، على إفشاء معلومات ذات الطابع الشخصي لأشخاص لا يحق لهم الاطلاع عليها. وقد أشرنا إلى حق الشخص المعني بالاطلاع وطلب التصحيح بخصوص المعلومات المُعالجة المتعلقة به، ولا بد من ضمان تقيد المسؤول عن المعالجة بموجباته لهذه الجهة، عبر فرض عقوبات رادعة على أي مخالفة. وتجرّم المادة ٣٣ لذلك عدم الاستجابة في مهلة قصيرة لطلب الشخص المعني بالاطلاع على المعلومات ذات طابع شخصي المتعلقة به أو بتصحيحها.

يتناول **الباب التاسع** المعنون "جرائم العنصرية والجرائم ضد الإنسانية بوسائل معلوماتية"[٣٥] الجرائم التالية: جرم نشر وتوزيع المعلومات العنصرية بوسائل معلوماتية، وجرم تهديد أشخاص أو التعدي عليهم بسبب انتمائهم العرقي أو المذهبي أو لونهم وذلك بوسائل معلوماتية، وجرم توزيع معلومات بوسيلة إلكترونية من شأنها إنكار أو تشويه أو تبرير أعمال إبادة جماعية أو جرائم ضد الإنسانية[٣٦]، وجرم المساعدة أو التحريض بوسيلة إلكترونية على ارتكاب جرائم ضد الإنسانية. تجرّم المادة ٣٤ فعل كل من أقدم قصداً على نشر وتوزيع معلومات تثير النعرات العنصرية وتهدف إلى التمييز العنصري بحق أشخاص معينين، وذلك بواسطة شبكة الإنترنت أو غيرها من الوسائل المعلوماتية. وتشترط المادة ٣٤ أن تكون وسيلة النشر أو وسيلة إيصال المعلومات إلى الغير وسيلة معلوماتية، وبالتالي تُستبعد الوسائل الورقية التقليدية من نطاق تطبيق هذه المادة كما باقي المواد اللاحقة. تجرّم المادة ٣٥ جرم تهديد أشخاص أو تحقيرهم أو التعدي عليهم بسبب انتمائهم العرقي أو المذهبي أو لونهم وذلك بواسطة شبكة الإنترنت أو بأي وسيلة معلوماتية أخرى. ففعل التحقير والتهديد هو ذاته المعرّف في نطاق قانون العقوبات العام، ولكن وسيلة تحقق الفعل قد اختلفت في هذه الحالة، فهي وسيلة معلوماتية. كما تحدّد المادة ٣٦ فعل توزيع معلومات عن قصد بوسيلة معلوماتية من شأنها إنكار أو تشويه أو تبرير أعمال إبادة جماعية أو جرائم ضد الإنسانية. ويقتضي تشديد العقوبات المطبّقة على جرائم هذا الباب بالنظر لخطورتها وطبيعتها وذهنية الفاعل المتطرفة. وأخيراً، وفي هذا الباب ذاته، تعتبر المادة ٣٧ أفعال المساعدة أو التحريض عن قصد بوسيلة معلوماتية على ارتكاب جرائم ضد الإنسانية بمثابة جرم. فيمكن أن يتم التحريض عبر إرسال رسائل بريد إلكتروني أو عبر منتديات الحوار.

يتضمن **الباب العاشر** المعنون "جرائم المقامرة وترويج المواد المخدرة بوسائل معلوماتية"[٣٧] الجرائم التالية[٣٨]: جرم تملك وإدارة مشروع مقامرة على الإنترنت، وجرم تسهيل وتشجيع مشروع مقامرة على الإنترنت، وجرم ترويج الكحول للقاصرين على الإنترنت، وجرم ترويج المواد المخدرة على الإنترنت. تجرّم المادة ٣٨ فعل كل من تملك أو أدار مشروع مقامرة أو عرض ألعاب مقامرة على شبكة الإنترنت أو بأي وسيلة معلوماتية

أخرى. في بعض الدول، تكون ألعاب المقامرة مشروعة في حال الترخيص، ويقتضي بالتالي مراعاة هذا الأمر. يُفترض بألعاب المقامرة وفق هذه المادة أن تكون مُتاحة على شبكة الإنترنت أو بوسيلة معلوماتية، وتُستبعد بالتالي ألعاب المقامرة التقليدية. وتتضمن هذه المادة ثلاثة أفعال جرمية: تملك مشروع مقامرة، إدارة مشروع وإن كان عائداً لشخص آخر، عرض ألعاب مقامرة ولو بصورة عرضية وفردية وخارج إطار مشروع مستمر. تُجرّم المادة ٣٩ فعل تسهيل وتشجيع إنشاء أو إدارة أو ترويج مشروع مقامرة على شبكة الإنترنت أو بوسيلة معلوماتية. يمكن أن تكون أفعال التسهيل أو التشجيع بجميع الطرق المتاحة، كالوعد بجلب زبائن أو المساهمة في تصميم موقع على شبكة الإنترنت. ولكن مشروع المقامرة يجب أن يكون مُتاحاً للجمهور بواسطة وسيلة معلوماتية. تتطرق المادة ٤٠ إلى جرم ترويج الكحول للقاصرين على الإنترنت، فيعد جرماً فعل ترويج الكحول مع استهداف القاصرين على شبكة الإنترنت أو باستعمال أي وسيلة معلوماتية أخرى. فمن شروط هذا الجرم الخاصة: ترويج الكحول من خلال وسيلة معلوماتية كشبكة الإنترنت، واستهداف القاصرين بشكل مباشر أي التوجه إليهم بشكل خاص أو التوجه إلى كل الفئات العمرية دون تخصيص ودون استثناء القاصرين وتنبيههم. تجرّم المادة ٤١ فعل ترويج أو بيع أو عرض طرق إنتاج المواد المخدرة على شبكة الإنترنت أو باستعمال أي وسيلة معلوماتية أخرى. إن ماهية المواد المخدرة هي معروفة ومحددة وفق القوانين الوطنية. إنما جديد هذه المادة هو الوسيلة التي يتم الترويج بها ألا وهي وسيلة معلوماتية أو شبكة الإنترنت.

يتناول **الباب الحادي عشر** المعنون "جرائم المعلوماتية ضد الدولة والسلامة العامة" الأفعال الجرمية الناشئة عن المعلوماتية التي تطال الدولة وسلامتها وأمنها واستقرارها ونظامها القانوني. وهذه الجرائم على قدر من الأهمية لتأثيرها على الدولة وانتظام عملها وبالتالي على المواطنين كافة، مما يقتضي معه تشديد العقوبات المقررة لهذه الجرائم. فالمادة ٤٢ تجرّم تعطيل الأعمال الحكومية أو أعمال السلطة العامة باستعمال أي وسيلة معلوماتية أو إنتاج أو توزيع أو حيازة برامج معدة لهذا الاستعمال. فالأعمال الحكومية وأعمال السلطة العامة تتعلق بإدارة الدولة وممارسة أجهزتها لمهامها وفق السلطات الممنوحة لها بموجب القوانين المرعية الإجراء. تجرّم المادة ٤٣ فعل كل من امتنع عن قصد أو أبلغ عن قصد بشكل خاطئ عن جرائم المعلوماتية. فجريمة الإبلاغ لا تتعلق بجميع الجرائم بل فقط بنوع خاص منها هو جرائم المعلوماتية. وهذه الجريمة هي جريمة قصدية، أي يجب أن يكون الجاني قد علم بحصول الجريمة المعلوماتية، وتمنع عن الإبلاغ عنها أو أبلغ عنها بشكل خاطئ ومضلّل لتجهيل الفاعل أو لاتهام آخرين أو لإخفاء الأدلة. تجرّم المادة ٤٤ فعل من أقدم على الاطلاع أو على الحصول على معلومات سرية تخص الدولة، وذلك من خلال شبكة الإنترنت أو باستعمال أي وسيلة معلوماتية أخرى. إن حمأي المعلومات السرية العائدة للدولة يجب أن تكون فعّالة، فتسريبها يمكن أن يمسّ بانتظام الدولة وكيانها وأمنها وسلامتها. وتشترط هذه المادة استعمال وسيلة معلوماتية للوصول إلى المعلومات السرية وليس أي وسيلة أخرى. في نهأي هذا الباب، تجرّم المادة ٤٥ فعل العبث بالأدلة القضائية المعلوماتية أو إتلافها أو تخبئتها أو التعديل فيها أو محوها. لقد أصبحت المعلوماتية تستخدم كوسيلة مساعدة لارتكاب أي جريمة، وقد تكون موضوع الجريمة نفسها. لذلك، فضبط الجرائم المعلوماتية وكذلك الجرائم العادية وإثباتها يتطلب جمع أدلة معلوماتية عليها وخصوصاً الحفاظ عليها من العبث والإتلاف والتخبئة أو التعديل فيها أو محوها لتفادي الإدانة[٣٩]. تجرّم المادة ٤٦ فعل بث أو إذاعة أو نشر بيانات أو معلومات تهدد الأمن والسلامة العامة في الدولة أو أي دولة أخرى، وذلك من خلال شبكة الإنترنت أو باستعمال أي وسيلة معلوماتية أخرى. فقد أصبحت الشبكات والوسائل المعلوماتية تستعمل كطرق فعّالة لنشر المعلومات بالنظر لقدرتها على تخطي الحواجز والأبعاد الجغرافية والوصول إلى كل مكتب وبيت، وإن جسامة الضرر الناجم عنها يفوق بأشواط ذلك العائد لأي وسيلة أخرى عادية، كالرسائل أو الخطابات الورقية أو الخطب العلنية. تجرّم المادة ٤٧ فعل كل من ارتكب أعمالاً إرهابية أو ساهم فيها أو حرّض عليها باستعمال شبكة الإنترنت[٤٠] أو أي وسيلة معلوماتية أخرى. فالأعمال الإرهابية[٤١] لا تقتصر على التفجيرات أو أعمال القتل الجماعي أو تعطيل مصالح الدولة بل أصبحت تطال الأنظمة المعلوماتية التي تتحكم بمختلف قطاعات الخدمات الحديثة المقدمة للمواطنين، كقطاع النقل الجوي أو المصارف أو الاتصالات. فتعطيل النظام المعلوماتي المعتمد لتنظيم سير الطائرات قد يؤدي إلى سقوطها. وإن تخريب هذه القطاعات من خلال اختراق الأنظمة المعلوماتية يشكّل بطبيعة الحال يشكل عملاً إرهابياً كونه يطال المصالح العليا للدولة والسلامة العامة. أخيراً، يعدّ جرماً وفق المادة ٤٨ فعل كل من أقدم على تحريض شخص آخر على القتل باستعمال شبكة الإنترنت أو أي وسيلة معلوماتية أخرى. فقد يتم ذلك من خلال توجيه رسائل بريد إلكتروني إلى القاتل أو صور أو أفلام مركبة تستفزّه وتحرضه على القتل.

يتطرق **الباب الثاني عشر** المعنون "جرائم تشفير المعلومات" إلى الأفعال الجرمية الناشئة عن التشفير[٤٢]. إن التشفير هو كل عمل يرمي إلى تحويل معلومات أو إشارات

واضحة، عبر اتفاقات سرية، إلى معلومات أو إشارات غامضة للغير، أو إلى إجراء العملية المعاكسة عبر وسائل مادية أو معلوماتية مخصّصة لهذا الغرض. ويستخدم التشفير لأغراض السرية عند نقل المعلومات أو تخزينها. فالمعلومات المشفرة تكون غير قابلة للفهم من قبل الغير إلا بعد فك التشفير. كذلك يُستخدم التشفير لتوثيق المعلومات وللمصادقة عليها ولوظيفة التوقيع الإلكتروني. ويكون بالتالي للتشفير وجهان للاستخدامات: استخدامات مدنية واستخدامات عسكرية. لذلك تحرص جميع الدول على فرض مراقبة قانونية على التشفير لمنع إساءة استعماله. وتقرن هذه المراقبة بعقوبات جزائية رادعة. تجرّم المادة ٤٩ فعل تسويق أو توزيع أو تصدير أو استيراد وسائل تشفير دون حيازة ترخيص أو تصريح من قبل المراجع الرسمية المختصة في الدولة. فأعمال التسويق أو التوزيع أو الاستيراد أو التصدير تجري على نطاق واسع، وفي معظم الأحيان من قبل تجار أو من قبل مؤسسات متخصصة. ويفترض أن تخضع للترخيص أو لموجب تقديم تصريح للمراجع المختصة في الدولة للتمكن من إخضاعها للرقابة مخافة تحول استخدام وسائل التشفير لارتكاب الجرائم أو لإخفاء معالمها أو لأعمال عسكرية عدوانية كالتجسس. تجرّم المادة ٥٠ فعل تقديم وسائل تشفير تؤمن السرية دون حيازة تصريح أو ترخيص من قبل الجهات الرسمية المختصة في الدولة. فهذا الفعل قد يتم لمرة واحدة فقط ومن قبل شخص غير متخصص أيضاً، إلا أن خطورته تنبع من استخدام التشفير لتأمين السرية، وقد يكون ذلك لأعمال غير شرعية كالتجسس أو التواصل بين الجماعات الإرهابية أو الإجرامية. تجرّم المادة ٥١ فعل كل من أقدم على بيع أو تسويق أو تأجير وسائل تشفير ممنوعة. فقد تحظّر المراجع الرسمية المختصة في الدولة بعض وسائل التشفير لاعتبارات متنوعة: عدم إمكانية مراقبة استخداماتها، عدم تعاون المصنّعين مع أجهزة الدولة، عدم موثوقية هذه الوسائل وإمكانية اختراقها. ولا بد من فرض عقوبات جزائية رادعة لضمان فعالية الحظر المطبّق.

يتناول **الباب الثالث عشر**[٤٣] العقوبات العائدة للجرائم المعددة في هذا الإرشاد. وتنص المادة ٥٢ على أن كل من يقترف أياً من الجرائم المحددة في هذا الإرشاد يتعرض لعقوبة السجن لفترة تحددها الدولة المعنية والغرامة أو بإحدى هاتين العقوبتين. ويُترك للدولة المعنية أمر تقدير مدة عقوبة السجن وقيمة الغرامة بحديها الأدنى والأعلى. أما المادة ٥٣ فتتعلق بمصادرة الأجهزة التي استخدمت في الجريمة. وتتعلق المادة ٥٤ بحالات تخفيف العقوبة أو تشديدها مثلاً في حال التكرار.

أما **الباب الرابع عشر**، فيتناول إنشاء هيئة وطنية قومية لمكافحة الجرائم المعلوماتية. فقد نصت المادة ٥٥ على أن تحرص الدول الأعضاء على إنشاء وحدة متخصصة في الأجهزة الأمنية التابعة للقضاء والموكلة بالتحقيقات القضائية، وتتولى أعمال التحقيق في الجرائم المعلوماتية ورصدها تحت إشراف القضاء. وتتألف هذه الوحدة من عناصر فنية متخصصة ذات كفاءة في مجال المعلوماتية والاتصالات. كما نصت المادة ٥٦ على أن تحرص الدول الأعضاء على التعاون فيما بينها في مجال التحقيقات القضائية المتعلقة بالجرائم المعلوماتية.

هوامش

١ – Internet وIntranet والشبكات الخاصة ببعض الأجهزة التابعة لمؤسسة أو منظومة واحدة مثل الشبكة التي تربط بين أجهزة حاسوب ضمن إدارة رسمية أو وزارة.

٢– *Actus rea*، تعبير لاتيني يعني الفعل الجرمي.

٣– *Means rea* ، تعبير لاتيني يعني الفكر الإجرامي أي نية ارتكاب عمل غير قانوني بمعرفة وقصد المرتكب. النص اللاتيني هو *actus non facit reum nisi mens sit rea* وترجمتها للعربية هي: لا يشكل الفعل جرماً ما لم يكن فاعله يقصد إحداث الجرم.

4- Virus/Malware. Crime on the Net,
http://rogerdarlington.me.uk/crimeonthenet.html#Hacking

Viruses, in the broadest sense, come in three forms:
- *Virus*: This is a code that attaches itself to a program in a computer and then reproduces itself. It can erase files or lock up a system.
- *Worm*: This is similar to a virus but does not attach itself to files or programs in a computer. This leaves it free to spread through a network on its own.

- *Trojan horse*: This is a program that performs malicious actions while pretending to do something else. It is similar to a virus but does not try to reproduce itself.

٥ – أمثلة على جرائم الانترنت:
http://www.lawoflibya.com/forum/showthread.php?t=3624
تشير مجلة لوس انجيلوس تايمز في عددها الصادر في ٢٢ مارس عام ٢٠٠٢ إلى أن خسارة الشركات الإمريكية وحدها من جراء الممارسات التي تتعرض لها و التي تندرج تحت بند الجريمة الإلكترونية تقدّر بحوالي ٠١ مليار دولار سنويا× و للتأكيد على جانب قد تغفله الكثير من مؤسسات الأعمال فان نسبة ٢٦٪ من تلك الجرائم تحدث من خارج المؤسسة و عن طريق شبكة الانترنت بينما تنتج النسبة الباقية (٨٣ ٪) من تلك الخسائر عن ممارسات تحدث من داخل المؤسسات ذاتها.

مثال آخر حديث قد لا يتوقع أحد كم الخسائر الناجمة عنه وهو تلك الأعطال و الخسائر في البرامج والتطبيقات والملفات ونظم العمل الآلية وسرعة وكفاءة شبكات الاتصال والذي ينجم عن التعرض للفيروسات والديدان مثل ذلك الهجوم الأخير والذي تعرضت له الحواسيب المتصلة بشبكة الانترنت في اغلب دول العالم من خلال فيروس يدعى (WS32.SOBIG) والذي أصاب تلك الأجهزة من خلال رسائل البريد الالكتروني بصورة ذكية للغاية حيث كان ذلك الفيروس يتخفي في الوثيقة الملحقة بالبريد الالكتروني (Attachment File) في صورة ملف ذي اسم براق و عند محاولة فتح ذلك الملف فان الفيروس ينشط ويصيب جهاز الحاسب و يبدأ في إرسال المئات من رسائل البريد الالكتروني من ذلك الجهاز المصاب مستخدما كل أسماء حسابات البريد الالكتروني المخزنة عليه. الأمر الذي أدى إلى إصابة عدد هائل من الحواسب الشخصية للأفراد والشركات وملء خوادم البريد الالكتروني بتلك الرسائل. مثال على ذلك إصابة خوادم البريد الالكتروني لشركة أميركا أون لاين بما يقارب ال ٠٢ مليون رسالة ملوثة وأدى ذلك أيضا إلى بطء شبكات وخطوط الاتصال بصورة كبيرة و أحيانا بالشلل التام مما أدى إلى تعطّل الكثير من الأعمال و تلف العديد من الملفات الهامة على تلك الحواسب. وقد قدرت الخسائر الناجمة عن ذلك الفيروس بما يقارب ال ٠٥ مليون دولار أمريكي في داخل الولايات المتحدة الامريكية وحدها.

6- Current and ongoing Internet trends and schemes identified by the Internet Crime Complaint Center along with its description, http://www.ic3.gov/crimeschemes.aspx

Auction Fraud, Counterfeit Cashier's Check, Credit Card Fraud, Debt Elimination, Parcel Courier Email Scheme, Employment/ Business Opportunities, Escrow Services Fraud, Identity Theft, Internet Extortion, Investment Fraud, Lotteries, Nigerian Letter or "419", Phishing/Spoofing, Ponzi/Pyramid, Reshipping, Spam, Third Party Receiver of Funds.

7- Cyber Crime Statistics from the 2006 Internet Crime Report, http://www.computer-forensics-recruiter.com/home/cyber_crime_statistics.html

- In 2006, the Internet Crime Complaint Center received and processed over 200,000 complaints.
- More than 86,000 of these complaints were processed and referred to various local, state, and federal law enforcement agencies.
- Most of these were consumers and persons filing as private persons.
- Total alleged dollar losses were more than $194 million.
- Email and websites were the two primary mechanisms for fraud.
- Although the total number of complaints decreased by approximately 7,000 complaints from 2005, the total dollar losses increased by $15 million.
- The top frauds reported were auction fraud, non-delivery of items, check fraud, and credit card fraud.
- Top contact mechanisms for perpetrators to victims were email (74%), web page (36%), and phone (18%) (there was some overlap).

The Internet Crime Complaint Center is a clearinghouse for online economic crime complaints. It is maintained by the National White Collar Crime Center and the Federal Bureau of Investigations. To review the results of the study, visit the National White Collar Crime Center's site.

Cyber Crime Statistics from the 12th Annual Computer Crime and Security Survey:

- Between 2006 and 2007 there was a net increase in IT budget spent on security.
- Significantly, however, the percentage of IT budget spent on security awareness training was very low, with 71% of respondents saying less than 5% of the security budget was spent on awareness training, 22% saying less than 1% was spent on such training.
- 71% of respondents said their company has no external insurance to cover computer security incident losses.
- 90% of respondents said their company experienced a computer security incident in the past 12 months.
- 64% of losses were due to the actions of insiders at the company.

The top 3 types of attack, ranked by dollar losses, were:

- financial fraud ($21.1 million)
- viruses/worms/trojans ($8.4 million)
- system penetration by outsiders ($6.8 million)

The complete results of this study, as well as past studies, which are conducted annually by the Computer Security Institute, can be found at the CSI website www.gocsi.com . Interestingly, these statistics are compiled from voluntary responses of computer security

professionals. Thus, there is certainly an inference that the damages due to computer security incidents are much higher than those cited here, as companies without responding security professionals undoubtedly were the victim of computer security incidents.

Cyber Crime Statistics from the Online Victimization of Youth, Five Years Later study:

- Increasing numbers of children are being exposed to unwanted sexual materials online.
- Reports of online sexual solicitations of youth decreased while reports of aggressive sexual solicitation of youth did not (perhaps indicating that some prevention and education measures may be working, while the most serious offenders may not be deterred).
- Online child solicitation offenses are rarely reported to any authority.
- Incidents of online harassment and bullying increased.

This is an empirical study based on approximately 1500 surveys conducted with online youth in 2005 that were compared to the results of a similar study in 2001. The study was conducted by the National Center for Missing and Exploited Children, the Crimes Against Children Research Center, and the Office for Juvenile Justice and Delinquency Prevention at the United States Department of Justice. The complete results of the study can be found here http://www.missingkids.com.

8- Types of Cybercrime, : http://www.brighthub.com/internet/security-privacy/articles/3435.aspx

Assault by Threat – threatening a person with fear for their lives or the lives of their families or persons whose safety they are responsible for (such as employees or communities) through the use of a computer network such as email, videos, or phones.
Child Pornography – the use of computer networks to create, distribute, or access materials that sexually exploit underage children.
Cyber Contraband – transferring illegal items through the internet (such as encryption technology) that is banned in some locations.
Cyber laundering – electronic transfer of illegally-obtained monies with the goal of hiding its source and possibly its destination.
Cyber stalking – express or implied physical threats that creates fear through the use of computer technology such as email, phones, text messages, webcams, websites or videos.
Cyber terrorism – premeditated, usually politically-motivated violence committed against civilians through the use of, or with the help of, computer technology.
Cyber theft – using a computer to steal. This includes activities related to: breaking and entering, DNS cache poisoning, embezzlement and unlawful appropriation, espionage, identity theft, fraud, malicious hacking, plagiarism, and piracy. Examples include:

- Advertising or soliciting prostitution through the internet. It is against the law to access prostitution through the internet (including in the state of Nevada in the United States) because the process of accessing the internet crosses state and sometimes national borders. This is a violation of the federal Digital Millennium Copyright Act http://www.copyright.gov/legislation/dcma.pdf.

- Drug Sales. Both illegal and prescription drug sales through the internet are illegal except as a customer through a state licensed pharmacy based in the United States http://www.fda.gov.

- Computer-based fraud. Fraud is different from theft because the victim voluntarily and knowingly gives the money or property to the criminal but would not have if the criminal did not misrepresent themselves or their offering. Fraud is a lie. If someone leads you on or allows you to believe something that is false to benefit them, they are lying and this is fraud. You become a victim when you voluntarily surrender monies or property based on their misrepresentation or lie. Losing money from computer crime can be especially devastating because often it is very difficult to get the money back. Examples are: scams and altering data to get a benefit, such as removing arrest records from the police station server, changing grades on the school computer system or deleting speeding tickets from driving records.

- Online Gambling. Gambling over the internet is a violation of American law because the gambling service providers require electronic payment for gambling through the use of credit cards, debit cards, electronic fund transfers which is illegal with the Unlawful Internet Gambling Enforcement Act http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:h4411eh.txt.pdf.

- Cyber tresspass – someone accesses a computer's or network's resources without the authorization or permission of the owner but does not alter, disturb, misuse, or damage the data or system. This is hacking for the purpose of entering an electronic network without permission. Examples might include:

- Using a wireless internet connection at a hotel at which you are staying and accessing the hotel's private files without disturbing them because they are available.

- Reading email, files, or noting which programs are installed on a third-party's computer system without permission just for fun, because you can. This is sometimes called Snooping.

- Cyber vandalism - Damaging or destroying data rather than stealing or misusing them (as with cyber theft) is called cyber vandalism. This can include a situation where network services are disrupted or stopped. This deprives the computer/network owners and authorized users (website visitors, employees) of the network itself and the data or information contained on the network. Examples:

- Entering a network without permission and altering, destroying, or deleting data or files.

- Deliberately entering malicious code (viruses, Trojans) into a computer network to monitor, follow, disrupt, stop, or perform any other action without the permission of the owner of the network.

- Attacking the server of the computer network (DDoS attack) so the server does not perform properly or prevents legitimate website visitors from accessing the network resources with the proper permissions.

9- Organized Crime.

10- Study of Russia-Georgia Cyber Conflict Brings Warnings To U.S. Businesses, Citizens, By Tim Wilson, Aug 18, 2009, available: http://www.darkreading.com/security/cybercrime/showArticle.jhtml;jsessionid=XNYFLA2S30SIPQE1GHPSKHWATMY32JVN?articleID=219400367.

11- Definition of Cyber terrorism, http://eziearticles.com/?An-Orthodox-Report-On-Organized-Cyber-Crime&id=5236455.
Many definitions exist for cyber terrorism like the various definitions of terrorism. A security expert named Dorothy Denning describes cyber terrorism as: politically induced hacking operations projected to cause massive loss like the severe economic breakdown or loss of life. Others denote cyber terrorism as a massive substantial attack that tears down computerized infrastructures like the telecommunications, electric power grid or the Internet without even touching a keyboard.

12 - Crime on the Net, http://rogerdarlington.me.uk/crimeonthenet.html#Hacking
Hacking can take several forms:

- Accessing - entering a network which is intended to be private
- Defacing – changing the content of another person's Web site
- Hijacking – redirecting elsewhere anyone trying to access a particular Web site
- Bombing – overwhelming a site with countless messages to slow down or even crash the server
- Denial of service – running a program which sends thousands of requests to a site simultaneously, frequently from more than one source, so that the relevant server slows down considerably or preferably (from the point of view of the hacker) crashes.

13- Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/l33193_en.htm
The main types of criminal offences covered by this Framework Decision are attacks against information systems such as piracy, viruses and denial of service attacks. This new criminal activity, which knows no borders, can be prevented and combated by:
- enhancing the security of information infrastructures
- giving law enforcement authorities the means to act.

To this end, the present Framework Decision proposes the approximation of criminal law systems and the enhancement of cooperation between judicial authorities concerning:

- illegal access to information systems;
- illegal system interference;
- illegal data interference.

In all cases, the criminal act must be intentional. Instigating, aiding, abetting and attempting to commit any of the above offences will also be liable to punishment.

14- See The CAN-SPAM Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (2003) (codified at 15 U.S.C. §§ 7701-7713 and 18 U.S.C. § 1037) took effect on January 1, 2004, http://www.spamlaws.com/federal/can-spam.shtml.

Fighting Back Against Email Spammers, Internet Hackers, and other Web Thieves, http://www.infohq.com/Computer/Spam/fight-internet-hackers-email-spammers.htm.

A hacker is an individual that attempts to take control over someone else's computer by using viruses, worms, and other types of Internet attacks. One of their favorite "tricks", is to use hacked computers to bring down a large web site by overloading the targeted site with millions of transmissions in a "denial of service" (DOS) attack.

While hackers were glorified in the early days of the Internet as people standing up for their rights against big corporations and the Government, hacking is now the hobby of criminals and thieves. Hackers prey on all citizens of the Internet and they are extremely dangerous to individuals, corporations, and governments.

How does a hacker find your computer?

Most hack attempts against personal computers result from viruses and worms running from an infected PC. It is not very difficult for the creator of the hacking program to predetermine the Internet addresses that his program will attack.
There are also amateur hackers, that use software programs, to randomly check for online computers to attack

What makes Spamming or Hacking Illegal?

The U.S. Congress outlawed certain types of spam with the CAN-SPAM Act of 2003. The law, which became effective January 1, 2004, covers email whose primary purpose is advertising or promoting a commercial product or service, including content on a Web site. However a "transactional or relationship message" – email that facilitates an agreed-upon transaction or updates a customer in an existing business relationship – may not contain false or misleading routing information, but otherwise is exempt from most provisions of the CAN-SPAM Act.

The Federal Trade Commission (FTC), the nation's consumer protection agency, is authorized to enforce the CAN-SPAM Act. CAN-SPAM also gives the Department of Justice (DOJ) the authority to enforce its criminal sanctions. Other federal and state agencies can enforce the law against organizations under their jurisdiction, and companies that provide Internet access may sue violators, as well.

However, 38 states have also passed anti-spam laws that have various penalties for illegal spammers and hackers. If you don't live in a state with an anti-spam law, you are still protected from fraudulent schemes, illegal pornography, and other illegal acts by various state and federal laws.

In addition, if a spammer or hacker causes harm to a Government computer they are subject to the penalties of USC Title 18, Part I, Chapter 47, Sec. 1030. - Fraud and related activity in connection with computers.

15- http://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf.
The term “hacking” is used to describe the unlawful access of a computer system. It is one of the oldest computer-related crimes, and in recent years has become a mass phenomenon. By targeting computer systems that host large databases, offenders can obtain identity-related data on a large scale, and this is an increasingly popular approach. In the largest case detected in the past in the USA, the thieves obtained more than 40,000,000 credit card records.

16- Prosecuting Computer crimes, February 2007- Computer Fraud and Abuse Act, Effective September 26, 2008, 18 U.S.C. § 1030 was amended by the Identity theft Enforcement and Restitution Act of 2008, http://www.justice.gov/criminal/cybercrime/ccmanual/01ccma.html.

17- F. Damaging a Computer or Information: 18 U.S.C. § 103(a)(5), http://www.justice.gov/criminal/cybercrime/ccmanual/01ccma.html#E.2.
Criminals can cause harm to computers in a wide variety of ways. For example, an intruder who gains unauthorized access to a computer can send commands that delete files or shut the computer down. Alternatively, intruders can initiate a "denial of service attack" that floods the victim computer with useless information and prevents legitimate users from accessing it. In a similar way, a virus or worm can use up all of the available communications bandwidth on a corporate network, making it unavailable to employees. In addition, when a virus or worm penetrates a computer's security, it can delete files, crash the computer, install malicious software, or do other things that impair the computer's integrity. Prosecutors can use section 1030(a)(5) to charge all of these different kinds of acts.

Section 1030(a)(5) criminalizes a variety of actions that cause computer systems to fail to operate as their owners would like them to operate. Damaging a computer can have far-reaching effects. For example, a business may not be able to operate if its computer system stops functioning or it may lose sales if it cannot retrieve the data in a database containing customer information. Similarly, if a computer that operates the phone system used by police and fire fighters stops functioning, people could be injured or die as a result of not receiving emergency services. Such damage to a computer can occur following a successful intrusion, but it may also occur in ways that do not involve the unauthorized access of a computer system.

Title 18, United State Code, Section 1030(a)(5) provides:

Whoever
(5)(A)(i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
(ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
(iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and
(B) by conduct described in clause (i), (ii), or (iii) of subsection (A), caused (or, in the case of an attempted offense, would, if completed, have caused) (i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;
(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;
(iii) physical injury to any person;
(iv) a threat to public health or safety; or
(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security
shall be punished as provided in subsection (c) of this section.

18- Crime on the Net, http://rogerdarlington.me.uk/crimeonthenet.html#Hacking.
One of the most common types of fraud on the Internet is designed to trick users of certain sites - notably banks and building societies - into disclosing their passwords or other confidential information needed to access their accounts. A common means of doing this is to e-mail customers advising that it is necessary to check or confirm their password by clicking onto a realistic but fake website and then inputting the confidential information. It is then possible for money to be fraudulently transferred from the individual's account.

In the Autumn of 2003, this type of fraud was perpetrated against UK customers of Barclays, Nat West, Lloyds TSB, Citibank, Halifax and Nationwide. In fact, no bank of financial institution would ever ask a customer to disclose confidential information in this way.

19- Credit Card Theft, http://www.ehow.com/list_7448512_cyber-identity-theft-methods.html.
Purchasing items on the Internet with your credit card can lead to having your card used by thieves to make purchases. When shopping online, stick with websites you know and trust. When making a purchase, always look at the address bar to make sure there is an "s" after the http. This indicates a secure transfer of your information. Use antivirus software that has firewall protection and prevents browser hijacking to reinforce your security.

20- Fighting Back Against Email Spammers, Internet Hackers, and other Web Thieves, http://www.infohq.com/Computer/Spam/fight-internet-hackers-email-spammers.htm.
Spam in a general sense is any email you don't want to receive. There are many types of email that you may not want e.g. advertisements, newsletters, or questionnaires, however these emails are not what the computer community refers to as spam. What the computer community is most concerned with is illegal email spam.

The definition of illegal email spam is -- attempts to deceive by falsification of seller identity or email address, and use of other trickery (defrauding), in the hope of gaining monetary advantage (stealing) from the email recipient and other parties.
The Federal Trade Commission's definition of spam, "Not all UCE is fraudulent, but fraud operators - often among the first to exploit any technological innovation - have seized on the Internet's capacity to reach literally millions of consumers quickly and at a low cost through UCE. In fact, UCE has become the fraud artist's calling card on the Internet. Much of the spam in the Commission's database contains false information about the sender, misleading subject lines, and extravagant earnings or performance claims about goods and services. These types of claims are the stock in trade of fraudulent schemes." From Prepared Statement Of The Federal Trade Commission On "Unsolicited Commercial email", November 3, 1999.

How does a spammer get your email address?
There are many ways a spammer can obtain your email address.

a. You can disclose it yourself by posting your email address on auctions, bulletin boards, advertising, or email locators.
b. Businesses might sell your email address or other personal information to a spammer.
c. Spammers can use software programs to collect email addresses from web sites or they can use random number generators to send spam out randomly.

21- Cyber Identity Theft Methods, http://www.ehow.com/list_7448512_cyber-identity-theft-methods.html.
One of the most frequent cyber crimes on the Internet is identity theft. Having your identity stolen cannot only lead to huge financial loss, it can be damaging to your reputation and leave you feeling violated as well. According to Javelin Strategies, "Incidences of the

crime increased by 11 percent from 2008 to 2009, altering the lives of 11 million Americans."
Identity theft is a form of theft in which the targets are bank accounts, credit cards, debit cards, social security numbers and information that is linked to a person's identity.

22- How spam works, http://computer.howstuffworks.com/internet/basics/spam.htm.
Spam is a huge problem for anyone who gets e-mail. According to Business Week magazine:
In a single day in May [2003], No. 1 Internet service provider AOL Time Warner (AOL) blocked 2 billion spam messages -- 88 per subscriber -- from hitting its customers' e-mail accounts. Microsoft (MSFT), which operates No. 2 Internet service provider MSN plus e-mail service Hotmail, says it blocks an average of 2.4 billion spams per day. According to research firm Radicati Group in Palo Alto, Calif., spam is expected to account for 45% of the 10.9 trillion messages sent around the world in 2003.

23- The CAN-SPAM Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (2003) (codified at 15 U.S.C. §§ 7701-7713 and 18 U.S.C. § 1037) took effect on January 1, 2004, http://www.spamlaws.com/federal/can-spam.shtml.

24- The globalization of crime a transnational organized crime threat assessment, UNODC, 2010, page 203- 209 (fig 161, 162, 163, 164, http://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf.

25- European Council framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography, Official Journal L 013 , 20/01/2004 P. 0044 – 0048, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004F0068:EN:HTML.
Child pornography: pornographic material that visually depicts or represents a real child involved or engaged in sexually explicit conduct, including lascivious exhibition of the genitals or the pubic area of a child, or a real person appearing to be a child involved or engaged in such conduct, or realistic images of a non-existent child involved or engaged in such conduct.

European Council Decision of 29 May 2000 to combat child pornography on the Internet, Official Journal L 138 , 09/06/2000 P. 0001 – 0004, http://eur- lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0375:EN:HTML.

26- The following is deemed to be punishable conduct that constitutes an offence related to child pornography, whether undertaken by means of a computer system or not:

- production of child pornography;
- distribution, dissemination or transmission of child pornography;
- supplying or making available child pornography;
- acquisition and possession of child pornography.

Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography, http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_trafficking_in_human_beings/l33138_en.htm..

27- Child Pornography Domains Reported To The Internet Watch Foundation (UK), FIG. 165, 166, 167, 168, 169 http://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf.

28- Child: anyone below the age of 18 years.
Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography, http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_trafficking_in_human_beings/l33138_en.htm.

29- Combating Online Infringement and Counterfeits Act, a bill introduced by Senator Patrick Leahy (D-VT), The Senate of the United States on September 20, 2010, http://www.wired.com/images_blogs/threatlevel/2010/09/CombatingOnlineInfringementAndCounterfeitsAct1.pdf.

30- The two forms of IP most frequently involved in cyber crime are copyrighted material and trade secrets. Piracy is a term used to describe IP theft—piracy of software, piracy of music, etc. Theft of IP affects the entire U.S. economy. Billions of dollars are lost every year to IP pirates. For example, thieves sell pirated computer software for games or programs to millions of Internet users. The company that actually produced the real product loses these sales and royalties rightfully due to the original creator. http://law.jrank.org/pages/11992/Cyber-Crime-Intellectual-property-theft.html.

31- Mississipi code of 1972- SEC. 97-45-9. Offense against intellectual property; penalties, http://www.mscode.com/free/statutes/97/045/0009.htm.
An offense against intellectual property is the intentional:
(a) Destruction, insertion or modification, without consent, of intellectual property; or
(b) Disclosure, use, copying, taking or accessing, without consent, of intellectual property.
Whoever commits an offense against intellectual property shall be punished, upon conviction, by a fine of not more than One

Thousand Dollars ($1,000.00), or by imprisonment for not more than six (6) months, or by both such fine and imprisonment. However, when the damage or loss amounts to a value of One Hundred Dollars ($100.00) or more, the offender may be punished, upon conviction, by a fine of not more than Ten Thousand Dollars ($10,000.00) or by imprisonment for not more than five (5) years, or by both such fine and imprisonment.
The provisions of this section shall not apply to the disclosure, use, copying, taking, or accessing by proper means as defined in this chapter.
Sources: Laws, 1985, ch. 319, Sec. 5, eff from and after July 1, 1985.

32- Internet Fraud: Tips to avoid Internet fraud, http://www.fbi.gov/scams-safety/fraud/internet_fraud/internet_fraud.

33- Financial and high-tech crimes, http://www.interpol.int/Public/FinancialCrime/Default.asp.
Payment card fraud is a generic term used to describe a range of offences involving theft and fraudulent use of payment card account data. Frequent types of payment card fraud include:

Application fraud – a type of ID theft crime in which payment cards are obtained through a fraudulent application process using stolen or counterfeit documents.
Account takeover – another type of ID theft crime, this usually involves deception of a financial institution, re-issue of a payment card and its redirection to a different address.
Lost / stolen card – as the name suggests, this type of fraud involves misuse of actual cards that are either lost or stolen from the genuine cardholder.

Counterfeit card – fraud undertaken using plastic cards that have been specifically produced or existing cards that have been altered. These cards are encoded with illegally obtained payment card account data in order to pay for goods and services or to withdraw cash.

Card not present (CNP) – fraud committed using payment card account data to undertake transactions where there is no face-to-face contact between the seller and purchaser. Typically, this type of fraud is committed by Internet, mail order or telephone. CNP fraud is currently the fastest growing payment card related type of fraud in many areas of the world.

34- Additional Protocol to the Convention on cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, Strasbourg, 28.I.2003, http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm.

35- Australian Human Rights Commission: Cyber racism is a term used for racism on the internet. It includes racist websites, images, blogs, videos and comments on web forums.
Racist material on the internet that is offensive, harassing or threatening may also be a criminal offence under Commonwealth as well as State and Territory law. This will depend upon the nature of material published. http://www.hreoc.gov.au/racial_discrimination/publications/cyberracism_factsheet.html.

36- Federal law prohibits individuals from betting on sports or gambling contests using a "wire communication facility," which includes the Internet. Yet the Internet allows immediate and anonymous communication that makes it difficult to trace gambling activity. Internet sites can be altered or removed in a matter of minutes. For these reasons organized crime operates Internet gambling sites.
Operators alter gambling software to be in their favor so the customer always loses. Unlike real casinos that are highly regulated, Internet gambling is unregulated and dangerous. Individuals gambling on the Internet risk providing credit card numbers and money to criminal gambling operators. Further, minors can gamble on the sites since the Internet is unaware of the age of its users. All a minor needs is access to a credit card number. Internet gambling also lures compulsive gamblers who may suffer devastating financial losses.

37- Internet Gambling: Overview of federal criminal law, http://books.google.com.lb/.

38- Evidence tampering: Tampering with evidence is the knowing and intentional physical manipulation, altering or destruction or falsification of evidence relevant to a criminal case or investigation. It is important to note that tampering is not the accidental destruction or modification of evidence, it is only if the individual had reason to believe the material or item was part of an investigation.
http://www.criminaldefenselawyer.com/crime-penalties/federal/Tampering-with-evidence.htm.

39- Computer Crime Research Center: What is a Cyber Crime? "Cyber-terrorism – attacking sabotage-prone targets by computer – poses potentially disastrous consequences for our incredibly computer-dependent society."
http://www.crime-research.org/library/Cyber-terrorism.htm.

40- Cyber Terrorism Vulnerabilities and Policy Issues “Facts Behind The Myth” by Dhanashree Nagre Priyanka Warade, http://www.contrib.andrew.cmu.edu/~dnagre/Final_Report_dnagre_pwarade.pdf

Cyberterrorism can be defined in different ways viz. it can be politically motivated hacking operations intended to cause grave harm such as loss of life or severe economic damage; or

It can be unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives, or

It can be a physical attack that destroys computerized nodes for critical infrastructures, such as the Internet, telecommunications, or the electric power grid, without ever touching a keyboard.

Thus, it is possible that if a computer facility were deliberately attacked for political purposes, all three methods described above (physical attack, EA, and cyber attack) might contribute to, or be labeled as "cyber terrorism."

41- Illinois Statute, January 1, 2009 (720 Illinois Compiled Statutes § 16D-5.5.), http://cyb3rcrim3.blogspot.com/2008/10/unlawful-use-of-encryption.html

A person shall not knowingly use or attempt to use encryption, directly or indirectly, to:
(a) commit, facilitate, further, or promote any criminal offense;
(b) aid, assist, or encourage another person to commit any criminal offense;
(c) conceal evidence of the commission of any criminal offense; or
(d) conceal or protect the identity of a person who has committed any criminal offense.

Telecommunications carriers and information service providers are not liable under this Section, except for willful and wanton misconduct, for providing encryption services used by others in violation of this Section.
A person who violates this Section is guilty of a Class A misdemeanor, unless the encryption was used or attempted to be used to commit an offense for which a greater penalty is provided by law. If the encryption was used or attempted to be used to commit an offense for which a greater penalty is provided by law, the person shall be punished as prescribed by law for that offense.
A person who violates this Section commits a criminal offense that is separate and distinct from any other criminal offense and may be prosecuted and convicted under this Section whether or not the person or any other person is or has been prosecuted or convicted for any other criminal offense arising out of the same facts as the violation of this Section.

٤٢- يمكن للدول التي تستعين بهذا الإرشاد الاستعاضة عن الباب الثالث عشر عبر الإحالة إلى قانون الجزاء أو العقوبات بالنسبة لارتكاب الجرائم المعلوماتية وذلك بإضافة مادة تنص على أنه تطبق على الجرائم المحددة بهذا الإرشاد (القانون)، العقوبات المشار إليها في المواد من . . . إلى قانون الجزاء.

٤٣- في الدول العربية قد يكون من الأجدى عدم حصر تطبيق المواد بالقاصرين فقط، ذلك أن الإباحية والمواد الجنسية تعتبر محرمة وممنوعة قانوناً، إلا أن اعتماد نص المواد والباب الخامس على عبارة القاصرين كان بسبب ذكرها في النصوص القانونية المسترشد بها مثل معاهدة بودابست ٢٠٠١ ولسهولة العودة إلى المرجع.

نص إرشاد الجرائم السيبرانية

تحرص الدول الأعضاء على تجريم الأفعال التالية:

الباب الأول: جرائم التعدي على البيانات المعلوماتية

المادة ١: جرم التعرض للبيانات المعلوماتية

كل من أقدم قصداً بصورة غير مشروعة على تعديل أو إلغاء أو محو أو إفساد أو تدمير البيانات المعلوماتية. يجوز الاشتراط أن يتسبّب الفعل المذكور بأضرار جسيمة لاعتباره جرماً.

المادة ٢: جرم اعتراض بيانات معلوماتية

كل من أقدم قصداً بصورة غير مشروعة على اعتراض بيانات معلوماتية بوسائل تقنية وذلك عند نقلها غير المُتاح للجمهور من النظام المعلوماتي أو إلى داخله. ويجوز اشتراط أن يتم الفعل بنية جرمية أو بنية الربط مع أنظمة معلوماتية أخرى.

الباب الثاني: جرائم التعدي على الأنظمة المعلوماتية

المادة ٣: جرم الولوج غير المشروع إلى نظام معلوماتي أو المكوث فيه

كل من أقدم قصداً على الولوج غير المشروع إلى نظام معلوماتي أو جزء منه أو المكوث غير المشروع فيه. ويجوز اشتراط أن يتم الفعل عن طريق مخالفة تدابير الحمأي الجارية على النظام المعلوماتي وبنيّة الحصول على بيانات رقمية أو بنيّة أخرى جرمية أو في ما يتعلق بالربط مع أنظمة معلوماتية أخرى.

المادة ٤: جرم الولوج غير المشروع إلى نظام معلوماتي أو المكوث فيه مع التعرض للبيانات المعلوماتية

كل من أقدم على الولوج غير المشروع إلى نظام معلوماتي أو جزء منه أو المكوث غير المشروع فيه مع قيامه بتعديل البيانات الرقمية أو البرامج أو إلغائها أو محوها أو إفسادها أو تدميرها أو المساس بعمل النظام المعلوماتي. ويجوز أيضاً اشتراط أن يتم الفعل عن طريق مخالفة تدابير الحمأي الجارية على النظام المعلوماتي وبنيّة الحصول على بيانات رقمية أو بنيّة أخرى جرمية أو بنية الربط مع أنظمة معلوماتية أخرى.

المادة ٥: جرم إعاقة عمل نظام معلوماتي

كل من أقدم بنيّة الغش، وبأي وسيلة، على إعاقة عمل نظام معلوماتي أو على إفساده.

الباب الثالث: إساءة استعمال الأجهزة أو البرامج المعلوماتية

المادة ٦: جرم إساءة استعمال الأجهزة أو البرامج المعلوماتية

كل من قدّم أو أنتج أو وزّع أو استورد أو صدر أو روّج أو حاز بغرض الاستخدام جهازاً أو برنامجاً معلوماتياً أو أي بيانات معلوماتية معّدة أو كلمات سر أو تراميز دخول، وذلك بغرض اقتراف أي من الجرائم المنصوص عليها في الإرشاد الحاضر.

الباب الرابع: جرائم التعدي على الأموال والمعاملات

المادة ٧: جرم الاحتيال أو الغش بوسيلة معلوماتية

كل من أقدم عن قصد و بنيّة الغش وبصورة غير مشروعة على إلحاق ضرر مالي بالغير عن طريق:

إدخال أو تبديل أو محو أو تدمير بيانات معلوماتية.

أي شكل من أشكال التعدي على عمل نظام معلوماتي.

وذلك للحصول دون وجه حق على منفعة مادية لنفسه أو للغير.

المادة ٨: جرم التزوير المعلوماتي

كل من أقدم عن قصد، وبصورة غير مشروعة، على إدخال أو تبديل أو محو أو تدمير بيانات معلوماتية، نتج عنها بيانات غير صحيحة، بقصد استخدامها، أو التعويل عليها في أغراض قانونية كما لو كانت صحيحة، بصرف النظر عما إذا كانت هذه البيانات مقروءة ومفهومة بشكل مباشر أو لا.

كل من أقدم عن قصد على استعمال البيانات المعلوماتية غير الصحيحة المذكورة في الفقرة الأولى.

المادة ٩: جرم الاختلاس أو سرقة أموال بوسيلة معلوماتية
كل من أقدم على سرقة أموال أو على اختلاسها باستعمال وسيلة معلوماتية.

المادة ١٠: جرم أعمال التسويق والترويج غير المرغوب بها
كل من أقدم على إرسال رسائل ترويج أو تسويق غير مرغوب بها إلى الغير دون تمكين المُرسل إليهم من إيقاف ورود هذه الرسائل، في حال رغبوا بذلك، بدون أن يتحملوا أي نفقات إضافية.

المادة ١١: جرم الاستيلاء على أدوات التعريف والهوية المستخدمة في نظام معلوماتي والاستخدام غير المشروع لها
كل من أقدم على الاستيلاء على أدوات التعريف والهوية العائدة لشخص آخر، والمستخدمة في نظام معلوماتي، وكذلك من أقدم عن قصد وبصورة غير مشروعة ومع علمه بالأمر على استخدام أدوات التعريف والهوية العائدة لشخص آخر في نظام معلوماتي.

المادة ١٢: جرم الاطلاع على معلومات سرية أو حساسة أو إفشائها
كل من أقدم عن قصد ودون سبب مشروع على الاطلاع بوسائل معلوماتية على معلومات سرية أو حساسة أو على إفشاء مثل هذه المعلومات بوسائل معلوماتية. يجوز اشتراط أن يؤدي الفعل إلى إلحاق الضرر بالغير أو بصاحب العلاقة.

الباب الخامس: جرائم الاستغلال الجنسي للقاصرين[٤٣]

المادة ١٣: تعاريف
تشمل المواد الإباحية الرسوم أو الصور أو الكتابات أو الأفلام أو الإشارات أو أي أعمال إباحية يشارك فيها قاصرون أو تتعلق باستغلال القاصرين في المواد الإباحية:

- قاصر يقوم بفعل جنسي صريح.
- شخص يبدو كقاصر يقوم بفعل جنسي صريح.
- صور واقعية أو مصطنعة بالمحاكاة تظهر قاصراً يقوم بفعل جنسي صريح.

القاصر هو كل من لم يتم الثامنة عشرة من عمره. ويجوز لدولة عضو أن تخفض السن إلى حدود أدنى، لا تقل عن السادسة عشرة.

المادة ١٤: جرم إنتاج مواد إباحية لقاصرين بقصد بثها بواسطة نظام معلوماتي
كل من أنتج قصداً، وبصورة غير مشروعة، مواد إباحية لقاصرين بقصد توزيعها أو بثها عبر نظام معلوماتي.

المادة ١٥: جرم عرض مواد إباحية لقاصرين بواسطة نظام معلوماتي
كل من عرض أو وفر أو قدّم قصداً، وبصورة غير مشروعة، مواد إباحية لقاصرين بواسطة نظام معلوماتي.

المادة ١٦: جرم توزيع أو بث أو نقل مواد إباحية لقاصرين بواسطة نظام معلوماتي
كل من وزّع أو بثّ أو نقل قصداً، وبصورة غير مشروعة، مواد إباحية لقاصرين بواسطة نظام معلوماتي.

المادة ١٧: جرم التزود أو تزويد الغير بمواد إباحية لقاصرين بواسطة نظام معلوماتي
كل من حصل قصداً، وبصورة غير مشروعة، على مواد إباحية لقاصرين عبر نظام معلوماتي لصالحه أو لصالح الغير.

المادة ١٨: جرم حيازة مواد إباحية لقاصرين على وسيطة إلكترونية أو نظام معلوماتي
كل من حاز قصداً، وبصورة غير مشروعة، مواد إباحية لقاصرين على وسيطة إلكترونية أو نظام معلوماتي.

المادة ١٩: جرم تحريض القاصرين على أنشطة جنسية غير مشروعة أو إعدادهم لذلك بوسيلة معلوماتية
كل من شجّع أو حرّض قاصراً على القيام بأنشطة جنسية غير مشروعة سواء مجاناً أو بعوض أو ساهم في إعداده لهذا الأمر، وذلك بأي وسيلة معلوماتية.

المادة ٢٠: جرم التحرش الجنسي بالقاصرين بوسيلة معلوماتية
كل من أقدم على التحرش جنسياً بقاصر على شبكة الإنترنت أو بأي وسيلة معلوماتية أخرى، من أجل إشباع الرغبة الجنسية أو من أجل إقناع القاصر بالقيام بأنشطة جنسية سواء مجاناً أو بعوض.

الباب السادس: جرائم التعدي على الملكية الفكرية للأعمال الرقمية

المادة ٢١: جرم وضع اسم مختلس على عمل
كل من أقدم بقصد الغش على وضع اسم مختلس على عمل أدبي رقمي أو كلّف الغير بذلك.

المادة ٢٢: جرم تقليد إمضاء المؤلف أو ختمه
كل من قلّد بقصد الغش إمضاء المؤلف أو ختمه أو إشارته.

المادة ٢٣: جرم تقليد عمل رقمي أو قرصنة البرمجيات
كل من أقدم قصداً على تقليد عمل أدبي فني رقمي أو على قرصنة البرمجيات. ويعتبر نسخ البرمجيات من قبيل أفعال التقليد.

المادة ٢٤: جرم بيع أو عرض عمل مقلّد أو وضعه في التداول
كل من أقدم على بيع أو عرض للبيع أو وضع بالتداول أو قدّم قصداً عملاً أدبياً فنياً رقمياً مقلداً.

المادة ٢٥: جرم الاعتداء على أي حق من حقوق المؤلف أو الحقوق المجاورة
كل من أقدم قصداً على الاعتداء على أي حق من حقوق المؤلف أو الحقوق المجاورة المتعلقة بالأعمال الرقمية.

الباب السابع: جرائم البطاقات المصرفية والنقود الإلكترونية

المادة ٢٦: جرم تقليد بطاقة مصرفية
كل من أقدم قصداً بصورة غير مشروعة على تقليد بطاقة مصرفية.

المادة ٢٧: جرم استعمال بطاقة مصرفية مقلّدة
كل من أقدم قصداً، مع علمه بالأمر، على استعمال بطاقة مصرفية مقلّدة سواء حصل بنتيجة هذا الاستعمال على أموال أو لم يحصل لسبب لا يعود إليه. في حال استعمال عن قصد أرقام بطاقات مصرفية مسروقة أو الاستيلاء عليها تطبق أحكام المادة ١١.

المادة ٢٨: جرم قبول الإيفاء ببطاقة مصرفية مقلّدة
كل من قبِلَ إيفاءه مبلغاً من المال بواسطة بطاقة مصرفية مقلّدة مع علمه بحقيقتها.

المادة ٢٩: جرم تزوير النقود الإلكترونية
كل من أقدم عن قصد بصورة غير مشروعة على تزوير نقود إلكترونية.

الباب الثامن: الجرائم التي تمسّ المعلومات الشخصية

المادة ٣٠: جرم معالجة معلومات ذات طابع شخصي دون حيازة تصريح أو ترخيص
كل من أقدم عن قصد على معالجة معلومات ذات طابع شخصي دون حيازة تصريح أو ترخيص مسبق يتيح له القيام بمثل هذه المعالجة من المراجع الرسمية.

المادة ٣١: جرم معالجة معلومات ذات طابع شخصي دون احترام القواعد القانونية
كل من أقدم عن قصد على معالجة معلومات ذات طابع شخصي دون التقيد بالقواعد القانونية المقررة لمعالجة المعلومات ذات الطابع الشخصي.

المادة ٣٢: جرم إفشاء معلومات ذات طابع شخصي
كل من أقدم، عن قصد أو عن إهمال، على إفشاء معلومات ذات طابع شخصي، لأشخاص لا يحق لهم الاطلاع عليها.

المادة ٣٣: جرم عدم الاستجابة لطلب الشخص المعني بالاطلاع أو التصحيح
كل من يرفض بدون وجه حق الاستجابة في مهلة قصيرة إلى طلب الشخص المعني بالاطلاع على المعلومات ذات الطابع الشخصي الخاصة به أو بتصحيحها.

الباب التاسع: جرائم العنصرية والجرائم ضد الإنسانية بوسائل معلوماتية

المادة ٣٤: جرم نشر وتوزيع المعلومات العنصرية بوسائل معلوماتية
كل من أقدم قصداً على نشر وتوزيع معلومات تثير النعرات العنصرية وتهدف إلى التمييز العنصري بحق أشخاص معينين، وذلك بواسطة شبكة الإنترنت أو غيرها من الوسائل المعلوماتية.

المادة ٣٥: جرم تهديد أشخاص أو التعدي عليهم بسبب انتمائهم العرقي أو المذهبي أو لونهم وذلك بوسائل معلوماتية

كل من أقدم على تهديد شخص أو تحقيره أو التعدي عليه بسبب انتمائه العرقي أو المذهبي أو لونه، وذلك بواسطة شبكة الإنترنت أو بأي وسيلة معلوماتية أخرى.

المادة ٣٦: جرم توزيع معلومات بوسيلة إلكترونية من شأنها إنكار أو تشويه أو تبرير أعمال إبادة جماعية أو جرائم ضد الإنسانية

كل من أقدم قصداً على توزيع أو نشر معلومات بواسطة شبكة الإنترنت أو بأي وسيلة معلوماتية أخرى من شأنها إنكار أو تشويه أو تبرير أعمال إبادة جماعية أو جرائم ضد الإنسانية.

المادة ٣٧: المساعدة أو التحريض بوسيلة إلكترونية على ارتكاب جرائم ضد الإنسانية

كل من ساعد قصداً أو حرّض بواسطة شبكة الإنترنت أو أي وسيلة معلوماتية أخرى شخصاً آخر على ارتكاب جرائم ضد الإنسانية.

الباب العاشر: جرائم المقامرة وترويج المواد المخدرة بوسائل معلوماتية

المادة ٣٨: جرم تملك وإدارة مشروع مقامرة على الإنترنت

كل من تملك أو أدار مشروع مقامرة أو عرض ألعاب مقامرة على شبكة الإنترنت أو بأي وسيلة معلوماتية أخرى.

المادة ٣٩: جرم تسهيل وتشجيع مشروع مقامرة على الإنترنت

كل من سهّل أو شجّع أو روّج لإنشاء مشروع مقامرة على شبكة الإنترنت أو باستعمال وسيلة معلوماتية أخرى.

المادة ٤٠: جرم ترويج الكحول للقاصرين على الإنترنت

كل من أقدم على ترويج الكحول مستهدفاً القاصرين على شبكة الإنترنت أو باستعمال أي وسيلة معلوماتية أخرى.

المادة ٤١: جرم ترويج المواد المخدرة على الإنترنت

كل من أقدم بصورة غير مشروعة على ترويج أو بيع أو شرح أو عرض طرق إنتاج المواد المخدرة على شبكة الإنترنت أو باستعمال أي وسيلة معلوماتية أخرى.

الباب الحادي عشر: جرائم المعلوماتية ضد الدولة والسلامة العامة

المادة ٤٢: جرم تعطيل الأعمال الحكومية بوسيلة معلوماتية

كل من أقدم على تعطيل الأعمال الحكومية أو أعمال السلطة العامة باستعمال أي وسيلة معلوماتية، وكل من أنتج أو وزع أو حاز برامج معدة لهذا الاستعمال.

المادة ٤٣: جرم الإخفاق في الإبلاغ أو الإبلاغ الخاطئ عن جرائم المعلوماتية

كل من امتنع عن قصد في الإبلاغ أو أبلغ عن قصد بشكل خاطئ عن جرائم المعلوماتية.

المادة ٤٤: جرم الحصول بوسيلة معلوماتية على معلومات سرية تخص الدولة

كل من أقدم على الاطلاع أو على الحصول أو الاطلاع على معلومات سرية تخص الدولة، وذلك من خلال شبكة الإنترنت أو باستعمال أي وسيلة معلوماتية أخرى.

المادة ٤٥: جرم العبث بالأدلة القضائية المعلوماتية

كل من أقدم على العبث بأدلة قضائية معلوماتية أو أقدم على إتلافها أو تخبئتها أو التعديل فيها أو محوها.

المادة ٤٦: جرم بث بيانات تهدد الأمن والسلامة العامة بوسيلة معلوماتية

كل من أقدم على بث أو إذاعة أو نشر بيانات أو معلومات تهدد الأمن أو السلامة العامة في الدولة أو أي دولة أخرى، وذلك من خلال شبكة الإنترنت أو باستعمال أي وسيلة معلوماتية أخرى.

المادة ٤٧: جرم الإرهاب بوسيلة معلوماتية

كل من ارتكب أعمالاً إرهابية أو ساهم فيها أو حرّض عليها باستعمال شبكة الإنترنت أو أي وسيلة معلوماتية أخرى.

المادة ٤٨: جرم التحريض على القتل بوسيلة معلوماتية

كل من أقدم على تحريض شخص آخر على القتل باستعمال شبكة الإنترنت أو أي وسيلة معلوماتية أخرى.

الباب الثاني عشر: جرائم تشفير المعلومات

المادة ٤٩: جرم عدم حيازة ترخيص أو تصريح عن تسويق أو توزيع أو تصدير أو استيراد وسائل تشفير
كل من أقدم على توزيع أو تسويق أو تصدير أو استيراد وسائل تشفير دون حيازة ترخيص أو تصريح من قبل المراجع الرسمية المختصة في الدولة.

المادة ٥٠: جرم تقديم وسائل تشفير تؤمن السرية دون حيازة تصريح أو ترخيص
كل من أقدم على توفير وسائل تشفير تؤمن السرية دون حيازة تصريح أو ترخيص من قبل الجهات الرسمية المختصة في الدولة.

المادة ٥١: جرم بيع أو تأجير وسائل تشفير ممنوعة
كل من أقدم على بيع أو تسويق أو تأجير وسائل تشفير ممنوعة.

الباب الثالث عشر: العقوبات

المادة ٥٢: يُعاقب كل من يرتكب إحدى الجرائم المحددة في هذا الإرشاد بعقوبة السجن وبالغرامة أو بإحدى هاتين العقوبتين. يُترك للدولة المعنية تحديد مدة عقوبة السجن وقيمة الغرامة بحدّيها الأدنى والأعلى.

المادة ٥٣: تُصادر الأجهزة الإلكترونية وخلافها التي استعملت في ارتكاب الجرم.

المادة ٥٤: تُشدد العقوبة في حال التكرار وفقاً للقواعد العامة المنصوص عليها في قوانين الجزاء. ويتم إبعاد الأجنبي لارتكابه إحدى هذه الجرائم.

الباب الرابع عشر: هيئة متخصصة لمكافحة الجريمة المعلوماتية

المادة ٥٥: تحرص الدول العربية على إنشاء وحدة متخصصة في الجرائم المعلوماتية في الأجهزة الأمنية المولجة بالتحقيقات القضائية تحت إشراف القضاء، كالضابطة العدلية. تتولى هذه الوحدة أعمال التحقيق في الجرائم المعلوماتية ورصدها تحت إشراف القضاء. ويتألف الجهاز البشري لهذه الوحدة من عناصر فنية متخصصة ذات كفاءة في مجال المعلوماتية والاتصالات.

المادة ٥٦: التعاون الدولي
على الدول العربية احترام المعاهدات والاتفاقيات الدولية ذات الطابع الجماعي أو الثنائي المتعلقة بمكافحة الجرائم بشكل عام مع مراعاة طبيعة الجرائم السيبرانية، وذلك لجهة تسهيل وتسريع الإجراءات الخاصة بجمع الأدلة وضبطها وتبادل المعلومات حول الجرائم المذكورة وملاحقة مرتكبيها؛ كما وتحرص الدول العربية على التعاون فيما بينها في مجال التحقيقات القضائية في الجرائم المعلوماتية، وأعمال رصدها ومكافحته.