الإرشاد الأول

الاتصالات الإلكترونية وحرية التعبير

١

الورقة البحثية الخلفية لإرشاد الاتصالات الإلكترونية وحرية التعبير

١- هدف البحث

تتناول الورقة البحثية الخلفية موضوع الاتصالات الإلكترونية وحرية التعبير في الدول العربية ورصد وتحليل التشريعات العربية التي عالجت هذه المواضيع ومقارنتها مع بعض التشريعات العالمية. وبالتالي تسليط الضوء على النقاط 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 بالاتصالات الإلكترونية وحرية التعبير.

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 بالاتصالات الإلكترونية وحرية التعبير.

شملت أعمال البحث بشكل رئيسي المواضيع التالية:

١) نقل المعلومات إلى الجمهور: يتناول أحكاماً عامةً حول مبدأ حرية نقل المعلومات إلى الجمهور عبر وسائل إلكترونية، والقيود المفروضة على هذا المبدأ، ودور مزود خدمات الشبكة ومستضيف البيانات فيما يتعلق بنقل المعلومات إلى الجمهور.

٢) النظام القانوني لمزودي خدمات الشبكات الإلكترونية: يتضمن الأحكام القانونية المنظّمة لنشاط مزودي خدمات الشبكات الإلكترونية وموجباتهم ومسؤولياتهم وتعاونهم مع السلطات العامة الأمنية والقضائية في سبيل المصلحة العامة وترسيخ العدالة.

٣) تشفير المعلومات: يتناول تراخيص استعمال وسائل التشفير واستيرادها وتصديرها ومسؤولية مزودي وسائل التشفير فيما يتعلق بخصوصية المعلومات والحالات التي يجب إفشاؤها بموجب حكم قضائي، ومسؤولية مزودي وسائل التشفير لضمان سرية المعلومات عن الضرر اللاحق بالأشخاص الذين يعهدون إليهم بإدارة اتفاقاتهم السرية المتعلقة بالتشفير، وذلك في حال حصول تعرض لسلامة أو سرية البيانات المحوّلة بواسطة الاتفاقات المذكورة.

٤) التنصت على الاتصالات الخاصة والشخصية: يتناول أحكاماً من شأنها منع التنصت أو المراقبة أو الاعتراض أو الإفشاء في ما خص الاتصالات الشخصية والخاصة. وإباحة التنصت في أحوال خاصة وفق القانون وبعد إجازة السلطات الدستورية والقضائية المختصة.

٥) أحكام جزائية: يتناول الأفعال موضوع التجريم والعقوبات المفروضة عند ارتكاب هذه الجرائم.

وأبرز ما تناوله البحث الأعمال التالية:

١) الوثائق الرسمية الأساسية الصادرة عن المجلس الأوروبي المتعلقة بهذا المجال ومنها:

- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

- Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services.

- Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector, 15 December 1997.

- Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce").

- DECLARATION on freedom of communication on the Internet (*Adopted by the Committee of Ministers on 28 May 2003 at the 840th meeting of the Ministers' Deputies*).

- Online Privacy: Using the Internet Safely Privacy Rights Clearinghouse / UCAN. Posted July 1995. Revised December 2010.
http://www.privacyrights.org/fs/fs18-cyb.htm

- Privacy and Telecommunications: Do We Have the Safeguards? By Prashant Iyengar and Elonnai Hickok in Privacy — Nov 22, 2010.
http://www.cis-india.org/advocacy/igov/privacy-india/privacy-telecommunications

- Protecting communications against forgery, by Daniel J. Bernstein.
http://cr.yp.to/antiforgery/forgery-20080501.pdf

- Practical attacks against WEP and WPA, by Martin Beck, Erik Tews, November 8, 2008.
http://dl.aircrack-ng.org/breakingwepandwpa.pdf

- Security of the WEP algorithm, by Nikita Borisov, Ian Goldberg, and David Wagner.
http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

- The Wireless Application Protocol (WAP), by Dave Singel´ee, Bart Preneel, September 2003.
http://www.citeseerx.ist.psu.edu

- The Status of Voice over Internet Protocol (VOIP) Worldwide, by the International Communication Union, 2006.
http://www.itu.int/osg/spu/ni/voice/papers/FoV-VoIP-Biggs-Draft.pdf

- Wiretapping and Electronic Eavesdropping, Olmstead v. United States, Olmstead, Berger v. New York, Katz v. United States.
http://law.jrank.org/pages/19166/Wiretapping-Electronic-Eavesdropping.html

- Privacy: An Abbreviated Outline of Federal Statutes Governing Wiretapping and Electronic Eavesdropping by Gina Marie Stevens and Charles Doyle American Law Division.
http://www.fas.org/sgp/crs/intel/98-327.pdf

- Report of the Director of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications, 2009.
http://epic.org/privacy/wiretap/2005_wiretap_report.pdf

- Telecommunications Security Guidelines for Telecommunications Management Network, John Kimmins, Charles Dinkel, and Dale Walters. U.S. Department of Commerce.
http://csrc.nist.gov/publications/nistpubs/800-13/sp800-13.pdf

- Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).

- Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services.

- Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector.

- Directive 97/13/EC of the European Parliament and of the Council of 10 April 1997 on a common framework for general authorizations and individual licenses in the field of telecommunications services.

٢) وتناولت أعمال البحث أيضا مختارات من تشريعات وطنية من دول أجنبية[1] مختلفة عالجت تنظيم الاتصالات الإلكترونية، وبخاصة منها التشريعات الأميركية، الفرنسية، الفنلندية، السويسرية، البريطانية، والأسترالية، بالإضافة إلى بعض التشريعات الخاصة من دول آسيا الوسطى.

٣) كما تم الاسترشاد بالمراجع الفقهية العالمية والعربية الخاصة بالاتصالات الإلكترونية وحرية التعبير وخصوصية البيانات:

- Encryption over IP-proof.
http://www.frequentis.com/NR/rdonlyres/7A85E0DD-518B-429C-9E18-BC6FC3D6758A/0/Frequentis_Line_Encryption.pdf

- The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy, by Jim Dempsey , September 22, 2010.
http://www.cdt.org/testimony/electronic-communications-privacy-act-promoting-security-and-protecting-privacy

-Testimony of Prof. Matt Blaze, House Committee on the Judiciary, Subcommittee on the Constitution, Civil Rights, and Civil Liberties, Hearing on ECPA Reform and the Revolution in Location Based Technologies and Services, June 24, 2010.
http://judiciary.house.gov hearings/pdf/Blaze100624.pdf

- "Lex Nokia" And Confidentiality In Electronic Communications In Finland, Posted July 26, 2010 *By Eija Warma, of Castren & Snellman, Helsinki, Finland*.
http://www.technologybar.org/2010/07/%E2%80%9Clex-nokia%E2%80%9D-and-confidentiality-in-electronic-communications-in-finland/

- Optimizing Cost and Performance in Online Service Provider Networks, by Zheng Zhang Purdue University, Ming Zhang Microsoft Research, Albert Greenberg Microsoft Research, Y. Charlie Hu Purdue University, Ratul Mahajan Microsoft Research, Blaine Christian Microsoft Corporation.
http://research.microsoft.com/en-us/um/people/ratul/papers/nsdi2010-entact.pdf

- Data Encryption- Post note by UK Parliamentary Office of Science and Technology, October 2006, available:
http://www.parliament.uk/documents/post/postpn270.pdf

- IS Auditing Procedure: P9 Evaluation of Management Controls Over Encryption Methodologies, by Information Systems Audit and control Association,
http://www.isaca.org/Knowledge-Center/Standards/Documents/P9EvalofMgmtControlsOverEncryptionMethodologie.pdf

- محاضرات الدكتور وسيم حرب – الدراسات العليا في القانون، كلية الحقوق - الجامعة اللبنانية، ١٩٩٥-٢٠٠٥، مكتب المحاماة والاستشارات القانونية والتحكيم.

- تشفير الاتصال باستخدام معايير WEP & WPA، للمؤلفة عالية تركي عبد الرحمن الحربي
http://coeia.edu.sa/images/stories/PDFs/Encrypted_communication_using_criteria_WEp__WPA.pdf

- أمن الشبكات اللاسلكية – توجيهات التمارين التطبيقية، إعداد: ألبيرتو إسكوديرو باسكال، T+46، النسخة العربية: أنس طويلة.
http://www.itrainonline.org/itrainonline/mmtk/wireless_ar/15_Wireless_Security/15_ar_mmtk_wireless_security_exercisesguidelines.doc

٥) وقد تم 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.

٦) كذلك تناولت أعمال البحث التشريعات ومشاريع القوانين التابعة للدول العربية الأعضاء في الإسكوا؛ إضافة إلى القرارات والقوانين النموذجية الصادرة عن جامعة الدول العربية والأنشطة والتجارب التي قامت بها ضمن هذا النطاق، وأبرزها الاستراتيجيات العربية والوطنية الخاصة بتكنولوجيا الاتصالات والمعلومات، ونذكر بعضها:

- الاستراتيجية العربية العامة لتكنولوجيا الاتصالات والمعلومات (٢٠٠٧-٢٠١٢).
http://www.aticm.org.eg/upload/ICTJuly2008.doc

- الإستراتيجية الوطنية لمجتمع عمان الرقمي (سلطنة عمان).
http://www.ita.gov.om/ITAPortal_AR/Services/eoman_strategy_C3.aspx?NID=110

- الاستراتيجية الوطنية لتكنولوجيا المعلومات والاتصالات (فلسطين).
http://www.mtit.gov.ps/index.php?option=com_content&task=view&id=28&Itemid=56

- استراتيجية تقانات الاتصالات والمعلومات للتنمية الاقتصادية والاجتماعية حتى ٢٠١٣ (سوريا).
http://www.reefnet.gov.sy/home/StrategySummary.doc

- الخطة الوطنية لتكنولوجيا المعلومات والاتصالات (السعودية).
http://coeia.edu.sa/index.php/ar/about-coeia/strategic-plan.html

- الرؤية الإستراتيجية لوزارة الاتصالات وتقنية المعلومات ٢٠٠١- ٢٠٢٥ (اليمن).
http://www.ptc.gov.ye/

تجدر الإشارة من ناحية أخرى إلى أنه تم التركيز على تحليل التشريعات الوطنية العربية الخاصة بتنظيم الاتصالات الإلكترونية ومقارنتها مع التشريعات الأجنبية لمعرفة مدى شمولية النقاط التي يتناولها هذا الإرشاد.

وبالتالي سنعرض أهم مخرجات البحث لهذه الجهة.

أ- التشريعات الوطنية الخاصة بالاتصالات الإلكترونية وحرية التعبير في منطقة الإسكوا

تبين أثناء أعمال البحث أن دول الإسكوا عملت على إصدار تشريعات خاصة بتنظيم الاتصالات، وهي التالية:

١- الاردن:

- قانون الاتصالات رقم (١٣) لسنة ١٩٩٥
http://www.trc.gov.jo/index.php?option=com_content&task=view&id=144&Itemid=378&lang=arabic

٢- الإمارات العربية المتحدة:

قانون اتحادي رقم (٣) لسنة ٢٠٠٣م وتعديلاته بشأن تنظيم الاتصالات
http://www.theuaelaw.com/vb/showthread.php?t=711

٣- البحرين:
- مرسوم بقانون رقم ٤٨ لسنة ٢٠٠٢ باصدار قانون الاتصالات
http://www.legalaffairs.gov.bh/htm/L4802.htm

- مرسوم سلطاني رقم ٣٠/ ٢٠٠٢ الخاص بانشاء "هيئة تنظيم الاتصالات"

٤- سلطنة عمان:
- قانون تنظيم الاتصالات بموجب المرسوم السلطاني رقم ٣٠ لسنة ٢٠٠٢ الخاص بتنظيم الاتصالات
http://www.tra.gov.om/newsite1/telecomActAr.aspx?Menu_ID=67&Lang=2

٥- سوريا:
- قانون رقم ١٨ لسنة ٢٠١٠ الخاص بالاتصالات
http://www.qun-engineer.org.sy/docs/communicationlaw.pdf

٦- السودان:
- قانون الاتصالات لسنة ٢٠٠١
http://www.moj.gov.sd/laws_3/10/5.htm

٧- العراق:
- قانون الاتصالات اللاسلكية رقم (١٥٩) لسنة ١٩٨٠
http://www.iraq-ild.org/PDF/1980/z1392.pdf

٨- فلسطين:
- قانون الاتصالات الفلسطيني لسنة ٢٠٠٥
http://www.pogar.org/publications/other/laws/media/telecomm-pal-05-a.pdf

٩- قطر:
- مرسوم بقانون رقم ٣٤ لسنة ٢٠٠٦ باصدار قانون الاتصالات
http://www.ict.gov.qa/files/law(1).pdf

١٠- الكويت:
- مشروع قانون الاتصالات الكويتي عام ٢٠١٠
http://www.eastlaws.com/News/News.aspx?ID=3928

١١- لبنان:
قانون تنظيم قطاع خدمات الاتصالات على الأراضي اللبنانية رقم ٤٣١ - صادر في ٢٢/٧/ ٢٠٠٢
http://www.tra.gov.lb/Library/Files/Uploaded%20files/Law431/Law-431.htm

- نظام التراخيص الممنوحة لمقدمي الخدمات
http://www.tra.gov.lb/Licensing-regulation-AR

١١-مصر:
- قانون الاتصالات المصري رقم ١٠ لسنة ٢٠٠٣
http://www.pogar.org/publications/other/laws/media/telecommorg-egy-03-a.pdf

١٣- السعودية:
- مرسوم ملكي رقم م/١٢ الصادر في ١٤٢٢/٣/١٢ هـ الخاص بنظام الاتصالات
http://www.mcit.gov.sa/NR/rdonlyres/8E82B7E1-DAB5-4386-ABD8-2CAC7601FAA6/0/TeleAct1.pdf

- لائحة النظر في مخالفات نظام الاتصالات
http://www.citc.gov.sa/NR/rdonlyres/0D52804A-BE7C-4E8B-A54C-74D800CF5862/0/Laeehat_AlNadhar.pdf

١٤- اليمن:
مشروع قانون الاتصالات وتقنية المعلومات
http://www.mtit.gov.ye/index.php?q=news_d&id=342

ب - شمولية التشريعات الوطنية الخاصة

لقد كرست جميع الدساتير العربية مبدأ سرية المراسلات والاتصالات السلكية وحدد بعضها مبدأ عدم جواز مراقبتها أو تفتيشها أو إفشاء سريتها أو تأخيرها أو مصادرتها إلا في الحالات التي يبينها القانون وبأمر قضائي. مثال الدستور اليمني حيث نصت المادة ٥٣ منه: "حرية وسرية المواصلات البريدية والهاتفية والبرقية وكافة وسائل الاتصال مكفولة ولا يجوز مراقبتها أو تفتيشها أو إفشاء سريتها أو تأخيرها أو مصادرتها إلا في الحالات التي يبينها القانون وبأمر قضائي".

أكدت بعض قوانين الاتصالات الوطنية الخاصة على سرية وخصوصية الاتصالات. مثال: قانون البحرين رقم ٤٨ لسنة ٢٠٠٢ الخاص بتنظيم الاتصالات حيث نصت المادة ٣ منه: "أن من مهام وصلاحية هيئة تنظيم الاتصالات حماية البيانات الخاصة وخصوصية الخدمات".

وقد حدد القانون السعودي لتنظيم الاتصالات الصادر عام ٢٠٠١ في المادة ٩ منه: "أن سرية المكالمات الهاتفية والمعلومات التي يتم إرسالها أو استقبالها عبر شبكات الاتصالات العامة مصونة. ولا يجوز الاطلاع عليها أو الاستماع إليها أو تسجيلها إلا في الحالات التي تبينها الأنظمة".

كما وحدد قانون الاتصالات المصري رقم ١٠ لسنة ٢٠٠٣ في البند ٦ من المادة ٥ منه. أن من مهام الجهاز القومي لتنظيم الاتصالات : "٦- وضع القواعد التي تضمن حماية المستخدمين بما يكفل سرية الاتصالات وتوفير أحدث خدماتها.."

أما القانون السوري الصادر عام ٢٠١٠ فقد نص في المادة ٣ منه، على أن من مهام الهيئة الناظمة لقطاع الاتصالات، (الفقرة (و) من البند ٤) "الحفاظ على سرية المعلومات الناجمة عن تقديم الخدمات وخصوصيتها". كما وأفرد هذا القانون باباً خاصاً لحماية البيانات والخصوصية والأمن القومي. فقد ورد في المادة ٥٠: " (أ)...تكون للاتصالات بين المستخدمين صفة الخصوصية. (ب) يتخذ كل مرخص له جميع الإجراءات الكفيلة بضمان سرية وخصوصية بيانات المشتركين لديه. (ج) تحدد اللائحة التنفيذية لهذا القانون شروط حماية خصوصية بيانات الحركة وخصوصية بيانات موقع المشترك".

وعملت قوانين أخرى خاصة بتنظيم الاتصالات على فرض عقوبات عند مخالفة هذه الأحكام وخرق أمن شبكة الاتصالات، مثال الإمارات العربية المتحدة حيث جاء في المادة ٧٢ من قانون تنظيم قطاع الاتصال لسنة ٢٠٠٣: "يعاقب بالحبس مدة لا تزيد عن كل من استغل أجهزة الاتصالات في الإساءة أو الإزعاج أو إيذاء مشاعر الآخرين أو لغرض أخر غير مشروع. كل من نسخ أو أفشى أو وزع بدون وجه حق فحوى أي اتصال أو رسالة هاتفية أو أي من خدمات الاتصالات".

أما القانون المصري الخاص بتنظيم الاتصالات فقد نص في المادة ٧٣ منه "يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر وبغرامة لا تزيد كل من قام أثناء تأدية وظيفته في مجال الاتصالات أو بسببها بأحد الأفعال التالية: ١ - إذاعة أو نشر أو تسجيل لمضمون رسالة اتصالات أو لجزء منها. ٢- إخفاء أو تغيير أو إعاقة أو تحوير أية رسالة اتصالات. ٤- إفشاء أية معلومات خاصة بمستخدمي شبكات الاتصال أو عما يجرونه أو ما يتلقونه من اتصالات وذلك دون وجه حق".

واكتفت بعض الدول العربية بالإحالة إلى قوانين عامة عند خرق مبدأ سرية الاتصالات، مثال قانون العقوبات اللبناني حيث جاء في الفصل الثاني من الباب الثامن: "في الجرائم الواقعة على الحرية والشرف" وقد تضمّن هذا الفصل نبذة خاصة عنوانها "في إفشاء الأسرار" (المواد من ٥٧٩ إلى ٥٨١).

كما وحددت القوانين الخاصة بتنظيم الاتصالات مسؤولية وواجبات مقدمي خدمات الاتصالات في المحافظة على سرية المعلومات، ونذكر منها على سبيل المثال: قانون قطر رقم ٣٤ لسنة ٢٠٠٦ الخاص بإصدار قانون الاتصالات والذي نص في المادة ٥٢ منه: (حماية معلومات العملاء) "على مقدمي الخدمة عند إدارة شبكاتهم ومرافقها والأنظمة المتصلة بها مراعاة حقوق الخصوصية للعميل. وتقع عليهم مسؤولية حفظ المعلومات والبيانات الخاصة بالعميل وباتصالاته التي تكون بحيازتهم، وعليهم توفير الحماية الكافية لها. ولا يجوز لمقدم الخدمة جمع أي معلومات أو استعمالها أو الاحتفاظ بها أو إعلانها عن أي عميل إلا بموافقته أو وفقاً لما يسمح به القانون.

وعلى مقدمي الخدمة التأكد من أن المعلومات المقدمة صحيحة وكاملة وصالحة لغرض استعمالها. وللعملاء الحق في أن يطلبوا تصحيح أو حذف أي معلومات خاصة بهم . وليس في أحكام هذه المادة ما يمنع السلطات المختصة من الحصول على أي معلومات سرية أو اتصالات خاصة بالعملاء وفقاً للقانون".

كما ونص القانون اللبناني رقم ٤٣١ لسنة ٢٠٠٢ الخاص بتنظيم قطاع خدمات الاتصالات على الأراضي اللبنانية، في المادة ٣٨ – (إجراءات المراقبة والتفتيش): "تعتبر المعلومات التي يطلع عليها المراقبون والمفتشون في معرض تنفيذهم لمهامهم سرية ولا يجوز لهم البوح بها إلا أمام رؤسائهم التسلسليين أو بناءً على طلب المرجع القضائي المختص. كما تطبق أحكام السرية على كل من يطلّع على هذه المعلومات بحكم عمله في الهيئة أو الوزارة".

كما وأكدت الاستراتيجيات الوطنية لتكنولوجيا المعلومات والاتصالات على السرية وحماية خصوصية البيانات، ونذكر ما ورد في بعض منها على سبيل المثال:

- الاستراتيجية العربية العامة لتكنولوجيا الاتصالات والمعلومات - بناء مجتمع المعلومات حتى ٢٠١٢، التي خصصت المحور الرابع منها لبناء الثقة والأمن في استخدام تكنولوجيا الاتصالات والمعلومات.

وفيما يلي الخطوط الرئيسية لتنفيذ هذا المحور: "

- المساهمة في تأمين وإدارة حقوق النشر الرقمية على شبكة الإنترنت وصياغة السياسات الملزمة لمكافحة التعدي على حقوق الملكية الفكرية.
- التعاون على المستوى الدولي لمكافحة جرائم الفضاء الالكتروني وإساءة استخدام تكنولوجيا الاتصالات والمعلومات.
- وضع وتفعيل تشريعات حماية البيانات وحماية خصوصية المواطن العربي.
- توفير أمن المعلومات والشبكات لضمان خصوصية المستخدم.
- إصدار قوانين وتشريعات تجرم اختراق الشبكات".

- الاستراتيجية الوطنية لمجتمع عمان الرقمي (سلطنة عمان): "إضافة إلى ذلك فقد تم إنشاء مركز البيانات الوطني ومقره هيئة تقنية المعلومات وذلك بالتنسيق مع الجهات الحكومية المهتمة ليعمل على ضمان استمرارية العمل وتحسين الكفاءة وتقليل التكلفة إلى جانب توفير بيئة آمنة للوصول للخدمات الإلكترونية على مدار الساعة والمحافظة على البيانات والمعلومات من حيث سريتها وسلامتها وحماية خصوصيتها."

- الاستراتيجية الوطنية لتكنولوجيا المعلومات والاتصالات (فلسطين)، التي حددت ضمن أهدافها العامة:
"٨. تسهيل الوصول إلى المعلومات والمعرفة واستخدام الإنترنت بشكل سريع وآمن لجميع شرائح المجتمع.
١١. حماية البيانات الفردية وخصوصيات الأفراد."

- استراتيجية تقانات الاتصالات والمعلومات للتنمية الاقتصادية والاجتماعية حتى ٢٠١٣ (سوريا)، حيث نصت على ما يلي: "برنامج بناء قطاع تقانة المعلومات: الذي يقوم على الإسراع بنشر الإنترنت في سورية؛ وعلى وضع قانون حديث لقطاع المعلوماتية، يعالج مواضيع خصوصية المعلومات، وحق الحصول على المعلومة العامة، وحقوق المعاملات والتوقيع الإلكتروني، والقواعد المتعلقة بالجرائم الإلكترونية؛ وعلى تنظيم المهنة".

- الخطة الوطنية لتكنولوجيا المعلومات والاتصالات (السعودية)، التي نصت على ما يلي: " بالإضافة إلى ذلك سيعمل مركز التميز لأمن المعلومات على تعليم مهندسين مؤهلين ليكونوا متخصصين في مجال أمن المعلومات و تشجيع الأفراد الموهوبين وكذلك الأفكار المتعلقة بمجال أمن المعلومات ليتم تحويلها إلى مشاريع ومنتجات تحت مسمى (صنع في المملكة العربية السعودية)".

هوامش

١– تراجع لائحة تشريعات الدول الأجنبية.

مقدمة إرشاد الاتصالات الإلكترونية وحرية التعبير

يرتدي الإرشاد الخاص بالاتصالات الإلكترونية وحرية التعبير أهمية خاصة بالنسبة لمجموع التشريعات السيبرانية، نظراً لأنه يتناول الجانب التقني والعملي الخاص بتحديد هويات الأطراف التي تقوم بتزويد خدمات الاتصال ونوعية ومدى مسؤوليتها. ولأن تحديد التبعة القانونية الناجمة عن أي مخالفة أو التعرض للاتصالات الإلكترونية يجب أن يستند إلى أدلة إلكترونية أو رقمية بشكل أساسي، ولتحديد مهام الأطراف المعنية بتلك الاتصالات، كان لا بد من تقنين جوانب الاتصالات الإلكترونية كافة.

مع تزايد وتنوع عدد المشتركين المتصلين بالإنترنت، ومع التطور الحاصل في إمكانية التواصل بوسائل إلكترونية بين المشتركين، فقد أصبح نقل المعلومات والبيانات الرقمية بواسطة الشبكات الإلكترونية أمراً شائعاً[1] مستعملاً على نطاق واسع في جميع الأنشطة الاقتصادية والاجتماعية والرسمية والخاصة[2]، نظراً لسرعة وسهولة التواصل بهذه الطريقة ولسهولة الولوج إلى البيانات على شبكة الانترنت. وللبيانات الرقمية المنقولة في بعض الأحيان أهمية خاصة، بحيث يؤدي إفشاؤها أو التعرض لها أو تحريفها إلى أضرار كبيرة ومسؤولية قانونية تترتب على عدد من الجهات غير المرتبطة مباشرةً بمن قام بأفعال الإفشاء أو التعرض أو التحريف. كما قد تشكل هذه البيانات المخزّنة أو المنقولة إلى الجمهور تعدياً على حقوق بعض الأشخاص، كحالة التعدي على الملكية الفكرية، ومن قبيل ذلك النسخ غير المشروع للأفلام أو الأغاني أو القدح والذم على موقع معين بحق شخص معين أو الترويج لنشاطات إجرامية ممنوعة. كما قد تكون الأدلة الإلكترونية حاسمة في إثبات عناصر بعض الجرائم الجزائية والوقائع المادية لا سيما تلك الجرائم المرتكبة بوسائل إلكترونية أو بواسطة شبكة الإنترنت أو التي يكون فيها جهاز الحاسوب أو برمجياته محلاً لها. ويقتضي إثبات هوية مُرسل الرسالة الإلكترونية أو مصدرها أو تاريخ إرسالها أو استلامها وتحديد الحاسب الخادم[3] الذي صدرت عنه. وقد نشأ بالتالي تخوف من وسائل نقل المعلومات بالطرق الإلكترونية، مما قد يحدو البعض إلى تقييدها بشكل مطلق وعدم السماح بها إلا بموجب تراخيص وحالات خاصة.

في مواجهة التحديات المذكورة الناشئة عن نقل المعلومات والبيانات بوسائل إلكترونية وتخزينها مؤقتاً لهذا الغرض، يلجأ المتعاملون عادةً إلى بعض الوسائل التقنية لحماية أنفسهم كتشفير[4] المعلومات المنقولة[5] لحفظ سريتها أو ضمان موثوقيتها، أو منع مزودي خدمات الإنترنت إظهار بعض المواقع المحظورة أو المسيئة أو قيام مستضيفي البيانات بحفظ معلومات كافية عن الأشخاص الذين يستضيفون بياناتهم. إلا أن هذه الحماية التقنية هي استنسابية وخاصة، أي أنها قد لا تكون شاملة وبالتالي فهي غير كافية ولا تُغني عن الحماية القانونية[6]. ويفترض تدخل المشترع لسن تشريعات واضحة تؤكد على مبدأ حرية نقل المعلومات للجمهور بوسيلة إلكترونية، ولكن ضمن ضوابط تتعلق بالنظام العام والسلامة العامة. كما تنظم هذه التشريعات عمل مزودي خدمات الاتصال ومستضيفي البيانات وموجباتهم ومسؤولياتهم لاسيما لجهة محتوى ومشروعية المعلومات المنقولة والمخزّنة من قبلهم، وإلزامهم بحفظ البيانات التقنية ومعلومات حركة البيانات والمعلومات التي تبين هوية الناشرين لديهم، وتقديمها للسلطات الأمنية والقضائية للمساعدة في التحقيقات وكشف الأدلة حول الجرائم. وتنظم التشريعات وسائل التشفير والترخيص لها ومنع إساءة استعمالها لارتكاب جرائم أو للمس بالأمن الوطني. كما تؤكد هذه التشريعات على خصوصية الفرد، بحيث تمنع التنصّت على الاتصالات الخاصة والشخصية إلا ضمن الضوابط التي يضعها القانون وتحت رقابة السلطات الدستورية والقضائية في الأحوال التي يجيزها القانون.

يأتي هذا الإرشاد حول الاتصالات الإلكترونية وحرية التعبير ليشكل إطاراً قانونياً متكاملاً في هذا المجال. وقد تم الاسترشاد بالإرشاد الأوروبي الصادر عام ٢٠٠٠ المتعلق بالتجارة الإلكترونية، وبالقانون الفرنسي رقم ٢٠٠٤/٥٧٥ الصادر بتاريخ ٢٠٠٤/٦/٢١ حول الثقة في الاقتصاد الرقمي، وبالقوانين الأسترالية حول تنظيم الاتصالات (قانون عام ١٩٧٩ وقانون عام ١٩٩٧) وبالقوانين الأجنبية والوطنية المختلفة في حقل إعداد نصوص الإرشاد الحالي الموجه للدول العربية حول الاتصالات الإلكترونية وحرية التعبير.

لقد تم تقسيم القانون الاسترشادي المُقترح على خمسة أبواب تتناول مسائل الاتصالات الإلكترونية وحرية التعبير وخصوصية البيانات. وهذه الأبواب هي:

الباب الأول: أحكام عامة.
الباب الثاني: النظام القانوني لمزودي خدمات الشبكات الإلكترونية.
الباب الثالث: تشفير المعلومات.
الباب الرابع: التنصّت على الاتصالات الخاصة والشخصية.
الباب الخامس: أحكام جزائية.

شروحات حول الإرشاد المتعلق بالاتصالات الإلكترونية وحرية التعبير

يتضمن **الباب الأول** المعنون «أحكام عامة» تعاريف لبعض المصطلحات التقنية والمفاهيم المُستعملة في متن الإرشاد. وكذلك يورد الباب الأول مبدأ حرية نقل المعلومات للجمهور بوسيلة إلكترونية ويضع لهذا المبدأ ضوابط. وتضع المادة ١ من الإرشاد تعاريف لنقل المعلومات للجمهور بوسيلة إلكترونية ولنقل المعلومات للجمهور على الخط ولمزود خدمات الشبكات الإلكترونية ولمزود خدمة الاتصال ولمستضيف البيانات وللمعلومات المتعلقة بحركة البيانات ولتخزين المعلومات مؤقتاً وانتقالياً ولتشفير المعلومات ولوسائل تشفير المعلومات.

تعرّف المادة ١ من الإرشاد نقل المعلومات للجمهور بوسيلة إلكترونية، فهو كل وضع بتصرف الجمهور أو فئات منه، بواسطة وسائل اتصالات إلكترونية، لإشارات أو كتابات أو صور أو أصوات أو رسائل من أية طبيعة كانت، والتي ليس لها طابع المراسلات الخاصة. فالعناصر التي تؤلف هذا المفهوم هي: الوضع بتصرف الجمهور لرسائل أياً كانت طبيعتها، واستعمال وسائل اتصالات إلكترونية، وأن لا يكون للرسائل طابع المراسلات الخاصة. أما نقل المعلومات للجمهور على الخط، فهو كل نقل، بناء لطلب فردي، لبيانات أو لمعلومات رقمية ليس لها طابع المراسلات الفردية، بواسطة وسائل اتصالات إلكترونية، تسمح بتبادل المعلومات بين المُرسل والمُستقبل. فهنا يجب أن يكون إرسال المعلومات بناء لطلب يُرسل من شخص معين. وهذا وجه الاختلاف مع المفهوم الأول. ويمكن أن يتم إرسال واستقبال المعلومات بشكل تفاعلي Interactive. ويُعرّف مزود خدمات الشبكات الإلكترونية[٧] بأنه إما مزود خدمة الاتصال أو مستضيف للبيانات. مزود خدمة الاتصال هو من يتيح للمستخدم الدخول إلى شبكة اتصالات ويمكّنه من نقل المعلومات عبرها. أما مستضيف البيانات، فهو من يتولى تخزين المعلومات العائدة للغير لديه، ولحساب هذا الغير، مقابل بدل مادي أو مجاناً. كما يتولى وضع هذه المعلومات بتصرف الجمهور من خلال استخدام شبكات الاتصال. بالتالي، على سبيل المثال، على كل شخص يرغب في التصفح على الإنترنت، الحصول على خدمة الوصول إلى شبكة الإنترنت والدخول إليها من خلال مزود خدمة الاتصال. أما الشخص الراغب في إنشاء موقع له على الإنترنت، فعليه وضع معلومات محتوى موقعه على الحاسب الخادم لدى مستضيف البيانات، للتمكّن من عرضها على شبكة الإنترنت.

وتعرّف المادة ١ من الإرشاد المعلومات المتعلقة بحركة البيانات[٨] بأنها أية معلومات تتعلق بعملية نقل للبيانات أو اتصال عبر شبكة إلكترونية، ينتجها النظام المعلوماتي المرتبط بالشبكة الإلكترونية، وتحدد هذه المعلومات مصدر الاتصال أو مُرسل البيانات والمُرسل إليه أو المُتلقي وخريطة طريق إرسال المعلومات ووقت الإرسال وتاريخه وحجم البيانات المُرسلة ومدة الإرسال وغيرها من المعلومات التقنية. فهذه المعلومات هي معلومات تقنية غير مرئية من قبل المستخدم العادي، ولا تهمه في المبدأ، ولا يعرف معظم المستخدمين بوجودها بالرغم من أنها تُحفظ لكل منهم على شبكات نقل المعلومات. وتشكل دليلاً أساسياً في التحقيقات القضائية الرامية إلى اقتفاء أثر الرسائل الإلكترونية المُرسلة على الشبكات الإلكترونية وتحديد مصدرها وهوية مُرسلها. ويقتضي تحديد المقصود بتخزين المعلومات انتقاليا ومؤقتاً وتمييزه عن التخزين النهائي للمعلومات الذي يتم بقصد الحفظ النهائي لسنوات عديدة وبقصد الاسترجاع لاحقاً، إذ أن التخزين الانتقالي أو المؤقت يتمّ بقصد نقل المعلومات كون وتيرة النقل لا تستوعب كل المعلومات دفعة واحدة، مما يحتّم إرسال المعلومات على دفعات، ومما يفرض تخزينها مؤقتاً لحاجات النقل. إن تخزين المعلومات انتقالياً ومؤقتاً يعني أن التخزين يخدم حصرياً تنفيذ عملية نقل هذه المعلومات على شبكة الاتصالات، ويشترط أن لا تزيد مدة التخزين عن الوقت المعقول اللازم لنقل المعلومات. فعمليات نقل المعلومات تشمل بطبيعتها التخزين الآلي المؤقت والوسيط أو الانتقالي للمعلومات المُرسلة ضمن الشرطين المذكورين أعلاه[٩].

تعرّف المادة ١ من الإرشاد وسائل تشفير المعلومات[١٠] بأنها تعني التجهيزات أو البرامج المعدّة من أجل تحويل البيانات، عبر اتفاقات سرية، أو من أجل تحقيق العملية المعاكسة. تهدف وسائل التشفير إلى ضمان سرية المعلومات المخزّنة أو المُرسلة أو تأمين سلامتها أو موثوقيتها. وإن تشفير المعلومات[١١] هو عملية تحويل المعلومات عبر اتفاقات سرية إلى رموز غير مفهومة بحيث ينبغي إعادتها إلى حالتها الأصلية لأجل قراءتها وفهمها. فالتشفير وفك التشفير يجريان بالاستناد إلى اتفاق سري يُبرم بين مُستقبل الرسالة ومُرسلها، بحيث إذا علم بهذا الاتفاق شخص ثالث تمكّن من قراءة محتوى الرسالة المُشفّرة[١٢]. فالرسالة المُشفرة تكون غير مفهومة من قبل الغير حتى لو تمكّن من اعتراضها. فعلى سبيل المثال البدائي عن التشفير، يقوم مُرسل الرسالة بتشفير الرسالة عبر كتابة الكلمات معكوسة بينما يفك مُستقبل الرسالة التشفير عبر عكس كل كلمة لاستعادة صيغتها الأصلية[١٣].

وحفاظاً على الحريات العامة وتحفيزاً للنشاط الاقتصادي والثقافي، تعلن المادة ٢ من الإرشاد مبدأ حرية نقل المعلومات للجمهور بوسيلة إلكترونية. فيمكن بالتالي استعمال شبكة الإنترنت بشكل حر لإنشاء المواقع عليها وعرض المعلومات والخدمات الإلكترونية ضمن أحكام القانون. ولكن المادة ٢ تضع لهذا المبدأ قيوداً، فلا يمكن الحد من ممارسة هذه الحرية إلا ضمن حدود احترام كرامة الإنسان وحرية الغير وملكيته وتعدد الآراء، ومن جهة أخرى ضمن حدود حماية النظام العام وحاجات الدفاع الوطني ومتطلبات المرافق العامة والمتطلبات التقنية لوسائل الاتصال. وأن تحترم حرية التعبير نظام حماية البيانات الشخصية.

يتضمن **الباب الثاني** المعنون «النظام القانوني لمزودي خدمات الشبكات الإلكترونية» الأحكام القانونية المنظّمة لنشاط مزودي خدمات الشبكات الإلكترونية وموجباتهم[١٤] ومسؤولياتهم[١٥] وتعاونهم مع السلطات العامة الأمنية والقضائية في سبيل المصلحة العامة وترسيخ العدالة.

تنظّم المادة ٣ مسألة تقييد الوصول إلى بعض المواقع والخدمات الإلكترونية وذلك حمايةً لبعض المعتقدات أو لحماية الأطفال[١٦] أو لحصر استخدام الإنترنت في الشركات والمؤسسات للعمل دون اللهو، وغيرها من الأمور. وبالتالي يجب بالتالي على مزود خدمة الاتصال أن يُعلم المستخدمين بوجود وسائل تقنية تسمح بتقييد الوصول إلى بعض المواقع الإلكترونية أو الخدمات الإلكترونية أو بالاختيار منها. وعلى مزود خدمة الاتصال تقديم هذه الوسائل للمستخدمين. وهذا الموجب هو موجب أساسي يقع على عاتق مزود خدمة الاتصال.

تعرض المادة ٤ من الإرشاد مسألة مدى إلزام مزود خدمة الاتصال ومستضيف البيانات بإجراء رقابة على المعلومات[١٧]. فهذا الأمر قد يكون صعباً لا بل مستحيلاً من الناحية التقنية بالنظر لحجم المعلومات الهائل وغير المحدود. وبالنظر للطابع المعقّد لهذه المعلومات كتعدد اللغات وأشكال المستندات، وبالنظر للطابع الدائم التغيّر لهذه المعلومات. وبالتالي فقد أعفت التشريعات الحديثة مزودي خدمة الاتصال ومستضيفي البيانات من إجراء رقابة مستمرة على جميع المعلومات المنقولة أو المخزّنة. إلا أنه يتوجب عليهم مراقبة بعض المعلومات أو المواقع الإلكترونية المحدّدة لفترة معينة وذلك بناءً لقرار قضائي[١٨]. وفي هذا السياق، لا تُخضع المادة ٤ من الإرشاد مزود خدمة الاتصال ومستضيف البيانات لموجب رقابة على مضمون المعلومات التي يرسلها أو يخزنها، ولا لموجب عام بالبحث عن الأعمال المتعلقة بنشاطات غير مشروعة[١٩]. يُستثنى من ذلك حالة صدور قرار قضائي يُلزم مزود خدمة الاتصال أو مستضيف البيانات بإجراء مراقبة مؤقتة ومحدودة لمعلومات محدّدة. إلا أن انتفاء موجب الرقابة على مستضيف البيانات لا يعفيه من موجب التصرف في حال علم بطابعها غير المشروع. فهو يبقى غير مسؤول طالما لم يكن يعلم بالطابع غير المشروع للمعلومات، ويصبح مسؤولاً إذا علم بهذا الطابع ولم يقدم فوراً على سحب هذه المعلومات أو جعل الوصول إليها مستحيلاً[٢٠]. وقد أثار المجلس الدستوري الفرنسي بموجب قراره رقم ٤٩٦ تاريخ ١٠ حزيران ٢٠٠٤ إشكالية وجوب كون الطابع غير الشرعي للمعلومات ظاهراً أو مُسنداً إلى قرار قضائي بسحب المعلومات، ولا يكفي إدلاء شخص ثالث بعدم مشروعية المعلومات. كذلك، يكون مزود خدمة الاتصال مسؤولاً إذا لم يمحُ المعلومات المخزّنة مؤقتاً بناءً على طلب مُرسلها، وكذلك بناءً لقرار صادر عن المحاكم. وهذا النظام لمسؤولية مزود خدمة الاتصال ينبع من الطابع المؤقت للتخزين مع انتفاء موجب الرقابة على المعلومات.

تنظّم المادة ٥ إجراءات إبلاغ مستضيف البيانات بالطابع غير المشروع للمعلومات، بحيث إذا تمت هذه الإجراءات وفق الأصول، اعتبرت معرفة مستضيف البيانات للطابع غير المشروع متحققة وفعلية، وترتبت عليه المسؤولية من جراء ذلك. فالمعطيات المطلوب إبلاغها هي: تاريخ التبليغ، عناصر التعريف عن هوية المُبلّغ، اسم المُرسل إليه ومقره، وصف الأعمال المُنازع بها ومكان تمركزها، الأسباب التي تدعو لسحب المعلومات مع ذكر القواعد القانونية والتعليل[٢١].

تتناول المادة ٦ من الإرشاد كيفية تحديد هوية الناشر بوسائل إلكترونية وذلك لتمكين الغير من مداعاته في حال ارتكابه فعلاً ضاراً به أو جرماً جزائياً كالقدح أو الذم أو انتهاك حقوق الملكية الفكرية. وتفرّق المادة ٦ في هذا الصدد بين الناشر المحترف والناشر غير المحترف. فيحق للأخير فقط إبقاء هويته سرية شرط تقديم عناصر التعريف الشخصية عنه لمستضيف البيانات الذي يخزّن معلوماته، وشرط تقديم عناصر التعريف العائدة لمستضيف البيانات للجمهور. وفي هذه القاعدة نجد تسهيلاً على الأفراد ولكن في نفس الوقت حفظاً لحقوق الغير. أما الناشر المحترف، فيُلزم دوماً بنشر عناصر التعريف العائدة له، ضماناً لشفافية معاملاته الكثيرة والمتكررة مع الغير، وتمكيناً لهذا الغير من تقدير كفاءة المحترف ومن مساءلته مباشرةً عند إخلاله بواجباته. ويجب على مستضيف البيانات أن يحتفظ بالبيانات التي تعرّف بهوية كل ناشر لمدة لا تقل عن عشر سنوات، وذلك حتى يستطيع تقديمها في كل نِزاع مستقبلي قد يثار حول

المعلومات المنشورة. أخيراً، بطبيعة الحال، وبالنظر لخصوصية المعلومات المُسلّمة إليه، يخضع مستضيف البيانات لموجب السر المهني بخصوص عناصر التعريف الشخصية، باستثناء حالة وجود قرار قضائي.

توجب المادة ٧ على كل من مزود خدمة الاتصال ومستضيف البيانات حفظ المعلومات المتعلقة بحركة البيانات والعائدة لجميع المستخدمين الذين يستفيدون من خدماته وذلك لمدة لا تقل عن خمس سنوات، إلا أنه لا يخضع لموجب الحفظ مضمون المعلومات ذاتها المُرسلة أو المخزّنة، أو المراسلات المُتبادلة. فغالباً ما تحتاج التحقيقات الإدارية والقضائية إلى مثل هذه المعلومات، ولكن لا يستطيع مزودو خدمات الشبكات الإلكترونية تقديمها لعدم أخذهم أي احتياط بحفظها. وكان لا بد من فرض ذلك بموجب نص قانوني مُلزم لهم، إذ غالباً ما يُهمل مزودو خدمات الشبكات الإلكترونية حفظ هذه المعلومات أو لا تكون لديهم مصلحة هامة بحفظها. وبطبيعة الحال، وتبعاً لخصوصية هذه المعلومات واتصافها بالطابع الشخصي كونها تحدّد بشكل مباشر أو غير مباشر أنشطة الشخص وعاداته واهتماماته وأشغاله وأمكنة تواجده، أخضعت المادة ٧ مزودي خدمة الاتصال ومستضيفي البيانات لموجب السر المهني بخصوص معلومات حركة البيانات، باستثناء حالة وجود قرار قضائي. كذلك ألزمتهم المادة ٧ بصون المعلومات حول حركة البيانات من التدمير أو المحو أو التعديل أو الإفشاء. وأخيراً فرضت عليهم محوها بعد انقضاء مدة الحفظ القانونية المحدّدة بخمس سنوات.

فرضت المادة ٨ على مزودي خدمة الاتصال ومستضيفي البيانات تقديم معلومات حركة البيانات وهوية الأشخاص الذين يستفيدون من خدماتهم للسلطات القضائية والأمنية العاملة تحت إشرافها، وكذلك تمكين هذه السلطات من الوصول إلى المعلومات المنوه عنها وفقاً لوقت الإرسال الحقيقي لها عند حصول أي عملية اتصال. فالمعلومات المنوه بها لا تتوفر إلا لدى مزودي خدمة الاتصال ومستضيفي البيانات، إلا أنها هامة جداً في إجراء التحقيقات وجمع الأدلة، ويقتضي بالتالي إلزامهم بتقديمها ضماناً لحسن سير التحقيقات[٢٢].

تأتي المادة ٩ من الإرشاد في نفس سياق المادة ٨ السابقة، لجهة مساهمة مزود خدمة الاتصال ومستضيف البيانات في مكافحة بعض الجرائم. فوفقاً للمادة ٩، يجب أن يساهم كل من مزود خدمة الاتصال ومستضيف البيانات بمحاربة الجرائم ولاسيما الجرائم ضد الإنسانية أو جرائم الإباحية للقاصرين أو التحريض على العنف أو التعرض لكرامة الإنسان. وعلى مزود خدمة الاتصال أو مستضيف البيانات بالتالي أن يضع بتصرف الجمهور آلية واضحة وسهلة للإبلاغ عن الأفعال المذكورة في هذه المادة، وعليه بعد حصول التبليغ إعلام السلطات العامة بذلك. وهذه المادة تطبيق لمبدأ عام هو واجب كل مواطن وشخص في مؤازرة عمل القضاء وتقصي الجرائم، لاسيما إذا كان ممتهناً وتتوفر له كل الوسائل التقنية لهذه المؤازرة.

تتناول المادة ١٠ من الإرشاد المسؤولية التعاقدية لكل من مزود خدمة الاتصال ومستضيف البيانات. وهي تستعيد المبادئ العامة الواردة في النظرية العامة للعقود وتطبقها على هذه الحالة الخاصة. فوفق المادة ١٠ المذكورة، يكون مزود خدمة الاتصال ومستضيف البيانات مسؤولاً عن حسن تنفيذ موجباته المنصوص عنها في العقود الموقّعة مع عملائه. ويجب أن تتضمن هذه العقود تحديداً لنوعية الخدمة المقدمة ولمواصفاتها ولمدتها، وتنتفي مسؤولية مزود خدمة الاتصال ومستضيف البيانات إذا أثبت أن عدم تنفيذ العقد تجاه عميله أو سوء تنفيذه هو ناتج عن خطأ العميل أو عن القوة القاهرة أو عن فعل الغير. إن هذه المادة هي كلاسيكية وفق قواعد القانون المدني، إذ أن كل شخص يقدم خدمة ما يكون مسؤولاً عن حسن تقديمها.

تنظّم المادة ١١ من الإرشاد حق الرد للشخص المعني المذكور في عملية نقل للمعلومات للجمهور، إذ يتمتع كل شخص تم ذكر اسمه في عملية نقل للمعلومات إلى الجمهور بحق الرد، مع عدم الإخلال بطلبات التصحيح أو الإلغاء التي يستطيع توجيهها لمزود الخدمة. توجه طلبات ممارسة حق الرد خلال ثلاثة أشهر من تاريخ النشر إلى مدير النشرة، وفي حال عدم إفشائه لاسمه للجمهور، توجه الطلبات المنوه عنها إلى مستضيف البيانات الذي يخزّن المعلومات موضوع طلب الرد، وعلى مستضيف البيانات إرسال طلب الرد دون تأخير إلى مدير النشرة. فحق الرد هو تطبيق لمبدأ عام بحفظ حق الدفاع وتمكين كل شخص من إبداء وجهة نظره حول معلومات خاصة به، لاسيما أن مدى الضرر الناتج عن النشر الإلكتروني يفوق بأضعاف ذاك الناشئ عن النشر الورقي تبعاً لإمكانية الوصول لعدد غير محدود من الأشخاص عبر الشبكات الإلكترونية.

ينظم **الباب الثالث** المعنون «تشفير المعلومات» هذه المسألة لجهة تراخيص استعمال وسائل التشفير[٢٣] واستيرادها وتصديرها ولجهة مسؤولية مزودي وسائل التشفير.

تتناول المادة ١٢ من الإرشاد إجراءات الترخيص لاستعمال وسائل التشفير[٢٤] وتقديمها واستيرادها وتصديرها، ويُراعى في ذلك خطورة وسائل التشفير واستعمالاتها المزدوجة

المدنية والعسكرية وإمكانية استخدامها لارتكاب جرائم أو للتواصل مع العدو أو بين العصابات الإجرامية[٢٥]. ففي المبدأ، إن استعمال وسائل التشفير هو حر. لكن تقديم ونقل واستيراد وتصدير وسائل التشفير التي تؤمن فقط وظيفة التوثيق أو تأمين سلامة المعلومات تخضع للترخيص أمام السلطات الرسمية المختصة. وللتخفيف من قسوة المبدأ المذكور، يمكن أن تحدّد كل دولة وسائل التشفير التي لا تخضع لأية معاملة رسمية، وذلك في ضوء متطلبات الحفاظ على الدفاع الوطني والأمن الداخلي والخارجي. كما أن تقديم ونقل واستيراد وتصدير وسائل التشفير التي تؤمن وظيفة سرية المعلومات تخضع للترخيص من السلطات الرسمية المختصة. في جميع الأحوال، يجب أن يحدد طالب الترخيص المواصفات التقنية لوسائل التشفير.

تتطرق المادة ١٣ من الإرشاد إلى مسؤولية مزودي وسائل التشفير تبعاً للضرر الذي يمكن أن ينجم عن انكشاف البيانات المشفرة أو الاتفاقات السرية المتعلقة بها. وبطبيعة الحال، وتبعاً لخصوصية المعلومات المعنية، يخضع مزوّدو وسائل التشفير لموجب السرية إلاّ في حالة صدور قرار قضائي. باستثناء الحالة التي يثبتون فيها عدم حصول خطأ مقصود أو إهمال، وبالرغم من كل نص مخالف، يُسأل مزودو وسائل التشفير لضمان سرية المعلومات عن الضرر اللاحق بالأشخاص الذين يعهدون إليهم بإدارة اتفاقاتهم السرية المتعلقة بالتشفير، وذلك في حال حصول تعرض لسلامة أو سرية البيانات المحوّلة بواسطة الاتفاقات المذكورة. إنّ هذه المادة قلبت عملياً عبء الإثبات، وذلك لصعوبته من قبل المستخدمين بوجه طرف مُمتهن كمزود وسائل التشفير، إذ تكون مسؤولية مزود وسائل التشفير مُفترضة، إلا أنه يستطيع التحلل منها بإثبات عدم ارتكابه خطأ مقصوداً أو إهمالاً.

يتعرض **الباب الرابع** المعنون «التنصّت على الاتصالات الخاصة والشخصية» لحماية الاتصالات الخاصة والشخصية من التنصّت[٢٦]، وإباحة التنصّت في أحوال خاصة وفق القانون وبعد إجازة السلطات الدستورية والقضائية المختصة[٢٧].

فوفق المادة ١٤ من الإرشاد، يمنع التنصّت أو المراقبة أو الاعتراض أو الإفشاء في ما خص الاتصالات الشخصية والخاصة إلا في الأحوال التي يجيزها القانون. وقد أجازت المادة ١٥ من الإرشاد التنصّت أو مراقبة أو اعتراض اتصالات خاصة وشخصية[٢٨] بإذن قضائي من أجل ضرورات التحقيقات القضائية الجزائية، أو بإذن من السلطات الأمنية أو الدستورية المختصة، من أجل تجميع المعلومات لمكافحة الإرهاب والجرائم الواقعة على أمن الدولة والجرائم المنظّمة[٢٩]. فالمبدأ هو منع التنصّت على الاتصالات الخاصة والشخصية، والاستثناء هو السماح به لضرورات الأمن العام والسلامة العامة[٣٠]. إذ أن حماية خصوصية الفرد وحميميته هي هامة، وهامة جداً، إلا أنها لا يمكن أن تعلو على المصلحة العامة للمجتمع في أمنه وسلامته واستقراره بتأمين العدالة فيه.

يتناول الباب الخامس المعنون «أحكام جزائية» النصوص العقابية التي تضمن فعالية تطبيق هذا الإرشاد والتزام الفرقاء بالموجبات التي أنشأها على عاتقهم[٣١]. فالمادة ١٦ من الإرشاد تحدد الأفعال الواجبة التجريم وهي: فعل عدم تعاون مزود خدمات الشبكات الإلكترونية مع القضاء بتقديم معلومات حركة البيانات أو بسحب بيانات أو بمنع الوصول إليها متى طلب منه ذلك، وفعل مزود خدمة الاتصال أو مستضيف البيانات بعدم حفظ معلومات حركة البيانات وبيانات التعريف الشخصية وفق ما يفرضه القانون[٣٢]. وفعل شخص بتقديم معلومات غير صحيحة عن قصد لمزود خدمات الشبكات الإلكترونية لحمله على سحب معلومات أو منع الوصول إليها، وفعل عدم قيام مدير النشرة بنشر رد الشخص المعني وفقاً للمادة ١١ من هذا الإرشاد، وفعل تقديم أو تصدير أو استيراد وسائل تشفير بصورة غير مشروعة دون الحصول على الترخيص المطلوب من السلطات الرسمية، وفعل التنصّت على الاتصالات الإلكترونية الخاصة والشخصية بصورة غير مشروعة خارج الحالات التي يجيزها القانون[٣٣].

إن غاية النصوص العقابية المنوه بها هي ردع المعنيين عن مخالفة مضمون هذا الإرشاد وحثهم على تلبية متطلباته. ويعود لكل دولة عضو أن تحدد العقوبات الرادعة وفق سلم العقوبات المعتمد لديها مع الأخذ بعين الاعتبار الأضرار الكبيرة الناجمة عن الجرائم المنوه عنها.

هوامش

1- See ITU World Telecommunication/ICT Indicators database, available:
http://www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf

- The number of Internet users has doubled between 2005 and 2010.
- In 2010, the number of Internet users will surpass the two billion mark, of which 1.2 billion will be in developing countries.
- A number of countries, including Estonia, Finland and Spain have declared access to the Internet as a legal right for citizens.
- With more than 420 million Internet users, China is the largest Internet market in the world.
- While 71% of the populations in developed countries are online, only 21% of the populations in developing countries are online. By the end of 2010, Internet user penetration in Africa will reach 9.6%, far behind both the world average (30%) and the developing country average (21%).
- By the end of 2010, there will be an estimated 5.3 billion million cellular subscriptions worldwide, including 940 million subscriptions to 3G services.
- Access to mobile networks is now available to 90% of the world population and 80% of the population living in rural areas.
- See Key Global Telecom Indicators for the World Telecommunication Service Sector, by International Telecommunication Union (2005-2010), available: http://www.itu.int/ITU-D/ict/statistics/at_glance/KeyTelecom.html
- See OECD Broadband statistics, June 2010, available: http://www.oecd.org/dataoecd/21/35/39574709.xls

2- See Testimony of Prof. Matt Blaze, House Committee on the Judiciary, Subcommittee on the Constitution, Civil Rights, and Civil Liberties, Hearing on ECPA Reform and the Revolution in Location Based Technologies and Services, June 24, 2010, available: http://judiciary.house.gov/hearings/pdf/Blaze100624.pdf

3- Server: A network device that provides service to the network users by managing shared resources. Note 1- The term is often used in the context of a client-server architecture for a local area network (LAN). Note 2- Examples are a printer server and a file server. Available: http://myrtle.forest.net/

٤- راجع تشفير الاتصال باستخدام معايير WEP & WPA، للمؤلفة عالية تركي عبد الرحمن الحربي.
http://coeia.edu.sa/images/stories/PDFs/Encrypted_communication_using_criteria_WEp__WPA.pdf
التشفير هو عملية تحويل البيانات إلى طلاسم حتى إذا استطاع المهاجمون (Attackers) الوصول إلى البيانات المنقولة عبر الشبكة لا يستطيعون الاستفادة من هذه البيانات.

٥- يمكن اعتبار أن أولى استعمالات وسائل التشفير الكهربائي والميكانيكي في آن في العصر الحديث يعود إلى آلات Enigma الخاصة بالجيش الألماني أبان الحرب العالمية الثانية، والتي أدى فك تشفيرها من قبل الحلفاء إلى تسريع انتصارهم في الحرب.
http://en.wikipedia.org/wiki/Enigma_machine

6- See "Lex Nokia" And Confidentiality In Electronic Communications In Finland, July 26, 2010, available:
http://www.technologybar.org/2010/07/%E2%80%9Clex-nokia%E2%80%9D-and-confidentiality-in-electronic-communications-in-finland/

In Finland, the Constitution guarantees everyone a basic right of privacy, and specifically states that "The secrecy of correspondence, telephony and other confidential communication is inviolable".

7- See Service Provider Designation of Agent to Receive Notification of Claims of Infringement, by United States Copyright Office, available: http://www.copyright.gov/onlinesp/
A "service provider" is defined as a provider of online services or network access, or the operator of facilities therefore, including an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received.
8- See the Internet Traffic Report (11/01/2001), available: http://www.internettrafficreport.com/
The Internet Traffic Report monitors the flow of data around the world. It then displays a value between zero and 100. Higher values indicate faster and more reliable connections.

9- See the Commonwealth Telecommunications (Interception and Access) Act 1979 (TIA Act) amended on 13 June 2006, is to protect the privacy of individuals who use the Australian telecommunications system, available: http://www.efa.org.au/Issues/Privacy/tia.html#storedcomms

Definition of Stored Communications

The TIA Act states:
Stored communication means a communication that:

(a) is not passing over a telecommunications system; and
(b) is held on equipment that is operated by, and is in the possession of, a carrier; and
(c) cannot be accessed on that equipment, by a person who is not a party to the communication, without the assistance of an employee of the carrier.

10- See Data Encryption- Postnote by UK Parliamentary Office of Science and Technology, October 2006, available: http://www.parliament.uk/documents/post/postpn270.pdf
Encryption is increasingly used to protect digital information, from personal details held on a computer to financial details transmitted over the Internet. Encryption has many benefits but can also be used to conceal criminal activity. This POSTnote outlines encryption techniques, their applications and their reliability. It also discusses controversial government proposals to give public authorities new powers under the Regulation of Investigatory Powers Act, relating to the handling of encrypted data in criminal investigations.

١١- يوجد عالمياً عدد كبير من وسائل التشفير، ومنها / Viaccess، Irdeto، Beta Crypt، Conax، Nagra Vis ، Trucrypt، Open VPN، GnuPG، PGP، OpenSSL الخ. . .

12- Pretty Good Privacy (PGP) is a popular program used to encrypt and decrypt e-mail over the Internet. It can also be used to send an encrypted digital signature that lets the receiver verify the sender's identity and know that the message was not changed en route. Available both as freeware and in a low-cost commercial version, PGP is the most widely used privacy-ensuring program by individuals and is also used by many corporations. Developed by Philip R. Zimmermann in 1991, PGP has become a de facto standard for e-mail security. PGP can also be used to encrypt files being stored so that they are unreadable by other users or intruders. Available: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci214292,00.html

13- *Communication Protocols:*
- Voice over Internet Protocol (VoIP) is referred to as and broadly includes Voice over Broadband (VoB), Voice over Digital Subscriber Line (DSL), Voice over Internet (VoI), Voice over Wireless Local Area Network and Internet telephony. http://www.itu.int/osg/spu/ni/voice/papers/FoV-VoIP-Biggs-Draft.pdf

- *WEP Wired Equivalent Privacy*, a security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. WEP is designed to provide the same level of security as that of a wired LAN. LANs are inherently more secure than WLANs because LANs are somewhat protected by the physicalities of their structure, having some or all part of the network inside a building that can be protected from unauthorized access. WLANs, which are over radio waves, do not have the same physical structure and therefore are more vulnerable to tampering. WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another. However, it has been found that WEP is not as secure as once believed. WEP is used at the two lowest layers of the OSI model - the data link and physical layers; it therefore does not offer end-to-end security. http://www.webopedia.com/TERM/W/WEP.html

- *WAP Wireless Application Protocol*, a secure specification that allows users to access information instantly via sand the low-bandwidth constraints of a wireless-handheld network. Although WAP supports HTML and XML, the WML language (an XML application) is specifically devised for small screens and one-hand navigation without a keyboard. WML is scalable from two-line text displays up through graphic screens found on items such as smart phones and communicators. WAP also supports WMLScript. It is similar to JavaScript, but makes minimal demands on memory and CPU power because it does not contain many of the unnecessary functions found in other scripting languages. Because WAP is fairly new, it is not a formal standard yet. It is still an initiative that was started by Unwired Planet, Motorola, Nokia, and Ericsson. http://www.webopedia.com/TERM/W/WAP.html

14- See Common Charter of Telecom Services, by Association of Unified Telecom Service Providers of India (AUSPI) 2005, available: http://www.auspi.in/pdf/Common-Charter-of-Telecom-Services-2005.pdf

15- See Data protection in the electronic communications sector, available: http://europa.eu/legislation_summaries/information_society/l24120_en.htm
The provider of an electronic communications service must protect the security of its services by:

- ensuring personal data is accessed by authorized persons only;
- protecting personal data from being destroyed, lost or accidentally altered;
- ensuring the implementation of a security policy on the processing of personal data.

In the case of an infringement of personal data, the service provider must inform the person concerned, as well as the National Regulatory Authority (NRA).

16- See US Code § 2258A. Reporting requirements of electronic communication service providers and remote computing service providers, available: http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00002258---A000-.html

17- See US Code 18 U.S.C. § 2511 (2)(A)(i) "It shall **not be** unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks." Available: http://www.cybertelecom.org/security/ecpaisp.htm

18- See Telecommunication Act of Australia 1997, available: http://www.acma.gov.au/WEB/STANDARD/pc=PC_100073
Section 324 of the Act requires an ISP to be able to intercept a communication passing over the ISP's network or facility in accordance with an interception warrant under the *Telecommunications (Interception) Act 1979*. In practice, when served with an interception warrant, the ISP will be required to intercept all traffic transmitted, or caused to be transmitted, to and from the identifier of the target service (for example, an electronic mail address) used by the interception subject and described on the face of the warrant. The ISP will need to deliver the intercepted communications to an agreed delivery point from which the intercepting agency may access those communications.

The ISP must also provide access to the traffic-related data generated to process the traffic. For interception of Internet traffic, traffic-related data will be the signaling information contained within the IP datagrams and, where applicable, the calling line identifier of the telephone service used by the interception subject to connect to the ISP.

19- See US Code 18 § 2258B. Limited liability for electronic communication service providers, remote computing service providers, or domain name registrar, available: http://www.law.cornell.edu/uscode/18/usc_sec_18_00002258---B000-.html

20- See Declaration on freedom of communication on the Internet, (Adopted by the Council of Europe Committee of Ministers on 28 May 2003 at the 840th meeting of the Ministers′ Deputies), available: https://wcd.coe.int/wcd/ViewDoc.jsp?id=37031

Principle 6: Limited liability of service providers for Internet content
Member states should not impose on service providers a general obligation to monitor content on the Internet to which they give access, that they transmit or store, nor that of actively seeking facts or circumstances indicating illegal activity. Member states should ensure that service providers are not held liable for content on the Internet when their function is limited, as defined by national law, to transmitting information or providing access to the Internet. In cases where the functions of service providers are wider and they store content emanating from other parties, member states may hold them co-responsible if they do not act expeditiously to remove or disable access to information or services as soon as they become aware, as defined by national law, of their illegal nature or, in the event of a claim for damages, of facts or circumstances revealing the illegality of the activity or information.

When defining under national law the obligations of service providers as set out in the previous paragraph, due care must be taken to respect the freedom of expression of those who made the information available in the first place, as well as the corresponding right of users to the information. In all cases, the above-mentioned limitations of liability should not affect the possibility of issuing injunctions where service providers are required to terminate or prevent, to the extent possible, an infringement of the law.

21- See US Code 18 § 2258A. Reporting requirements of electronic communication service providers and remote computing service providers, available: http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00002258---A000-.html

22- See Declaration on freedom of communication on the Internet, (Adopted by the Council of Europe Committee of Ministers on 28 May 2003 at the 840th meeting of the Ministers′ Deputies), available: https://wcd.coe.int/wcd/ViewDoc.jsp?id=37031

Principle 7: Anonymity
In order to ensure protection against online surveillance and to enhance the free expression of information and ideas, member states should respect the will of users of the Internet not to disclose their identity. This does not prevent member states from taking measures and co-operating in order to trace those responsible for criminal acts, in accordance with national law, the Convention for the Protection of Human Rights and Fundamental Freedoms and other international agreements in the fields of justice and the police.

23- See Protecting communications against forgery, by Daniel J. Bernstein, available: http://cr.yp.to/antiforgery/forgery-20080501.pdf

24- See IS Auditing Procedure Evaluation of Management Controls over encryption methodologies, available: http://www.isaca.org/Knowledge-Center/Standards/Documents/P9EvalofMgmtControlsOverEncryptionMethodologie.pdf
Risk Assessment in use of Encryption - The most critical aspect of encryption is the determination of what data should be encrypted and where and when it should be encrypted.

25- In a *New York Times* article by Charlie Savage (September 27, 2010) news that the Obama administration is proposing new legislation that would provide the U.S. Government with direct access to all forms of digital communication, «including encrypted e-mail transmitters like BlackBerry, social networking Web sites like Facebook and software that allows direct `peer to peer′ messaging like Skype to be technically capable of complying if served with a wiretap order. The mandate would include being able to intercept and unscramble encrypted messages.» In other words, the U.S. Government is taking exactly the position of the UAE and the Saudis: no communications are permitted to be beyond the surveillance reach of U.S. authorities. The new law would not expand the Government's legal authority to eavesdrop -- that's unnecessary, since post-9/11 legislation has dramatically expanded those authorities -- but would require all communications, including ones over the Internet, to be built so as to enable the U.S. Government to intercept and monitor them at any time when the law permits. In other words, Internet services could legally exist only insofar as there would be no such thing as truly private communications; all must contain a «back door» to enable government officials to eavesdrop.

Available: http://boingboing.net/2010/09/27/obama-administration.html

- The FRA law (*FRA-lagen* in Swedish) is a Swedish legislative package that authorizes the state to warrantlessly wiretap all telephone and Internet traffic that crosses Sweden′s borders. It was passed by the Parliament of Sweden on June 18, 2008, by a vote of 143 to 138 (with one delegate abstaining and 67 delegates not present) and took effect on January 1, 2009. In more detail, «FRA-law» is the common name for a new law as well as several modifications to existing laws, formally called Government proposal 2006/07:63 – Changes to defence intelligence activities (Swedish *proposition 2006/07:63 – En anpassad försvarsunderrättelseverksamhet*). It was introduced as anti-terrorism legislation, and gives the government agency Swedish National Defence Radio Establishment (FRA, Swedish *Försvarets radioanstalt*) the right to conduct signals intelligence on - to intercept - all internet exchange points that exchange traffic that crosses Swedish borders, though experts argue that it is impossible to differentiate between international traffic and traffic between Swedes. Available: http://en.wikipedia.org/wiki/FRA_law
See Figure of Signals Intelligence according to the «FRA-law».

26- See:
- US Code Chapter 119 § 2511. Interception and disclosure of wire, oral, or electronic communications prohibited, available: http://www.law.cornell.edu/uscode/uscode18/usc_sec_18_00002511----000-.html
- US Patriot Act 2001, available: http://epic.org/privacy/terrorism/hr3162.html

27- See The Finnish Electronic Communications Privacy Act (516/2004), available: http://www.technologybar.org/2010/07/%E2%80%9Clex-nokia%E2%80%9D-and-confidentiality-in-electronic-communications-in-finland

The 2002 directive was enacted in Finland in 2004 by the Act. The purpose of the Act is to guarantee confidentiality in electronic communications and define specific circumstances when confidentiality is allowed to be breached. According to the Act, a breach is permissible in the following situations: 1) by consent of a sender or recipient, 2) to facilitate handling of providing and using services, 3) to allow handling for billing purposes, 4) to allow handling for marketing purposes by the service provider, 5) handling for the purposes of technical development, 6) handling for the purpose of detecting a technical fault or error; and 7) handling in cases of misuse.

28- See Wiretap report 2009 - US courts - Table 4 Summary of Interceptions of Wire, Oral, or Electronic communications, January 1 through December 31, 2009, available: http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2009/Table4.pdf

A total of 2,376 intercepts authorized by Federal and state courts were completed in 2009. The number of applications for orders by federal authorities was 663. The number of applications reported by state prosecuting officials was 1,713, with 24 states providing reports, two more than in 2008. Installed wiretaps were in operation an average of 42 days per wiretap in 2009, compared to 41 days in 2008. The average number of persons whose communications were intercepted rose from 92 per wiretap order in 2008 to 113 per wiretap order in 2009. The average percentage of intercepted communications that were incriminating remained unchanged at 19 percent in 2009.

Public law 106-197 amended 18 U.S.C § 2519 (2) (b) to required that reporting should reflect the number of wiretap applications granted for which encryption was encountered and whether such encryption prevented law enforcement officials from obtaining the plain text of communications intercepted pursuant to the court orders. In 2009, one instance was reported of encryption encountered during a state wiretap; however, this did not prevent the officials from obtaining the plain text of the communications.

29- See Comprehensive Counter-Terrorism Act of 1991 (Introduced in Senate - IS) Subtitle B--Electronic Communications SEC. 2201. Cooperation of Telecommunications Providers with Law Enforcement, available: http://thomas.loc.gov/cgi-bin/query/F?c102:1:./temp/~c102zN0Wau:e30557

It is the sense of Congress that providers of electronic communications services and manufacturers of electronic communications service equipment shall ensure that communications systems permit the government to obtain the plain text contents of voice, data, and other communications when appropriately authorized by law.

30- See Electronic communication Flow Chart, available: http://www.plymouth.gov.uk/eleccomm3.pdf

31- See:
- US Code Chapter 119 § 2511. Interception and disclosure of wire, oral, or electronic communications prohibited, available: http://www.law.cornell.edu/uscode/uscode18/usc_sec_18_00002511----000-.html
- US Patriot Act, 20001 available: http://epic.org/privacy/terrorism/hr3162.html

32- See Telecommunications (Interception and Access) Act 1979 (C′th), available: http://www.efa.org.au/Issues/Privacy/tia.html#scw

Prohibition on Access to Stored Communications. Section 108 states:

(1) A person commits an offence if:

(a) the person:
(i) accesses a stored communication; or
(ii) authorizes, suffers or permits another person to access a stored communication; or
(iii) does any act or thing that will enable the person or another person to access a stored communication; and

(b) the person does so with the knowledge of neither of the following:
(i) the intended recipient of the stored communication;
(ii) the person who sent the stored communication.

Penalty: Imprisonment for 2 years or 120 penalty units, or both.

Note: This section does not prohibit accessing of communications that are no longer passing over a telecommunications system, from the intended recipient or from a telecommunications device in the possession of the intended recipient.

(1A) Without limiting paragraph (1)(b), a person is taken for the purposes of that paragraph to have knowledge of an act referred to in paragraph (1)(a) if written notice of an intention to do the act is given to the person.

33- See Electronic Communications Privacy Act (ECPA) enacted by the US Congress in 1986, available: http://www.fas.org/sgp/crs/intel/98-327.pdf
Title III/ECPA bars the use of any mechanism (device), tape recorder included, to intentionally capture the spoken word or any communication being transmitted electronically (intercept wire, oral, or electronic communications) without the consent of one of the participants or a court order, 18 U.S.C. 2511(1)(a),(b). This applies to all telephone conversations whether a cell telephone is involved or not. It likewise applies to all face to face conversations unless they occur in a public place or under other circumstances where the speakers should reasonably have expected that their conversation would be overheard.

نص إرشاد الاتصالات الإلكترونية وحرية التعبير

الباب الأول: أحكام عامة

المادة ١: تعاريف

نقل المعلومات للجمهور بوسيلة إلكترونية: هو كل وضع بتصرف الجمهور أو فئات منه، بواسطة وسائل اتصالات إلكترونية، لإشارات أو كتابات أو صور أو أصوات أو رسائل من أية طبيعة كانت، والتي ليس لها طابع المراسلات الخاصة.

نقل المعلومات للجمهور على الخط: هو كل نقل، بناء لطلب فردي، لبيانات أو لمعلومات رقمية ليس لها طابع المراسلات الفردية، بواسطة وسائل اتصالات إلكترونية، تسمح بتبادل المعلومات بين المُرسل والمُستقبِل.

مزوِّد خدمات الشبكات الإلكترونية: يكون مزود خدمات الشبكات الإلكترونية إما مزود خدمة الاتصال أو مستضيفاً للبيانات.

مزوِّد خدمة الاتصال: هو من يتيح للمستخدم الدخول إلى شبكة اتصالات ويمكّنه من نقل المعلومات عبرها.

مستضيف البيانات: هو من يتولى تخزين المعلومات العائدة للغير لديه، ولحساب هذا الغير، مقابل بدل مادي أو مجاناً، كما يتولى وضع هذه المعلومات بتصرف الجمهور من خلال استخدام شبكات اتصال.

المعلومات المتعلقة بحركة البيانات: هي أية معلومات تتعلق بعملية نقل للبيانات أو اتصال عبر شبكة إلكترونية، ينتجها النظام المعلوماتي المرتبط بالشبكة الإلكترونية، وتحدد هذه المعلومات مصدر الاتصال أو مُرسل البيانات والمُرسل إليه أو المُتلقي وخريطة طريق إرسال المعلومات ووقت الإرسال وتاريخه وحجم البيانات المُرسلة ومدة الإرسال وغيرها من المعلومات التقنية.

تخزين المعلومات انتقالياً ومؤقتاً: إن تخزين المعلومات انتقالياً ومؤقتاً يعني أن التخزين يخدم حصرياً تنفيذ عملية نقل هذه المعلومات على شبكة الاتصالات، ويشترط أن لا تزيد مدة التخزين عن الوقت المعقول اللازم لنقل المعلومات. فعمليات نقل المعلومات تشمل بطبيعتها التخزين الآلي المؤقت والوسيط أو الانتقالي للمعلومات المُرسلة ضمن الشرطين المذكورين أعلاه.

وسائل تشفير المعلومات: تعني وسائل التشفير التجهيزات أو البرامج المعدّة من أجل تحويل البيانات، عبر اتفاقات سرية، أو من أجل تحقيق العملية المعاكسة. تهدف وسائل التشفير إلى ضمان سرية المعلومات المخزّنة أو المُرسلة أو تأمين سلامتها أو موثوقيتها.

تشفير المعلومات: عملية تحويل المعلومات عبر اتفاقات سرية إلى رموز غير مفهومة بحيث يجب إعادتها إلى حالتها الأصلية لأجل قراءتها وفهمها.

المادة ٢: حرية نقل المعلومات للجمهور بوسيلة إلكترونية

إن نقل المعلومات للجمهور بوسيلة إلكترونية هو حر.
لا يمكن الحد من ممارسة هذه الحرية إلا ضمن حدود احترام كرامة الإنسان وحرية الغير وملكيته وتعدد الآراء، ومن جهة أخرى ضمن حدود حماية النظام العام والآداب العامة وحاجات الدفاع الوطني ومتطلبات المرافق العامة والمتطلبات التقنية لوسائل الاتصال. كما وأن حرية التعبير يجب أن تحترم نظام حماية البيانات الشخصية.

الباب الثاني: النظام القانوني لمزودي خدمات الشبكات الإلكترونية

المادة ٣: تقييد الوصول إلى بعض المواقع والخدمات الإلكترونية

يجب على مزود خدمة الاتصال أن يُعلم المستخدمين بوجود وسائل تقنية تسمح بتقييد الوصول إلى بعض المواقع الإلكترونية أو الخدمات الإلكترونية أو بالاختيار منها، وعلى مزود خدمة الاتصال تقديم هذه الوسائل التقنية للمستخدمين.

المادة ٤: رقابة مزود خدمة الاتصال ومستضيف البيانات على المعلومات

لا يخضع مزود خدمة الاتصال ومستضيف البيانات لموجب رقابة على مضمون المعلومات التي يرسلها أو يخزنها، ولا لموجب عام بالبحث عن الأعمال المتعلقة بنشاطات غير مشروعة. يُستثنى من ذلك حالة صدور قرار قضائي يُلزم

مزود خدمة الاتصال أو مستضيف البيانات بإجراء مراقبة مؤقتة ومحدودة لمعلومات محدّدة.
ولا يكون مستضيف البيانات مسؤولاً عن المعلومات المخزّنة:

- إذا لم يكن يعلم بطابعها غير المشروع الظاهر.
- أو إذا أقدم على سحب هذه المعلومات أو جعل الوصول إليها مستحيلاً منذ اللحظة التي يعلم فيها بطابعها غير المشروع الظاهر.

يكون مزود خدمة الاتصال مسؤولاً إذا لم يمحُ المعلومات المخزّنة مؤقتاً بناءً على طلب مُرسل هذه المعلومات، وكذلك بناءً لقرار قضائي.

المادة ٥: إجراءات الإبلاغ بعدم مشروعية المعلومات

يُعتبر مستضيف البيانات أنّه قد عَلِمَ بالطابع غير المشروع للمعلومات التي يخزّنها عندما يتم إبلاغه المعلومات التالية:

- تاريخ التبليغ
- إذا كان المُبلّغ شخصاً طبيعياً: اسمه ومهنته ومقره وجنسيته وتاريخ ومكان الولادة
- إذا كان المُبلّغ شخصاً معنوياً: شكله القانوني، مركزه القانوني، واسم المفوض بتمثيله
- اسم المُرسل إليه ومقره
- وصف الأعمال المُنازع بها ومكان تمركزها
- الأسباب التي تدعو لسحب المعلومات مع ذكر القواعد القانونية والتعليل.

المادة ٦: عدم إفشاء هوية الناشر وحفظ بيانات التعريف الشخصية له

يحق لكل شخص ينشر معلومات، بصفة غير مهنية أو غير محترفة، للجمهور عبر الاستفادة من خدمات مستضيف بيانات، أن يبقي هويته سرية وأن يقدم إلى الجمهور عناصر التعريف العائدة فقط لمستضيف البيانات، شرط تقديم عناصر التعريف الشخصية عنه لمستضيف البيانات.
أما الناشر المحترف، فيجب عليه دوماً تقديم عناصر التعريف الشخصية به للجمهور.

يجب على مستضيف البيانات أن يحتفظ بالبيانات التي تعرّف بهوية كل ناشر لمدة لا تقل عن عشر سنوات.

كما يخضع مستضيف البيانات لموجب السر المهني بخصوص عناصر التعريف الشخصية باستثناء حالة وجود قرار قضائي.

المادة ٧: حفظ معلومات حول حركة البيانات

يجب على كل من مزود خدمة الاتصال ومستضيف البيانات حفظ المعلومات المتعلقة بحركة البيانات والعائدة لجميع المستخدمين الذي يستفيدون من خدماته، وذلك لمدة لا تقل عن خمس سنوات. لا يخضع لموجب الحفظ مضمون المعلومات ذاتها المُرسلة أو المخزّنة أو المراسلات المُتبادلة.

يخضع مزود خدمة الاتصال ومستضيف البيانات لموجب السر المهني بخصوص معلومات حركة البيانات باستثناء حالة وجود قرار قضائي.

يلتزم مزود خدمة الاتصال ومستضيف البيانات بصون المعلومات حول حركة البيانات من التدمير أو المحو أو التعديل أو الإفشاء، كما يلتزم بمحوها بعد انقضاء مدة الحفظ القانونية المحدّدة بخمس سنوات.

المادة ٨: تقديم معلومات حركة البيانات للسلطات القضائية والأمنية

يجب على كل من مزود خدمة الاتصال ومستضيف البيانات تقديم المعلومات المتعلقة بحركة البيانات وبهوية الأشخاص الذين يستفيدون من خدماتهم، وذلك إلى السلطات القضائية والأمنية المختصة العاملة تحت إشرافها. وكذلك يجب عليهم تمكين هذه السلطات من الوصول إلى المعلومات المنوه عنها وفقاً لوقت الإرسال الحقيقي لها عند حصول أي عملية اتصال.

المادة ٩: مساهمة مزود خدمة الاتصال ومستضيف البيانات في مكافحة بعض الجرائم

يجب أن يساهم كل من مزود خدمة الاتصال ومستضيف البيانات بمحاربة الجرائم ولاسيما الجرائم ضد الإنسانية أو الجرائم الإباحية للقاصرين أو بالتحريض على العنف أو التعرض لكرامة الإنسان. وعلى مزود خدمة الاتصال أو مستضيف البيانات بالتالي أن يضع بتصرف الجمهور آلية واضحة وسهلة للإبلاغ عن الأفعال المذكورة في هذه المادة، وعليه بعد حصول التبليغ إعلام السلطات العامة بذلك.

المادة ١٠: المسؤولية التعاقدية لمزود خدمة الاتصال ومستضيف البيانات

يكون كل من مزود خدمة الاتصال ومستضيف البيانات مسؤولاً عن حسن تنفيذ موجباته المنصوص عنها في

العقود الموقّعة مع عملائه. ويجب أن تتضمن هذه العقود تحديد نوعية الخدمة المقدمة ومواصفاتها ومدتها.

تنتفي مسؤولية مزود خدمة الاتصال ومستضيف البيانات إذا أثبت أن عدم تنفيذ العقد تجاه عميله أو سوء تنفيذه هو ناتج عن خطأ العميل أو عن القوة القاهرة أو عن فعل الغير.

المادة ١١: حق الرد للشخص المعني المذكور في عملية نقل المعلومات للجمهور

يتمتع كل شخص تم ذكر اسمه في عملية نقل للمعلومات إلى الجمهور على الخط بحق الرد، مع عدم الإخلال بطلبات التصحيح أو الإلغاء التي يستطيع توجيهها لمزود الخدمة. توجه طلبات ممارسة حق الرد خلال ثلاثة أشهر من تاريخ النشر إلى مدير النشرة. وفي حال عدم إفشائه لاسمه للجمهور، توجه الطلبات المنوه عنها إلى مستضيف البيانات الذي يخزّن المعلومات موضوع طلب الرد. وعلى مستضيف البيانات إرسال طلب الرد دون تأخير إلى مدير النشرة.

الباب الثالث: تشفير المعلومات

المادة ١٢: استعمال وسائل التشفير وتقديمها واستيرادها وتصديرها

إن استعمال وسائل التشفير هو حر.

إن تقديم ونقل واستيراد وتصدير وسائل التشفير التي تؤمن فقط وظيفة التوثيق أو تأمين سلامة المعلومات يخضع للترخيص من قبل السلطات الرسمية المختصة. يمكن أن تحدّد كل دولة وسائل التشفير التي لا تخضع لأية معاملة رسمية، وذلك في ضوء متطلبات الحفاظ على الدفاع الوطني والأمن الداخلي والخارجي.

إن تقديم ونقل واستيراد وتصدير وسائل التشفير التي تؤمن وظيفة سرية المعلومات يخضع للترخيص من قبل السلطات الرسمية المختصة.

في جميع الأحوال، يجب أن يحدد طالب الترخيص المواصفات التقنية لوسائل التشفير.

المادة ١٣: مسؤولية مزودي وسائل التشفير

يخضع مزوّدو وسائل التشفير لموجب السرية باستثناء حالة صدور قرار قضائي.

باستثناء الحالة التي يثبتون فيها عدم حصول خطأ مقصود أو إهمال، وبالرغم من كل نص مخالف، يُسأل مزودو وسائل التشفير لضمان سرية المعلومات عن الضرر اللاحق بالأشخاص الذين يعهدون إليهم بإدارة اتفاقاتهم السرية المتعلقة بالتشفير، وذلك في حال حصول تعرض لسلامة أو سرية البيانات المحوّلة بواسطة الاتفاقات المذكورة.

الباب الرابع: التنصّت على الاتصالات الخاصة والشخصية

المادة ١٤: عدم جواز التنصّت على الاتصالات الخاصة والشخصية

تضمن الدول الأعضاء الحق في سرية الاتصالات الإلكترونية الخاصة والشخصية، بحيث لا تخضع هذه الاتصالات لأي نوع من أنواع التنصّت أو المراقبة أو الاعتراض أو الإفشاء إلا في الأحوال التي يجيزها القانون.

المادة ١٥: جواز التنصّت بإذن قضائي أو لضرورات الأمن الوطني

يمكن لكل دولة عضو أن تجيز التنصّت أو مراقبة أو اعتراض أو إفشاء اتصالات خاصة أو شخصية في الحالتين التاليتين:

- بإذن قضائي، من أجل ضرورات التحقيقات القضائية الجزائية.

- بإذن من السلطات الأمنية أو الدستورية المختصة تحت إشراف القضاء، من أجل تجميع المعلومات لمكافحة الإرهاب والجرائم الواقعة على أمن الدولة والجرائم المنظّمة.

الباب الخامس: أحكام جزائية

المادة ١٦: أحكام جزائية

ضماناً للفعالية في تطبيق أحكام هذا الإرشاد، تحرص الدول الأعضاء على تجريم الأفعال التالية:

- عدم تعاون مزود خدمات الشبكات الإلكترونية مع القضاء بتقديم معلومات حركة البيانات أو بسحب بيانات أو بمنع الوصول إليها متى طُلب منه ذلك.

- فعل مزود خدمة الاتصال أو مستضيف البيانات بعدم حفظ معلومات حركة البيانات وبيانات التعريف الشخصية وفق ما يفرضه القانون.

- قيام شخص بتقديم معلومات غير صحيحة عن قصد لمزود خدمات الشبكات الإلكترونية لحمله على سحب معلومات أو منع الوصول إليها.

- عدم قيام مدير النشرة بنشر رد الشخص المعني وفقاً للمادة ١١ من هذا الإرشاد.

- تقديم أو تصدير أو استيراد وسائل تشفير بصورة غير مشروعة دون الحصول على الترخيص المطلوب من السلطات الرسمية.

- التنصّت على الاتصالات الإلكترونية الخاصة والشخصية بصورة غير مشروعة خارج الحالات التي يجيزها القانون.