حقوق امنیت اطلاعات شبکه

سیدوحید ابوالمعالی الحسینی*
زهراسادات علیزاده طباطبایی**

تاریخ دریافت: ۸۷/۸/۲۰ تاریخ تأیید: ۸۷/۹/٦

چکیده

در این حقیقت که سلامت و بقای هر اجتماعی نیازمند امنیت است، تردیدی نیست، ولی هنگام کاربرد قواعد امنیت در حوزهٔ اطلاعات به تجزیهٔ قسمت‌های مختلف آن مجبور می‌شویم، چنان‌که در این حوزه، مفاهیم متعددی مانند: جرایم اینترنتی، حریم خصوصی و مسئولیت مدنی را می‌توان بررسی کرد. حقوق امنیت اطلاعات، نمونه‌ای از یک ماتریس بین‌رشته‌ای است که به‌سختی می‌توان تعریف مشخصی از آن ارائه داد. در این مقاله به‌طور اجمال به معرفی گوشه‌ای از این ساختار چندوجهی می‌پردازیم.

واژگان کلیدی: *امنیت اطلاعات، حریم خصوصی، امنیت داده، جرایم اینترنتی.*

* دانشجوی دکتری حقوق جزا و جرم‌شناسی دانشگاه تهران (vahid_abolmaali@yahoo.com).
** دانشجوی دکتری حقوق جزا و جرم‌شناسی دانشگاه تهران (Zahra.at@gmail.com).

۱. جنبه‌های گوناگون امنیت اطلاعات

اطلاعات از دیرباز موضوعی قابل توجه بوده است و حمایت از امنیت اطلاعات (به‌ویژه برخی اطلاعات مهم و حیاتی) همواره از اهمیت زیادی برخوردار بوده است، ولی در واقع، مسئلهٔ نخست و مهم در فن صحیح حفظ امنیت نیست، بلکه در تعریف امنیت و نقض امنیت نهفته است. روشن است که پرداختن به مسائل صرفاً فنی این موضوع تا زمانی که مبانی امنیت به‌طور کلی موجود نباشد و ناقص باشد یا توافقی بر اصول آن وجود نداشته باشد، تمرکز بر امنیت فضای سایبر حتی در بهترین وضعیتِ قانونگذاری، مشکل مهمی را برطرف نخواهد ساخت. به همین دلیل، تمرکز بر مسائل «پسینی» حقوق امنیت اطلاعات باید پیش‌تر بر اصول محکم‌تری به نام مبانی «پیشینی» امنیت بنا شود که اجماع نظر دولت و ملت در ذات اهداف امنیت است. بنابراین، پرسش نخست اینکه امنیتِ کدام اطلاعات و براساس چه معیارهایی باید حفظ شود و ضمانت اجرای آن چیست؟

مطالعهٔ تطبیقی آثار خارجی دربارهٔ حقوق امنیت اطلاعات سایبری، در بیشتر موارد به جرایم رایانه‌ای و حقوق مسئولیت ختم می‌شود. در واقع، حقوق امنیت اطلاعات در متن قوانین جرایم رایانه‌ای، تحصیل دلیل، مسئولیت مدنی و حریم خصوصی بحث شده است (Miawald, 2004: 98)؛ زیرا در حقوق خارجی، دربارهٔ مسائل پیشینی امنیت، وفاق ملی و قانون اساسی وجود دارد و قطعات اصلی موضوعاتی که باید در حمایت قانون قرار گیرد و امنیت اطلاعات آن حفظ شود، موجود است. برای توضیح بیشتر، نخست با جنبهٔ پیشینی و پسینی امنیت اطلاعات آشنا می‌شویم.

۲. جنبه‌های «پیشینی» و «پسینی» امنیت اطلاعات

جنبه‌های پیشینی امنیت اطلاعات مربوط به بنیادی‌ترین تعریفی است که دولت از امنیت و گونه‌های مختلف آن ارائه می‌دهد و به‌عبارت دقیق‌تر، بازتابی از نظام سیاسی یک کشور است؛ به‌عنوان مثال، اصل ۲۵ قانون اساسی ایران می‌گوید: «بازرسی و نرساندن نامه‌ها، ضبط و فاش کردن مکالمات تلفنی، افشای مخابرات تلگرافی و تلکس، سانسور

یا عدم مخابره و ارسال آنها، استراق سمع و هرگونه تجسس ممنوع است، مگر به حکم قانون». در واقع، این بخش از اطلاعات خصوصی افراد، موضوعی است که در قانون اساسی حمایت شده است و قانون موضوعه برای حمایت از این حقی که در قانون اساسی به رسمیت شناخته شده است، به تدوین اصول، قواعد و نحوهٔ اجرای آن ملزم شده است. با تأکید بر این نکته که این اصل قانون اساسی فقط به نهادهای دولتی دارندهٔ اطلاعات شخصی افراد و با مصادیق کاملاً محدود منحصر است ـ و از این نظر ممکن است آن را نسخهٔ بسیار ابتدایی و سادهٔ قواعد «حمایت از داده» و یا «حریم خصوصی» محسوب کنیم ـ، زمانی که این اطلاعات به‌دست نهادهای اداری و دولتی می‌رسد و یا این نهادها به‌نحوی به تبادل آن می‌پردازند، باید تمهیدات ایمنی لازم را برای محافظت از محتوای آن به‌کار گیرند. پس، قانون حفظ این محتوا را حکم می‌کند و متخصصان فن باید قواعد فنی برای محافظت از این اطلاعات را به‌کار گیرند.

نهادهای دولتی و رژیم حقوقی مدیریت اطلاعات دولتی نیز موضوعی مهم از نقطه نظر امنیت اطلاعات محسوب می‌شوند. دولت، بزرگترین منبع تولید اطلاعات است و مدیریت دسترسی و یا ممنوعیت دسترسی به این اطلاعات، موضوعی برای به‌کار بستن قواعد و فنون امنیت است. در یک نظام بستهٔ سیاسی، بخش بزرگی از اطلاعات دولتی مشمول قواعد محرمانگی است و به‌طور معمول منابع مالی و انسانی زیادی صرف حفظ امنیت این اطلاعات می‌شود. در این سیستم، اصل عملی عدم دسترسی وجود دارد و باید برای آزادی دسترسی به هر بخش از اطلاعات دولتی، قوانین مشخصی تصویب کرد (انصاری، ۱۳۷٤: ٤٥). در نتیجه، نگاه امنیتی در این بخش، جزئی‌نگر، فراگیر و وسیع است و چون اصل عملی محدویت دسترسی به اطلاعات دولتی وجود دارد، نظام قانونی و فنی کشور باید تمهیدات لازم را برای محافظت از آن بخش وسیع از اطلاعات به‌کار گیرد و هر هزینه‌ای برای امنیت این ساختارِ اطلاعاتی حجیم، موجه است و توجیه اقتصادی آن فرع بر مسائل پیشینی امنیت و اهداف آن است. این رویکرد پیشینی برخلاف قوانین کشورهایی است که قانون آزادی اطلاعات را تصویب کرده‌اند و یا سیستم کتابخانه‌ای دسترسی به اطلاعات دولتی وجود دارد که نگاه امنیتی، کاملاً محدود و موردی است. در این صورت فقط بخش ناچیزی از اطلاعات دولتی مشمول قواعد

محرمانگی است. در حالی که طیفی از اصول برای حفظ امنیت اطلاعات به‌کار گرفته خواهند شد که تضمین‌کنندهٔ دسترسی شهروندان به اطلاعات دولتی است. طبق همین دیدگاه است که کشورهای اروپایی کاربرد قواعد امنیت اطلاعات را بدون توجه به معیارهای حقوق بشر و دموکراسی، بی‌ارزش و غیرمفید می‌دانند (اصل پنجم رهنمودهایی برای امنیت سیستم‌ها و شبکه‌های اطلاعاتی، OECD، ۲۰۰۲). بنابراین، بحث دربارهٔ هزینه‌های منطقی در دسترس قرار دادن اطلاعات، دغدغهٔ اصلی این نظام‌هاست (Green, Paper on Public Sector Information in the Information Society, 1998: 13-15). در حقیقت در هر دو نظام بسته و باز، بدون هیچ تردیدی برای امنیت اطلاعات هزینه می‌شود و تفاوت فقط در این است که در یک نظام باز به‌دلیل وجود اصل آزادی دسترسی به اطلاعات دولتی، بخش کوچکی از اطلاعات مشمول محرمانگی است، در نتیجه حفظ محرمانگی بهتر، مؤثرتر و کم هزینه‌تر است.

۳. امنیت اطلاعات

امنیت به‌معنای ایمنی در برابر خطرات احتمالی و یا واقعی که موجودیت و بقای یک پدیدهٔ زنده، فرد یا جامعه را تهدید می‌کند، تعریف شده است (یزدی، ۱۳۸٤: ۲٦۳). تعریفی از امنیت در علم رایانه، آن را به حداقل رساندن خطر افشای اطلاعات در بخش‌های غیرمجاز می‌داند (king & Osmanoghlu, 2001: 74). امنیت اطلاعات مجموعه‌ای از ابزارها برای جلوگیری از سرقت، حمله، جنایت، جاسوسی و خرابکاری (هاشمیان، ۱۳۷۹: ۳۷) و علم مطالعهٔ روش‌های حفاظت از داده‌ها در رایانه‌ها و نظام‌های ارتباطی در برابر دسترسی و تغییرات غیرمجاز است (عبداللهی، ۱۳۷۵: ۷۳). در واقع، می‌توان گفت امنیت اطلاعات اصولاً در صورت رعایت سه خصوصیت «محرمانه بودن اطلاعات» (یعنی اطلاعات فقط در دسترس کسانی که مجوز دارند، قرار خواهد گرفت و سطح محرمانگی نیز با توجه به درجهٔ اهمیت اطلاعات تعیین می‌شود)، «صحت اطلاعات» (یعنی حفاظت از دقت و صحت اطلاعات و جلوگیری از تغییرات غیرمجاز و از بین بردن اطلاعات و راه‌های مناسب پردازش آن) و «در دسترس بودن اطلاعات» (اطمینان از اینکه کاربران مجاز هر زمان نیاز داشته باشند، امکان دسترسی به اطلاعات

را دارند) تأمین می‌شود (electronic information security, 2008: 3-5). از دیدگاه صرفاً حقوقی، مسئلهٔ امنیت اطلاعات به‌طور معمول در قوانین جرایم رایانه‌ای، تجارت الکترونیکی، امضای الکترونیکی و امضای دیجیتال نمود یافته است (UNCITRAL Model Law on Electronic Signatures with Guide to Enactment, 2001).

سازمان همکاری و توسعهٔ اقتصادی OECD (Organization For Economic Coopration & Development) در تعریف خود به هدف امنیت توجه کرده است و می‌گوید: هدف امنیت سیستم‌های اطلاعاتی، حفاظت از منافع آنهایی است که به سیستم‌های اطلاعاتی در برابر نقص در دسترس بودن، محرمانگی و تمامیت، اطمینان کرده‌اند (رهنمود OECD، ۱۹۹۲: ۱۱ـ۱۲). اتحادیهٔ بین‌المللی مخابرات نیز در اجلاس ژولای ۲۰۰۵، پس از تعریف واژه‌های سایبر، امنیت و امنیت سایبری، در نهایت مسئله را در چهار دستهٔ اصلی جمع‌بندی می‌کند:

۱. **منع**: تمرکز و استفاده از قانونگذاری چندجانبه در زمینهٔ جرایم سایبری و...؛

۲. **پیشگیری**: طراحی و استفاده از سیستم‌های بیشتر ایمن، مدیریت بهتر امنیت و توسعهٔ مکانیزم‌های امنیتی و...؛

۳. **کشف**: مکانیزم تهیهٔ سیاست‌های همکاری جهت هشدار در زمینهٔ حملات و...؛

٤. **عکس‌العمل**: طراحی زیرساخت‌های قوی‌تر اطلاعاتی، برنامه‌های مدیریت بحران و اقدامات پلیسی و قضایی و... ([ITU] thematic meeting on cybersecurity, 2005: 24).

دربارهٔ حمایت از امنیت اطلاعات در فضای سایبر، سه دسته از اقدامات باید از هم تفکیک شوند:

اول. قواعدی که به‌طور معمول در مقررات تجلی می‌یابند و بخشی از قانون موضوعهٔ کشور را تشکیل می‌دهند. در این باره می‌توان به دو قانون که مربوط به جدیدترین نوآوری‌های دولت فدرال امریکا دربارهٔ حریم خصوصی در فضای سایبر هستند، اشاره کرد: «قانون مدرنیزه کردن خدمات مالی» موسوم به «گراهام لیچ بلیلی» و «قانون قابلیت نقل و انتقال و حساب‌پذیر بودن بیمهٔ سلامتی» (health insurance portability and accountability act 1996 – HIPAA) نمونه‌هایی از مقررات فنی ـ حقوقی امنیت اطلاعات سایبری در امریکا هستند که در متن قانون نخست،

قواعد فنی دقیقی نسبت به رعایت حریم خصوصی افراد و نحوهٔ انتشار و در دسترس قرار دادن اطلاعات معرفی شده است. در حاشیهٔ این قانون، بعضی از فنون مؤثرِ امنیت (مانند قانون امضای دیجیتال در ارتباطات سازمان‌های دولتی)، به‌طور مستقل توجه شده است تا وسیله‌ای برای کارآمدتر شدن این مقررات محسوب شود (Michael A Benoit & Joseph D. Looney). دربارهٔ «قانون قابلیت نقل و انتقال و حساب‌پذیر بودن بیمهٔ سلامتی»، نهادهای ذی‌ربط به اجرای استانداردهای حفاظتی اطلاعات سلامتی افراد موظف شدند و اداره‌ای با عنوان «ادارهٔ خدمات سلامت انسانی» برای اجرای این مقررات تأسیس شد. منظور نهایی این مقررات، اطمینان از محرمانگی، تمامیت و در دسترس بودن اطلاعات پزشکی محافظت شده (Protected Health Information-PHI) است که نگهداری شده‌اند.

دوم. قواعد فنی و تخصصی که در دستورالعمل‌های فنی، کدهای رفتاری و استانداردهای اجباری به تفصیل ذکر می‌شوند. در این باره می‌توان از تکنیک‌های کنش‌گرایانه و یا واکنشی، برحسب زمان عکس‌العمل در برابر یک مشکل امنیتی، برای تأمین امنیت اطلاعات استفاده کرد (Venter & Eloff, 2003: 26).

فناوری‌های کنش‌گرایانه مربوط به انجام عملیات پیش‌گیرانهٔ قبل از به‌وجود آمدن یک مشکل خاص امنیتی؛ مانند استفاده از رمزنگاری (cryptography)، امضاهای دیجیتال (digital signatures)، گواهی‌های دیجیتالی (digital certificates)، شبکه‌های مجازی خصوصی (virtual private networks)، نرم‌افزارهای آسیب‌نما (vulnerability scanners)، پویشگرهای ضدویروس (anti-virus scanner)، پروتکل‌های امنیتی (security protocols) و سخت‌افزارهای امنیتی (security hardware) بوده است و فناوری‌های واکنشی، انجام عکس‌العمل لازم پس از وقوع یک مشکل خاص امنیتی؛ مانند دیوار آتش (firewalls)، کنترل دسترسی (access control)، کلمات عبور (passwords)، زیست‌سنجی (biometric) و به‌ویژه نظام‌های آشکارسازی نفوذی (intrusion detection systems (IDS)) و واقعه‌نگاری (logging) هستند (اسدی، ١٣٨٤: ٥٦).

سوم. انتشار استانداردهای جهانی به‌وسیلهٔ سازمان‌های تخصصی مثل ایزو که سیستم‌های قضایی به‌عنوان بهترین معیارهای آزمون عقلانیت، آنها را مبنای تشخیص

خود قرار می‌دهند. خوشبختانه نزدیک به یک دهه از ارائهٔ یک ساختار امنیت اطلاعـات به‌وسیلهٔ مؤسسهٔ استاندارد انگلیس می‌گذرد. در این مـدت، اسـتاندارد مـذکور (BS7799) بازنگری شد و در سال ۲۰۰۰ میلادی نیز مؤسسهٔ بین‌المللی ISO نخستین بخـش آن را در قالب استاندارد ISO17799 ارائه کرده اسـت. ایـن اسـتاندارد در تشـخیص نقـض امنیـت سیستم، به‌عنوان کلید تشخیص دادگاه‌های امریکا نقش ایفا می‌کند (Miawald, 2002: 128).

در ادامهٔ بحث، مسائل حقوقی مربوط به امنیت اطلاعات در فضای سایبر را به چهار دستهٔ کلی جرایم رایانه‌ای، مسئولیت مدنی، حریم خصوصی و ادلهٔ اثبات تقسیم می‌کنیم و به‌صورت جداگانه به بررسی هریک خواهیم پرداخت.

۱ـ۳. جرایم رایانه‌ای

پیشرفت فنی در زمینهٔ فناوری ارتباطـات، باعـث ظهـور قواعـد حقـوقی و بـه‌تبـع آن، رفتارهای جدید فاصله‌گیر از هنجارها (هنجارگریزی) شده است و این موضوع نـه‌تنهـا اموال (مانند: تقلب‌های رایانه‌ای)، بلکه اشخاص (سوء استفاده از اطلاعـات و داده‌هـای شخصی افراد) و دولت‌ها (تروریسم و جاسوسی سایبری) را نیز دربرگرفتـه اسـت و از آنها حمایت می‌کند (دلماس مارتی، ۱۳۸۷: ۷۵).

دربارهٔ جرایم رایانه‌ای، تعریف‌های مختلفی ارائه شـده اسـت. نخسـتین گـام بـرای تعریف جرایم رایانه‌ای در سال ۱۹۸۳ به‌وسیلهٔ گروهـی از متخصصـان کـه بـه دعـوت سازمان همکاری و توسعهٔ اقتصادی (OECD) در پاریس جمع شده بودند، ارائـه شـده است که عبارت است از: «سوء استفاده از رایانه‌ها شامل هر رفتار غیرقانونی، غیراخلاقی یا غیرمجاز مربوط به پردازش خودکار و انتقال داده است. در ایـن تعریـف، گرچـه بـه صراحت از جرایم رایانه‌ای نام برده نشده است، ولی منظـور از سـوء اسـتفاده از رایانـه همان جرایم رایانه‌ای است. در تعریف دیگری آمده است: «هر عمل مثبت غیرقانونی که رایانه در آن، ابزار یا موضوع جرم باشد، جرم رایانه‌ای است» (نشریهٔ بین‌المللـی سیاسـت جنایی، ۱۳۷٦: ۱۱۸). پلیس جنایی فدرال آلمان نیز تعریفی از جرایم رایانـه‌ای ارائـه داده است که مقرر می‌دارد: «جرم رایانه‌ای دربرگیرندهٔ همهٔ اوضاع و احوال و کیفیاتی اسـت که در آن، شکل‌های پردازش الکترونیک داده‌ها، وسیلهٔ ارتکاب و یـا هـدف یـک جـرم

قرار گرفته است و مبنایی برای نشان دادن این ظنّ است که جرمی ارتکاب یافته است» (دزیانی، ۱۳۷۳: ۱۵۷ـ۱۵۸).

تاریخچهٔ جرایم رایانه‌ای را می‌توان به سه نسل طبقه‌بندی کرد [البته باید خاطرنشان کرد که طبقه‌بندی این جرایم در قالب سه نسل، براساس نسل‌های تکاملی سیستم‌های رایانه‌ای نبوده است و معیارهای دیگری مدنظر قرار گرفته است (انزالی، ۱۳۷٤: ۳۷)]:

نسل اول که تا اواخر دههٔ ۱۹۸۰ است و بیشتر اقدامات غیرمجاز در این نسل، به ایجاد اختلال در کارکرد این سیستم‌ها و به تبع آن، دستکاری داده‌ها مربوط می‌شد. بنابراین، تدابیری که برای مقابله با آنها اتخاذ می‌شد، بیشتر رویکرد امنیتی داشت؛ به‌عنوان مثال، برای حفظ امنیت پردازشگرهای داده‌های الکترونیکی (EDP)، هفت مؤلفه تعیین شده بود که عبارت‌اند از: ۱. امنیت اداری و سازمانی؛ ۲. امنیت پرسنلی؛ ۳. امنیت فیزیکی؛ ٤. امنیت مخابرات الکترونیکی؛ ۵. امنیت سخت‌افزاری و نرم‌افزاری؛ ٦. امنیت عملیاتی؛ ۷. برنامه‌ریزی احتیاطی (دزیانی، ۱۳۷٦: ۷٤).

نسل دوم که جرایم داده‌ها نامیده می‌شود تا اواخر دههٔ ۱۹۹۰ ادامه داشته است. مشخصهٔ بارز این نسل، توجه به داده‌ها سوای از واسط آنهاست. در این مقطع، مباحث حقوقی و به تبع آن رویکردهای مقابله با جرایم رایانه‌ای نیز تغییر یافت، به‌نحوی که تدابیر پیشگیرانه از جرایم رایانه‌ای با محوریت داده‌ها ـ و نه واسطشان ـ تنظیم شدند و حتی این رویکرد در قوانینی که در آن زمان به تصویب می‌رسید نیز قابل مشاهده است (همو، ۱۳۸۳: ٤).

نسل سوم که از اواسط دههٔ ۱۹۹۰ شروع می‌شود، جرایم رایانه‌ای با عنوان جرایم سایبر (cyber crime) یا جرایم در محیط سایبر (cyber space) معروف شد. در این نسل، بحث دربارهٔ ابعاد گوناگون فضای سایبر به‌ویژه مسائل حقوقی آن، وارد مرحلهٔ جدیدی شد؛ زیرا تا آن زمان شبکه‌های رایانه‌ای در ابعاد منطقه‌ای و محلی و در حوزه‌های محدودی مانند سیستم‌های تابلوی اعلانات (bulletin board system) که معمولاً برای بارگذاری (loading) و پیاده‌سازی (downloading) برنامه‌ها و پیام‌ها و همچنین ارتباطات پست الکترونیک به‌کار می‌رفتند، به فعالیت می‌پرداختند (جلالی فراهانی، ۱۳۸٤: ۱٤۷). خصوصیات منحصر به فرد محیط سایبر باعث شد جرایم

کامپیوتری از جنبهٔ اقتصادی وسیع‌تر شود و ابعاد جدیدتری به خود بگیرد. این خصوصیات باعث به‌وجود آمدن امکان تعرض به شبکه‌های حیاتی متصل به فضای سایبر؛ مانند بیمارستان‌ها و نیروگاه‌های بزرگ و تخریب آنها می‌شود و می‌تواند خساراتی معادل جنگ‌های تسلیحاتی یا حتی فراتر از آن را به‌بار آورد. در این باره می‌توان به ورود کرم اینترنتی که برای نخستین بار به‌وسیلهٔ یک دانشجوی امریکایی ساخته شده بود و باعث شد تا سیستم رایانه‌ای حدود ٦٢٠٠ کاربر اینترنت، شامل دانشگاه‌ها، سرویس‌های نظامی و سایت‌های بیمارستان‌ها مختل شود و هزینهٔ تعمیراتی حدود ۹۸ میلیون دلار در پی داشته باشد، اشاره کرد. گرچه بعد از مدتی این دانشجو دستگیر شد و پس از محاکمه به پرداخت تمام مبالغ پیش‌گفته محکوم شد، ولی برخی از خسارات به‌وجود آمده غیرقابل جبران بود (Gerald, 2001: 298). علاوه بر این، هم‌اکنون بحث هرزه‌نگاری در عرصهٔ اینترنت، به‌ویژه هرزه‌نگاری کودکان (child pornography)، به معضلی بین‌المللی تبدیل شده است، طوری که در سال ۱۹۹۹، اجلاس یونسکو با بررسی این موضوع، اعلامیه‌ای را برای مقابله با آن صادر کرد (حسینی، ۱۳۸۲: ۷۵).

در واقع، جرم رایانه‌ای به مفهومی که امروز وجود دارد، نتیجهٔ بیش از چهار دهه تلاش دانشگاهی و قانونگذاری در سطح ملی و بین‌المللی است. در سال ۱۹٦۳، گروه کارشناسان رایانه در OECD به‌وجود آمد و شورای اروپا از سال ۱۹٦۸ مسائل مربوط به حفاظت از داده‌های شخصی را مورد توجه جدی قرار داد. OECD در سال ۱۹۸۳ مطالعه برای هماهنگ‌سازی بین‌المللی جرایم رایانه‌ای را در دستور کار خود قرار داد و در سال ۱۹۸٦ رهنمود جرایم مرتبط با رایانه را منتشر کرد. پس از تکمیل گزارش OECD، شورای اروپا طرح مطالعه‌ای برای تدوین رهنمودی جهت کمک به قانونگذاران را در دستور کار خود قرار داد. در این مطالعه، فهرست حداقل OECD گسترش یافت و مسائلی مانند حریم خصوصی، بزهدیدگان، پیشگیری و مسائل آیین‌دادرسی، شامل جنبه‌های بین‌المللی تفتیش و توقیف بانک‌های داده و همکاری بین‌المللی جرایم رایانه‌ای مورد توجه قرار گرفت. همچنین، در پاراگراف‌های ٤٢ــ٤٤ پیشنهاد کنگرهٔ هشتم پیشگیری از جرایم و رفتار با مجرمان سال ۱۹۹۰ سازمان ملل متحد،[1] به‌طور مشخص از جرایم رایانه‌ای بحث شده است. در دوازدهمین نشست

1. Eight United Nations Congress on Crime Prevention and Criminal Justice.

عمومی کنگرهٔ هشتم، نمایندهٔ کانادا پیش‌نویس قطعنامه‌ای را دربارهٔ جرایم مرتبط با رایانه ارائه داد که از جمله به مدرنیزه کردن قوانین کیفری برای جبران خسارت‌هایی که از راه جرایم مرتبط با رایانه به‌وجود می‌آید، تأکید داشت. در این قطعنامه، مشکلاتی مانند: تعقیب، تحقیق، کشف جرایم، آموزش قضات و نهادهای مسئول برای امر تعقیب و تحقیق، آشنایی این نهادها با عصر انفورماتیک و سیاست حمایت از بزهدیدگان رایانه‌ای و... مدنظر قرار گرفته بود. پس از آن، OECD در سال ۱۹۹۲ رهنمودی دربارهٔ امنیت سیستم‌های اطلاعاتی منتشر کرد که مورد توجه قانونگذاران ملی و بعضاً بنگاه‌های خصوصی در تدوین چارچوب‌های امنیتی قرار گرفت. در همین سال، شورای اروپا بر مسائل آیین دادرسی و همکاری‌های بین‌المللی تمرکز کرد. کنوانسیون اروپایی جرایم رایانه‌ای، سال ۲۰۰۱ در بخش اول (جرایم ماهوی)، نخست تقسیم‌بندی موضوعی از جرایم ارائه می‌دهد و سپس در مواد ۲ـ۱۳ به تعریف انواع آن می‌پردازد.[1] در جدیدترین کنگره،[2] به سرقت خدمات مخابراتی یا رایانه‌ای از راه فنون هک تصریح شده است.

جرایم رایانه‌ای شامل حمله به بانک‌ها و سیستم‌های مالی و کلاهبرداری از جمله انتقال متقلبانهٔ وجوه الکترونیکی، بازاریابی از راه دور به‌وسیلهٔ فیشینگ یا کلک اسپم و جرایم نقض حق مؤلف سایبری (cyber copyright) است. همچنین، جرایمی مثل زورگیری و آزار از راه سیستم‌های درون‌خط گزارش شده است. تروریسم و اینترنت نیز از جمله مسائل قابل توجه است؛ زیرا اینترنت وسیله‌ای مؤثر برای نقل و انتقال آسان منابع مالی و لجستیکی حملات تروریستی است. همچنین، از سیستم‌های اطلاعاتی به‌عنوان وسیله‌ای برای ارتکاب جرایمی مثل: تغییر داده‌ها، جعل عام و جعل پول الکترونیکی، سرقت اطلاعات، جاسوسی صنعتی و نقض حق مؤلف (cyber-related copyright) استفاده می‌شود. در نهایت اینکه هنگام مبارزه با جرایم رایانه‌ای،

۱. در این کنوانسیون، انواع جرایم عبارت‌اند از: ۱. دسترسی غیرقانونی؛ ۲. قطع و شنود غیرقانونی؛ ۳. مداخله در داده‌ها؛ ٤. مداخله در سیستم؛ ۵. سوء استفاده از وسایل؛ ٦. جعل رایانه‌ای؛ ۷. کلاهبرداری رایانه‌ای؛ ۸. پورنوگرافی کودک؛ ۹. جرایم نقض حق مؤلف و حقوق هم‌جوار؛ ۱۰. تلاش، مساعدت و معاونت؛ ۱۱. مسئولیت تضامنی؛ ۱۲. ضمانت اجراها.
در واقع، جرایم نُه‌گانهٔ نخست، اَشکال مختلف نقض امنیت سیستم‌ها محسوب می‌شود که در تکمیل روش‌های مبارزه با آن، مسائل آیین دادرسی و بین‌المللی مد نظر قرار می‌گیرد.

2. Eleventh United Nations Congress on Crime Prevention and Criminal Justice, 2005.

تعدادی از مشکلات حقوقی سد راه مراجع تعقیب، تحقیق و رسیدگی است. تعقیب و تحقیق مؤثر جرم رایانه‌ای معمولاً مستلزم ردگیری فعالیت‌های مجرمانه در سراسر ISPها و شرکت‌هاست که گاهی ورای مرزهای جغرافیای است، در نتیجه با مشکلاتی مثل صلاحیت و حاکمیت کشورها مواجه می‌شویم. پس، مبارزهٔ مؤثر با جرایم رایانه‌ای به همکاری بین‌المللی نیاز دارد که لازمه‌اش تجهیز کشورها به قانون، آیین دادرسی و ابزارهای اداری است. البته مرتکبان جرایم رایانه‌ای نیز برای مصون ماندن از تعقیب مراجع محلی، به‌طور معمول از تسهیلات برون‌مرزی استفاده می‌کنند که هم شناخته نشوند و هم در صورت شناسایی، نهادهای ذی‌صلاح را با مشکلات ناشی از قواعد صلاحیت رسیدگی مواجه سازند. در واقع، کشورهای فاقد قانون مبارزه با جرایم رایانه‌ای، سکویی برای ارتکاب جرایم سایبری در کشورهای دارای قانون شده‌اند. این مسئله بیانگر این موضوع است که کشورهای دارای قانون جرایم سایبری، در نتیجهٔ برخورداری از یک زیرساخت قانونی مناسب، اقتصاد اینترنتی قابل توجهی را به‌وجود آورده‌اند که اکنون هدف خوبی برای دستبرد و سوء استفاده محسوب می‌شوند. علاوه بر این، نکتهٔ قابل توجه اینکه مهارت مرتکبان جرایم رایانه‌ای با توجه به سطح اقدامات امنیتی فرق می‌کند. در کشورهایی که معیارهای دقیق، روشن و سخت برای حفاظت از سیستم‌ها در دو بُعد پیشگیری و تعقیب وجود دارد، برای نفوذ به سیستم، مهارت زیادی لازم است.

علاوه بر این، عناوین مجرمانه در فضای سایبر محدود به مناطقی است که تحت حفاظت قرار می‌گیرند و چون استانداردهای بحث حفاظت، از کشوری به کشور دیگر فرق می‌کند، در عمل دربارهٔ مورد فرامرزی و زمانی که بیش از یک کشور درگیر بحث شوند ـ که خیلی وقت‌ها چنین است ـ، طیف وسیعی از مشکلات نمایان می‌شود. نکتهٔ مهم در تبیین و تدوین قواعد فنی، پیش‌بینی قواعد عادلانهٔ کیفری سایبری است؛ زیرا مجازات افراد بدون آنکه شخص مرتکب در اثر مراقبت‌ها و محافظت‌های معقول سازمان‌ها و اشخاص بداند یا باید بداند که اقدام وی تلاشی مجرمانه برای به مخاطره انداختن سیستم محسوب می‌شود، ناعادلانه خواهد بود. به‌عبارت دیگر، بدون وجود معیارهای فنی امنیت سیستم‌ها، تشخیص منافع حفاظت شده از حفاظت نشده و احراز

عامدانه بودن فعل، نه کار آسانی است و نه مطابق با دادرسی عادلانه.

همچنین، دربارهٔ جرایم رایانه‌ای مسئلهٔ قابل توجه آنکه باید میان واژه‌های «کاربری نادرست رایانه» و «سوء استفاده از رایانه» به اندازهٔ کافی تفاوت قائل شد. فعل مجرمانه، فعل توأم با قصد و سوءنیت است، در نتیجه در فضای سایبر باید میان حوادث ناشی از اتفاق، بی‌مبالاتی و بی‌مبالاتی منجر به مسئولیت کیفری از یک طرف و فعل عامدانه برای سوء استفاده از سیستم، فرق گذاشت. بنابراین، لازم است امنیت چنان دقیق و عینی مدرّج شود که موارد نقض آن به سادگی قابل فهم و قابل تمییز از موارد سهل‌انگاری باشد. کدهای رفتاری، دستورالعمل‌ها، استانداردها و مقررات قانونی ـ فنی برای کمیت‌پذیر کردن مفهوم نقض امنیت، ابزاری برای قضاوت عادلانه و قابل پیش‌بینی در این عرصه است.

در هر حال باید اذعان داشت، همان‌طور که در سند کنگرهٔ یازدهم سازمان ملل (A/Conf. 203/14) تصریح شده است، تکنولوژی اطلاعات و ارتباطات به‌حدی از پیشرفت رسیده است که اکنون نه‌تنها خطری برای محرمانگی، تمامیت و در دسترس بودن سیستم‌های رایانه‌ای محسوب می‌شود، بلکه همچنین خطر مهمی برای خود زیرساخت‌های امنیتی محسوب می‌شود. مقابله با جرایم سایبری بسی فراتر از حقوق جزا، آیین دادرسی کیفری و قواعد اجراست. همکاری بین‌المللی در همهٔ سطوح میان کشورها، کشورها و ISPها، بخش‌های دولتی، خصوصی و غیردولتی؛ ارتقای سطح علمی و فنی دولت‌ها دربارهٔ تحقیقات جرایم رایانه‌ای؛ بررسی استفاده از تکنولوژی رایانه در بهره‌برداری از زنان و کودکان در مسائل پورنوگرافی؛ امکان‌سنجی تأسیس ستاد تشکیلاتی اینترنت جهانی؛ تشویق و روزآمد ساختن قوانین جرایم رایانه‌ای برای پوشش دادن انواع جرایم و قبول این واقعیت که تکنولوژی اطلاعات به هر شهروند عادی امکان می‌دهد که فاجعه‌ای در فضای سایبر به‌وجود آورد، ضرورت ایجاد بنیان‌های اخلاقی مناسب این فضا را مطرح می‌سازد.

۲ـ۳. حریم خصوصی

یکی از مهم‌ترین چالش‌های امنیت اطلاعات، حمایت از اطلاعات خصوصی افراد در فضای سایبر است. در واقع، تلاش کشورها برای حمایت از حریم زندگی خصوصی،

امروزه به‌دلیل ظهور فناوری‌های اطلاعاتی و ارتباطی نوین، مورد تهدید قرار گرفته است. برای توضیح بیشتر باید گفت در عصر فناوری اطلاعات، حمایت از حریم خصوصی، در قالب جدیدی با عنوان «حمایت از داده» شکل تازه‌ای به خود می‌گیرد و مفهوم جدیدی از حق خلوت را پوشش می‌دهد. در نتیجه، هر نوع اطلاعات که جنبهٔ شخصی دارند؛ مانند اطلاعات جسمانی، تصویر، صدا، روابط جنسی، عقاید فلسفی، مذهبی، سیاسی، ریشه‌های نژادی و قومی و حتی نوع علایق و سلیقه‌ها، به محض پذیرش از راه داده‌های الکترونیکی، باید مورد حمایت قانونگذار قرار گیرند[1] (قاجار قیونلو، ۱۳۷۹: ۷۱)؛ به‌عنوان مثال، یکی از روش‌هایی که در حوزهٔ سایبر به‌طور غیرمستقیم حریم افراد را تهدید می‌کند، سیستم‌های تأیید هویت است. در فضای سایبر، برای اینکه به اشخاص اجازهٔ ورود به محیط‌های خاص داده شود، برخی اطلاعات که شامل اطلاعات شخصی یا حتی اطلاعات شخصی حساس می‌شود، از آنها گرفته می‌شود. نگرانی‌ای که در اینجا وجود دارد، دربارهٔ امکان سوء استفادهٔ متصدیان این سایت‌ها از این اطلاعات یا امکان افشای آنهاست که به دلایل مختلف مانند فقدان سیستم امنیتی کارآمد برای حفاظت از اطلاعات، ممکن است انجام گیرد (Kent, 2004: 55). این موضوع تا آن حد جدی تلقی شده است که در سال ۱۹۹۹ در ایالات متحده برای حمایت از کودکانی که چنین اطلاعاتی از آنان گرفته می‌شود، قانون حمایت از حریم آنلاین کودکان (the children's online privacy protection act) به تصویب رسید.

۱. بخش اول قانون حمایت از داده‌های انگلستان (Data Protection Act, 1998)، در تعریف داده‌های شخصی مقرر می‌دارد: «داده‌هایی که با زندگی شخصی افراد ارتباط دارد و می‌تواند از راه معیارهای ذیل مشخص گردد: الف. از راه خودِ داده‌ها؛ ب. از راه داده‌ها یا اطلاعاتی که در اختیار کنترل‌کنندهٔ داده‌هاست یا احتمالاً قرار خواهد گرفت. همچنین، اصطلاح مذکور شامل هرگونه عقیدهٔ مرتبط با اشخاص یا هرگونه نشانه‌ای دال بر مقاصد کنترل‌کننده یا اشخاص دیگر است که با افراد مذکور مرتبط باشد.» در ضمن، در بخش دوم این قانون، داده‌های شخصی حساس تعریف شده است: «داده‌های شخصی‌ای که بر اطلاعات ذیل مشتمل باشد: الف. داده‌های مربوط به مسائل قومی و نژادی؛ ب. عقاید سیاسی؛ ج. اعتقادات مذهبی یا مانند آن؛ د. عضویت در یک اتحادیهٔ تجاری (به آن مفهوم که مشمول قانون اتحادیه‌های تجاری و روابط کارگری مصوب ۱۹۹۲ قرار گیرد)؛ هـ. شرایط فیزیکی و روانی؛ و. مسائل جنسی؛ ز. ارتکاب یا ادعای ارتکاب هرگونه جرم؛ ح. هرگونه تعقیب کیفری دربارهٔ جرایم ارتکابی یا جرایمی که ادعای ارتکاب آن به‌وسیلهٔ شخص مربوط مطرح شده باشد و همچنین هر حکمی که از سوی هر دادگاه در اثر این تعقیب صادر شده باشد».

پردازش الکترونیکی اطلاعات شخصی کـه در بحـث از حـریم خصوصـی ارتباطـات الکترونیکی، ممنوعیت‌ها و محدودیت‌هایی برای آن وضع شده است، از دید دستورالعمـل اروپایی مورخ ٢٤ اکتبر ١٩٩٥ دربـارهٔ «حمایـت از اشـخاص حقیقـی در مقابـل پـردازش داده‌های دارای وصف شخصی و آزادی جریان این داده‌هـا»، عبـارت اسـت از: «هرگونـه عملیات یا مجموعه عملیاتی که صرف‌نظر از استفاده یا عدم استفاده از روش‌های خودکار دربارهٔ داده‌های با ماهیت شخصی، از راه جمع‌آوری، ثبـت، سـازماندهی، حفـظ، تـدوین، تفسیر، استخراج، مشاوره، استفاده و مبادلهٔ آن از راه انتقال یا هر شکل دیگر، از دسترسـی، تماس یا ارتباط همزمان و نیز حذف یا انهدام، اِعمال شود».

در واقع، نخستین قانون ملی حمایت از داده‌ها در سال ١٩٧٣ در سوئد تصویب شد. همچنین، در این باره می‌توان به قانون حمایت از داده (data protection)، سـال ١٩٨٤ انگلستان که در سال ١٩٩٨ با قانونی به همین نـام جـایگزین شـد (Bainbridge, 2002: 359) اشاره کرد. غیر از کشورهایی که حمایت از داده‌های شخصی را در قالـب قواعـد حقوقی درآورده‌اند، برخی از سازمان‌های بین‌المللی از مدت‌ها پیش گام‌های مهمـی در این حقوق برداشته‌اند؛ از آن جمله می‌توان سازمان همکاری و توسعهٔ اقتصادی OECD را نام برد که در سال ١٩٧٧ اصولی را به‌منظور حمایت از داده ارائه کرده است. سازمان ملل متحد هم با توجه به پیشرفت‌های فناوری اطلاعات، به موضوع از دیـدگاه حقـوق بشر نگریسته است و در سال ١٩٩٠ رهنمودهایی برای قانونگذاری فایل‌هـای داده‌هـای شخصی رایانه‌ای ارائه کرده است، ولـی دربـارهٔ اسـناد بـین‌المللـی و منطقـه‌ای دربـارهٔ حمایت از این اصل، ابتدا باید به مادّهٔ ١٥ کنوانسیون جـرایم سـایبر اشـاره کـرد کـه بـا رویکردی عام از دول عضو خواسته است قوانین و مقررات خـود را بـرای حمایـت از حقوق و آزادی‌های بشر که در کنوانسیون شورای اروپا، میثاق بین‌المللی حقوق مدنی و سیاسی و اسناد لازم‌الاجرای بین‌المللی دیگر منعکس شده اسـت، تصـویب کننـد و بـه اجرا درآورند. علاوه بر این، باید به پارلمان و شورای اروپا اشاره کرد که از سال ١٩٧٦ فعالیت خود را برای تدوین دستورالعمل‌هایی برای کشورهای عضو دربـارهٔ حمایـت از داده‌های شخصی آغاز کرده است که به‌عنوان مثال، دستورالعمل‌های تصـویب شـده در سال‌های ١٩٩٥ و ٢٠٠٢ را می‌توان نام برد. مطـابق دسـتورالعمل اروپـایی ٩٥/٤٦ اکتبـر

۱۹۹۵ شورا و پارلمان اروپا، داده‌ها باید به‌صورت صحیح و قانونی پردازش شوند، پردازش باید متناسب و مرتبط با اهداف مورد نظر باشد و از افراط در استفاده از آنها خودداری شود، پردازش داده‌هایی که متضمن ریشه‌های نژادی، قومی، عقاید سیاسی، اعتقادات مذهبی یا فلسفی و یا تعلقات صنفی باشد و نیز پردازش داده‌های مرتبط با سلامتی و زندگی جنسی، ممنوع است، مگر با رضایت صریح ذی‌نفع در این پردازش و علاوه بر این، تکلیف اطلاع‌رسانی اشخاص که داده‌ها نزد آنان سپرده شده است، حق دسترسی افراد ذی‌نفع به داده‌های پردازش شده، حق مخالفت با پردازش داده، رازداری نسبت به داده‌های شخصی، امنیت داده‌های شخصی باید مورد توجه قرار گیرد. دستورالعمل شمارهٔ ۲۰۰۲/۵۸/CE مورخ ۱۲ ژوئیه ۲۰۰۲ با عنوان «زندگی خصوصی و ارتباطات الکترونیکی»،[1] از یک سو جانشین دستورالعمل شمارهٔ ۹۷/٦٦/CE پارلمان و شورای اروپا دربارهٔ «پردازش داده‌های شخصی و حمایت از حریم خصوصی در بخش ارتباطات از راه دور» است و از سوی دیگر، مکمل دستورالعمل اروپایی مورخ ۲٤ اکتبر ۱۹۹۵ است.[2]

در امریکا نیز ادارهٔ فدرال بازرگانی ایالات متحده (FTC)، اقداماتی در جهت افزایش اطمینان و احساس امنیت مشتری در عرصهٔ بازرگانی آنلاین انجام داده است.[3] FTC در

1. 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).

۲. ویژگی‌های این دستورالعمل در مقایسه با دستورالعمل مورخ ۲٤ اکتبر ۱۹۹۵، عبارت‌اند از: تضمین امنیت خدمات ارتباطات الکترونیکی به‌وسیلهٔ ارائه‌دهندگان خدمات اینترنتی، به‌لحاظ فنی؛ تکلیف اطلاع‌رسانی ارائه‌دهندگان خدمات اینترنتی از خطرات مرتبط با نقض امنیت شبکه؛ تضمین محرمانگی ارتباطات در خصوص داده‌های عبوری؛ لزوم بی‌نام بودن داده‌های عبوری و مستثنیات آن؛ تکلیف اطلاع‌رسانی ارائه‌دهندکان خدمات اینترنتی از اَشکال داده‌های عبوری آنها؛ لزوم ارائهٔ صورتحساب کامل از سوی ارائه‌دهندگان خدمات اینترنتی و اصل احترام به زندگی خصوصی مشترکان؛ تکلیف ارائه‌دهندگان خدمات اینترنتی دربارهٔ معرفی مورد نظر و خطوط وصل شده و محدودیت‌های آن؛ لزوم کسب رضایت برای پردازش داده‌های ثابت کاربران یا مشترکان؛ لزوم رضایت کاربر یا مشترک دربارهٔ ارتباطات ناخواسته و یا رایگان.

۳. FTC، پنج اصل مهم را با عنوان «قوانین به‌کارگیری منصفانهٔ اطلاعات» یا «اصول FTC» گسترش داد که عبارت‌اند از: آگاه‌سازی و اطلاع‌رسانی (شامل ارائهٔ هویت نهادی که اطلاعات را جمع‌آوری

جهت اقدامات مذکور، دعاوی حقوقی را نیز دربارهٔ نقـض حـریم خصوصـی و امنیـت اطلاعات اقامه کرده است (Michael A. Benoit & Joseph D. Looney)؛ از جملهٔ این دعاوی می‌تـوان بـه شـکایت FTC علیـه سـایت Geocities اشـاره کـرد. ایـن سـایت سرویس‌های بی‌شماری را به اعضای خود ارائه داده بـود کـه شـامل تخصـیص فضـای رایگان و غیررایگان و ایمیل رایگان به مشتری‌ها بود. این سایت در فرم‌های مخصوصی به جمع‌آوری اطلاعات اجبـاری و غیراجبـاری از مشـتریان خـود مبـادرت مـی‌کـرد و اطلاعاتی مانند: نام، درآمد، تحصیلات، وضعیت تأهل، سـن و... آنهـا را در یـک بانـک اطلاعاتی جمع‌آوری می‌کرد. همچنین، در این فرم‌ها از متقاضیان ثبت‌نام می‌خواست که انتخاب کننـد آیـا پیشـنهادات تبلیغـاتی بـه‌خصـوص یـا محصـولات مخصـوص و یـا سرویس‌هایی از شرکت‌های خاص را می‌خواهند دریافت کنند یا خیر. FTC شکایتی را اقامه کرد مبنی بر اینکه گردانندگان سایت مذکور چنین وانمود کرده‌انـد کـه اطلاعـات هویت شخصی افراد فقط برای ارائهٔ پیشنهادهای تبلیغاتی خاص به‌کـار گرفتـه خواهـد شد و این اطلاعات (شامل: اجباری یا اختیاری) برای هیچ‌کس بدون اجازهٔ اعضا، فـاش نخواهد شد، ولی این اطلاعات به بازاریابان (به‌عنوان عامل ثالث) فاش می‌شد و آنان از این اطلاعات برای جلب مشتری استفاده می‌کردند. سرانجام سایت Geocities اتهامات خود را پذیرفت و متعاقب آن به پذیرش موافقتنامه‌ای که شامل تعهد این سایت به عدم تکرار اقدامات موضوع شکایت و ارائهٔ فرصتی برای اعضا جهت پاک کـردن اطلاعـات مربوط به خود و الزام به گرفتن رضایت والدین قبل از دریافـت اطلاعـات از کودکـان کمتر از ۱۲ سال و برخی موارد دیگر بود، ملزم شد.

می‌کند؛ تعیین مصارف اطلاعاتی که گرفته می‌شود و...)، ایجاد حق انتخـاب و لـزوم جلـب رضـایت مشتری (حق انتخاب می‌تواند به‌صورت یک گزینـهٔ «بلـه» یـا «خیـر» و یـا گزینـه‌هـای «انتخـاب» و «صرف‌نظر» باشد که این امکان را برای مشتری فراهم سازد تا ماهیت اطلاعاتی را که ارائه می‌دهند یا نوع استفاده‌ای که نهاد جمع‌آوری‌کنندهٔ اطلاعات از آنها می‌کند، سازگار سازند)، دسترسی و مشارکت (شامل اعطای مجوز به مشـتریان دربـارهٔ دسترسـی بـه داده‌هـای مربـوط بـه خودشـان)، تمامیـت و یکپارچگی و امنیت (شامل پیش‌بینی اقدامات مدبرانه‌ای مانند ایجاد محدودیت در دسترسی کارمندان به اطلاعات شخصی و تضمین این موضوع که اطلاعات فقط در دسترس افـراد مجـاز قـرار خواهـد گرفت) و اِعمال قانون و پیش‌بینی جبران ضررهای وارده و چاره‌اندیشی دربارهٔ کاستی‌ها (برای جلب رضایت افراد صدمه دیده).

در حال حاضر جدیدترین و کارآمدترین مکانیزم‌ها، ابزارها و سـرویس‌هـای امنیتـی که برای تأمین حق گمنام ماندن و حریم خصوصی افراد به‌وجـود آمـده‌انـد، بـا عنـوان تکنولوژی‌های PET (privacy enhancing technologies) شناخته می‌شوند که به‌عنوان مثال می‌توان به تکنولـوژی‌هـای Anonymizer، LPWA (lucent personalized web assistant)، P3P (privacy preferences project)، GAP (GNUnet's anonymity protocol) و... اشاره کرد؛ مثلاً تکنولـوژی ناشـناس‌کننـده (anonymizer)، تـدابیری را برای ناشناخته ماندن کـاربران در محـیط سـایبر و آشـکار نشـدن آدرس IP آنهـا و در نهایت، عدم امکان دسترسـی بـه اطلاعـات کـاربران در نظـر گرفتـه اسـت. البتـه ایـن تکنولوژی‌ها باید همراه با راهنماهایی که برای تأمین هرچه بیشـتر امنیـت اطلاعـات در اختیار کاربران و ISPها و ESPها قرار می‌گیرد و همچنین، در کنار آگـاهی از مقـررات حقوقی این حوزه مورد استفاده قرار گیرد (Pereira, 2007: 87).

۳ـ۳. مسئولیت مدنی

علاوه بر مواردی که نقض آنها باعث مسئولیت کیفری است (سوء استفاده از رایانـه) و در قانون تجارت الکترونیکی ایران نیز به چنـد مـورد از آنهـا اشـاره شـده اسـت، نـوع دیگری از مسئولیت وجود دارد که در نتیجهٔ سهل‌انگاری و بی‌مبالاتی به‌وجـود مـی‌آیـد (کاربرد غلط رایانه) و فاعل آن، عمدی در ورود ضرر ندارد.

شایع‌ترین مشکلی که می‌تواند منجر به اقامهٔ یک دعوی مسئولیت مدنی شود، زمانی است که سازمان (الف) اقدامات مناسب امنیتی را اجرا نمی‌کند و به یکی از سیستم‌های آنان نفوذ می‌شود. سپس این سیستم ممکن است که در جهت حملـه بـه سـازمان (ب) مورد استفاده قرار گیرد. در این حالت، سازمان (الف) ممکـن اسـت در برابـر سـازمان (ب) مسئول شناخته شود. در کامن‌لا و سیستم اروپایی، پرسش این است که آیا سازمان (الف) مراقبت معقول و اقدامات مناسبی در جهـت ممانعـت از ایـن واقعـه انجـام داده است یا خیر؟ استانداردهای مواظبت و مراقبت دربارهٔ امنیت اطلاعات، مسئلهٔ پیچیده‌ای است و توصیف بیشتری نیـاز دارد؛ بـه‌عنـوان مثـال، در مـادهٔ (۲ــ ح) قـانون تجـارت الکترونیکی ایران، از سیستم اطلاعاتی مطمئن تعریف مناسبی ارائه شـده اسـت. مطـابق

این تعریف: «سیستم اطلاعاتی مطمئن (secure information system) سیستمی است که: ۱. به‌نحوی معقول در برابر سوء استفاده و نفوذ محفوظ باشد؛ ۲. سطح معقولی از قابلیت دسترسی و تصدی صحیح را داشته باشد؛ ۳. به‌نحوی معقول متناسب با اهمیت کاری که انجام می‌دهد، پیکربندی و سازماندهی شده باشد؛ ٤. موافق با رویّهٔ ایمن باشد». و در قسمت بعدی (۲ـ ط) از رویّهٔ ایمن چنین تعریفی ارائه داده است: «رویّهٔ ایمن (secure method) رویّه‌ای است برای تطبیق صحت ثبت (داده پیام)، منشأ و مقصد آن با تعیین تاریخ و برای یافتن هرگونه خطا یا تغییر در مبادله، محتوا و یا ذخیره‌سازی (داده پیام) از یک زمان خاص. یک رویّهٔ ایمن ممکن است با استفاده از الگوریتم‌ها یا کدها، کلمات یا ارقام شناسایی، رمزنگاری، روش‌های تصدیق یا پاسخ برگشت و یا راه‌های ایمنی مشابه انجام شود». در این قانون، برای نخستین بار در ایران به‌طور صریح از قاعدهٔ «عقلی» برای تعیین میزان امنیت اطلاعات استفاده شده است و به چندین دههٔ حکومت بلامنازع عرف خاتمه داده شده است. در واقع، نقش سنجش عقلانی در زمینهٔ امنیت اطلاعات، غیرقابل جایگزین با تکنیک‌های حقوقی دیگر است و براساس همین قاعدهٔ عقلانی است که دادگاه‌ها آزادانه و به‌طور قانونی برای فهم سنجش امنیت در شبکه‌ها و سیستم‌های اطلاعاتی، به استانداردهای جهانی که نمودی از خِرد جمعی عقلای یک صنعت و یا بخش است، مراجعه می‌کنند. ایزو ۱۷۷۹۹ یکی از این استانداردهای جهانی است و سازمان‌هایی که بتوانند گواهی این ایزو را به‌دست آورند، بدون تردید پیشرفت زیادی در توسعهٔ امنیت سیستم‌ها داشته‌اند. در این استاندارد، موارد متعددی از جمله سیاست امنیت، کنترل دسترسی به سیستم، مدیریت رایانه و تصدی‌گری، نگهداری و توسعهٔ سیستم، امنیت فیزیکی و محیطی، تطبیق، امنیت پرسنلی، امنیت سازمانی، ممیزی طبقه‌بندی و کنترل و مدیریت استمرار بنگاه وجود دارد که هریک به‌طور تفصیلی و دقیق، جنبه‌های گوناگون امنیت را پوشش می‌دهند. دریافت گواهی ایزو ۱۷۷۹۹ یک امتیاز بزرگ فرامرزی برای بنگاه‌ها و سازمان‌ها محسوب می‌شود و در زمینه‌ای که بیش از پیش فعالیت‌های تجارت الکترونیکی بسط و گسترش می‌یابد، مزیّن شدن به آن، یک امتیاز رقابتی محسوب می‌شود.

۴ـ۳. مدیریت مواجهه با بحران و ادلهٔ اثبات

در مرحلهٔ بعدی بروز یک فاجعهٔ امنیتی که عوامل پیشگیرانه و مقدماتی کارساز و مؤثر واقع نشدند، نوبت به مدیریت مواجه با بحران می‌رسد. در این مرحله باید از فناوری‌های امنیت اطلاعات واکنشی استفاده کرد. در واقع، غرض از «واکنشی»، انجام عکس‌العمل لازم پس از وقوع یک مشکل خاص امنیتی است. در چنین مواردی به موضوعاتی اشاره می‌شود که ما را در مقابله با یک مشکل، پس از وقوع آن کمک خواهند کرد؛ از جملهٔ این تکنیک‌ها ـ همان‌گونه که قبلاً نیز اشاره شد ـ می‌توان به دیوار آتش، کنترل دسترسی، کلمات عبور، زیست‌سنجی و به‌ویژه نظام‌های آشکارسازی نفوذی و واقعه‌نگاری اشاره کرد.[1]

در این مقطع است که کار ادارهٔ حقوقی، وکلا و سیستم دادگستری نیز آغاز می‌شود. در کشورهایی که قانون جرایم رایانه‌ای، آیین دادرسی رایانه‌ای و مقررات فنی ـ حقوقی وجود دارد، بلافاصله پس از تماس با پلیس، اقدامات لازم برای تأمین دلایل انجام خواهد شد. تا این فاصله، سازمان باید اقداماتی مثل قرنطینه کردن سیستم تا زمان رسیدن مأموران را انجام دهد. در سیستم‌های حقوقی که معیارهای حرفه‌ای بنگاه‌های اقتصادی از قدمت زیادی برخوردار است، انجام فراگردهای معمول کاری ــ اداری از استحکام کافی برای ارائه به دادگاه، به‌عنوان دلیل برخوردار است، ولی در کشورهایی مثل ایران که مفهوم فراگرد معمول اداری ـ کاری به اندازهٔ کافی کمیت‌پذیر نشده است، معمولاً باید اقدامات تأمین دلیل ـ حفظ ادلهٔ جرم را که یک فعالیت قضایی است، انجام داد.

---

۱. به‌عنوان مثال، دیوار آتش یک ابزار نرم‌افزاری است که به‌عنوان فیلتر، مانع یا گلوگاه میان یک سازمان داخلی یا شبکهٔ امین و شبکه غیرامین (اینترنت) قرار می‌گیرد و هدف آن جلوگیری از ارتباطات غیرمجاز در درون یا بیرون شبکهٔ داخلی سازمان یا میزبان است (Oppliger, 1998: 58) و نظام‌های آشکارسازی نفوذی، نظامی تدافعی است که فعالیت‌های خصمانه را در یک شبکه تشخیص می‌دهد و نکتهٔ کلیدی در آنها، تشخیص و احتمالاً جلوگیری از فعالیت‌هایی است که ممکن است امنیت شبکه را به‌خطر بیاندازند. در واقع، نظام‌های آشکارساز نفوذی، فرایندی برای شناسایی و تقابل با فعالیت‌های مشکوک است که منابع رایانه‌ای و شبکه‌ها را هدف قرار داده‌اند. علاوه بر این، ابزارها و تجهیزات این نظام می‌توانند میان تهاجم‌های داخلی (از داخل سازمان به‌وسیلهٔ کارمندان یا مشتریان) و تهاجم‌های خارجی (حملاتی که به‌وسیلهٔ هکرها انجام می‌شود) تمایز قائل شوند (اسدی، ۱۳۸٤، ۹۳).

نکتهٔ مهم اینکه در کشورهای حقوق نوشته از جمله ایران که از سیستم دلایل معنوی در محاکمات جزایی پیروی می‌کنند، هر نوع دلیلی برای کشف حقیقت استفاده می‌شود. بنابراین، تحقیق و تحصیل اطلاعات به‌نحو الکترونیکی، اصولاً قابل پذیرش است. این مورد به‌خصوص در مقررات این کشورها که تفتیش و توقیف را نسبت به هر «چیز» قابل اِعمال می‌دانند (مادهٔ ٥٤ قانون آیین دادرسی کیفری فرانسه و فصل ۱۰۳ آیین دادرسی کیفری آلمان)، کارکرد دارد. با این وجود، مشکل بزرگی وجود دارد که قانون آیین دادرسی کیفری معمولاً مناسب با تفتیش، توقیف و کشف جرم در اشیای مادی و محسوس است.[1] در واقع، باید به این موضوع اذعان داشت که نظام‌های سنّتی آیین دادرسی کیفری نمی‌تواند پاسخ‌گوی مسائل جدیدی باشد که در زمینهٔ جمع‌آوری و ارائهٔ دلایل مطرح می‌شود و در این رابطه، به‌خصوص تفتیش و توقیف داده‌های ذخیره یا پردازش شده در سیستم‌های رایانه‌ای، یکی از مهم‌ترین مباحث مربوط به تحصیل دلایل است، ولی نکته اینجاست که تخصصی بودن عملیات تفتیش و توقیف در محیط‌های سایبر، یک فرض قطعی است که در غیر این صورت، مأموران قضایی نمی‌توانند در مواقع ضروری اقدام شایسته‌ای در تحصیل ادلهٔ رایانه‌ای انجام دهند. بنابراین، آموزش نیروی ویژهٔ این کار الزامی است.

علاوه بر این، اعتباری که به ادلهٔ رایانه‌ای در سیستم قضایی داده می‌شود نیز از اهمیت به‌سزایی برخوردار است؛ یعنی در دعاوی حقوقی، ادلهٔ اثبات دعوی فقط در قالب‌های خاص اقرار، اسناد کتبی، شهادت، امارات و قسم، قابل قبول‌اند.[2] دربارهٔ ادلهٔ رایانه‌ای در برخی کشورها برای آنکه جنبهٔ استنادپذیری مناسبی در قالب ادلهٔ رایج در قوانین حقوقی به آن بدهند، آن را در حکم سند قرار داده‌اند (قاجار قیونلو، ۱۳۷٤: ٤٧).

۱. به‌عنوان مثال، طبق فصل سوم قانون آیین دادرسی کیفری ۱۳۷۸: تفتیش و بازرسی منازل، اماکن، اشیاء، اسباب، آلات و دلایل جرم، همگی ظهور در اشیای مادی و محسوس دارد و حتی آنجا که به مسئلهٔ اطلاعات صِرف توجه می‌شود، می‌گوید: از اوراق و نوشته‌ها و اشیای دیگر متعلق به متهم، فقط آنچه که مربوط به واقعهٔ جرم است، تحصیل و در صورت لزوم به شهود تحقیق ارائه می‌شود و قاضی مکلف است دربارهٔ نوشته‌های دیگر و اشیای متعلق به متهم، با کمال احتیاط رفتار کند و باعث افشای مضمون و محتوای آنها که ارتباط به جرم ندارد، نشود (مادهٔ ۱۰۱ قانون آیین دادرسی کیفری).
۲. مادهٔ ۱۲۵۸ قانون مدنی.

البته می‌توان در قالب اماره و یا رجوع به‌کارشناسی نیز به این ادله استناد کرد. رجوع به‌کارشناسی در مواردی پیش می‌آید که دادرس با مسائلی مواجه می‌شود که تشخیص و اظهارنظر در مورد آن، رأساً از طرف وی امکان‌پذیر نباشد و باید با همکاری متخصصان فن به آن مبادرت ورزد (صدرزاده افشار، ۱۳۷۳: ۱۶۱).

بنابراین، به‌نظر می‌رسد بهترین راه برای فائق آمدن بر مشکلات مزبور، در نظر گرفتن ادلهٔ سایبری به‌صورت مجزا به‌عنوان گونه‌ای جدید از ادله و متعاقب آن، پیش‌بینی مقررات خاص در موارد مربوطه، از جنبه‌های مختلف آیین دادرسی از جمله مسائل مربوط به صلاحیت، جمع‌آوری ادلهٔ الکترونیکی و سایبری و نگهداری و ارائهٔ آنها و استنادپذیری ادلهٔ مذکور و مباحث دیگر مربوط به آنهاست. خوشبختانه این مهم در بخش دوم قانون جرایم رایانه‌ای مورد توجه قرار گرفته است، به این صورت که در فصل اول از این بخش، مسائل مربوط به صلاحیت در این حوزه توجه می‌شود و در فصل دوم، با عنوان جمع‌آوری ادلهٔ الکترونیکی، مقررات مربوط به نگهداری داده‌ها، حفظ فوری داده‌های رایانه‌ای ذخیره شده در موارد لازم، ارائهٔ داده‌ها، تفتیش و توقیف داده‌ها و سیستم‌های رایانه‌ای و مخابراتی و استنادپذیری ادلهٔ الکترونیکی، بیان شده است.

نتیجه

ابعاد حقوقی امنیت اطلاعات شبکه و یا حقوق مرتبط با امنیت اطلاعات شبکه به‌دلیل گوناگونی اصول حاکم بر آن، به سختی تن به تعریفی مشخص و قابل قبول می‌دهد و معمولاً به‌واسطهٔ شناخت پدیده‌های بیرونی‌اش به آن می‌شود. به‌دلیل همین گوناگونی، موارد ذیل به‌طور اجمالی توجه شده است:

اصول و مبانی «پیشینی» امنیت در حقوق ایران به اندازهٔ کافی مدوّن و روشن نیست. نه‌تنها همهٔ جنبه‌های آن در قانون اساسی کشورمان ذکر نشده است، بلکه در مرحلهٔ سیاست‌های کلی نظام و قوانین موضوعه، این ابهام رفع نشده است. در نتیجه نمی‌توان از وضعیت فعلی، رویکردی برای قانونگذاری صحیح در عرصهٔ قانونمند ساختن جریان اطلاعات در فضای سایبر ـ جز تا حدی در زمینهٔ اطلاعات اداری و نظامی ـ بهره جست.

هرچند توسعهٔ روزافزون فناوری اطلاعات و ظهور جامعهٔ اطلاعـاتی، دسـتاوردهای فوق‌العاده مهمی را برای بشر به ارمغان آورده است، ولی تهدیدهای بسـیاری در حـوزهٔ امنیت اطلاعات شبکه و سیستم اطلاعـات افـراد وجـود دارد کـه مشـکلات پیچیـده و متعددی را به‌وجود می‌آورد. فضـای سـایبر بهتـرین مکـان بـرای اسـتفادهٔ مجـرمین در دستیابی به اطلاعات افراد است. با توجه به اینکه اطلاعات شخصی و حتی دولتی و نظامی بسیاری در این فضا جابه‌جا می‌شود، امکان قرار گرفتن این اطلاعـات در اختیـار مجـرمین افزایش می‌یابد و چون باعث تهدید امنیت جامعه و دولـت مـی‌شـود، بـا ابزارهـای سـنّتی نمی‌توان با آن مقابله کرد. برای رویارویی با تهدیداتی که سلامت و امنیت فضای سـایبر بـا آن مواجه است، سه رویکرد وجود دارد که شامل جرم‌انگاری با توسـل بـه قـانون؛ ایجـاد قانون ویژهٔ جرایم رایانه‌ای و ایجاد و به‌کـارگیری تـدابیر حفـاظتی و کنترلـی و پیشـگیری وضعی و اجتماعی از این تهدیدات است. تدابیر حفاظتی و کنترلی نیز شـامل بـه‌کـارگیری فناوری‌های امنیت اطلاعات کنش‌گرایانه و واکنشی است. رویکرد پیشگیری نیز با آمـوزش کاربران و توانمندسازی و آگـاه کـردن آنهـا در برابـر تهدیـدات و همچنـین بـه‌کـارگیری فناوری‌هایی مانند رمزنگاری، دسترسـی محـدود و... امکـان‌پـذیر اسـت. در واقـع، امنیـت اطلاعات در فضای سایبر فقط در گرو همکاری متقابل همـهٔ بـازیگران ایـن حـوزه یعنـی کاربران اینترنت، ارائه‌دهندگان سرویس‌های اینترنتی (ISP) و ارائه‌دهندگان سرویس‌های از راه دور (ESP)ها و روزآمد بودن اطلاعات همهٔ این گروه‌هـا دربـارهٔ اقـدامات تکنیکـی و حقوقی مرتبط با حمایت از حریم خصوصی اطلاعات در این حوزه است.

علاوه بر مواردی که نقض آنها باعث مسئولیت کیفری می‌شود (سوء استفاده از رایانه)، نوع دیگری از مسئولیت وجود دارد که در نتیجهٔ سهل‌انگاری و بی‌مبالاتی به‌وجود می‌آیـد (کاربرد غلط رایانه) و فاعل آن، عمدی در ورود ضرر ندارد. در این بـاره تعیـین معیـار معقـول و مناسـب بـودن اقـدامات بـرای تشـخیص قابلیـت اسـتناد ضـرر وارده بـه ارائه‌دهندگان خـدمات سـایبری و همچنـین سـازمان‌هـا و ادارات مربوطـه، از اهمیـت بسیاری برخوردار است. با اینکه در حقوق سنّتی ایران این معیارها با توجه به عرف تعیین می‌شوند، ولی خوشبختانه در قانونگذاری‌های جدید ماننـد قـانون تجـارت الکترونیکـی، سعی شده است تا تعریف‌های مشخصی از معقول و مناسب بودن اقدامات شود.

پدید آمدن اَشکال جدید جرایم رایانه‌ای و سایبری و تفاوت ماهوی آنها با جرایم دیگر، باعث می‌شود تا رسیدگی به دعاوی مربوط به آنها با قوانین عادی، باعث بروز مشکلاتی از لحاظ تطبیق مصادیق و بررسی عناصر مادی و معنوی جرم با رفتار مورد نظر شود. بنابراین، نبودِ زیرساخت کلید عمومی (public key infrastructure–PKI) در این باره، عدم وجود دستورالعمل‌های قانونی، کدهای رفتاری (codes of conduct)، استانداردها، مرجع مشخص برای اعلام و توسعهٔ استانداردها، نبودِ نیروهای متخصص در سیستم قضایی، پلیسِ آموزش‌دیده و همچنین، نبودِ دادگاه‌های تخصصی برای رسیدگی به دعاوی انفورماتیک و عام بودن نحوهٔ رسیدگی و عدم وجود آیین دادرسی کیفری ویژهٔ جرایم رایانه‌ای و مخصوصاً بستر تجارت الکترونیکی و در پیشرفته‌ترین وضعیت، فقدان دادرسی سایبری از نقایص دیگری است که می‌توان به آنها اشاره کرد. این امر، لزوم تصویب هرچه سریع‌تر قانون مربوط به جرایم رایانه‌ای را روشن می‌سازد.

منابع

۱. *اسدی، مریم؛* «فناوری‌های امنیت اطلاعات: با یک دیدگاه طبقه‌بندی»؛ **علوم اطلاع‌رسانی**، دورهٔ ۲۰، ش ۱ و ۲، بهار و تابستان ۱۳۸٤.

۲. *انزالی، امیراسعد؛* **رایانه‌های امروزی**؛ تهران: مجتمع فنی تهران، ۱۳۷٤.

۳. *انصاری، ولی‌الله؛* **مجموعهٔ قوانین دربارهٔ حقوق اطلاعات (گردآوری و تنظیم)**؛ دبیرخانهٔ شورای عالی انفورماتیک کشور، تهران، بهمن ۱۳۷٤.

٤. *حسینی، بیژن؛* **جرایم اینترنتی علیه اطفال و زمینه‌های جرم‌شناسی آن**؛ پایان‌نامهٔ کارشناسی ارشد، دانشگاه آزاد اسلامی، واحد علوم و تحقیقات، ۱۳۸۲.

۵. *دزیانی، محمدحسن؛* «ابعاد جزایی کاربرد رایانه و جرایم رایانه‌ای»؛ **خبرنامهٔ انفورماتیک شورای عالی انفورماتیک کشور**، ش ۵۸، دی و اسفند ۱۳۷۳.

٦. *دزیانی، محمدحسن؛* **جرایم رایانه‌ای**؛ ج ۱، دبیرخانهٔ شورای عالی انفورماتیک، تهران، ۱۳۷٦.

۷. *دزیانی، محمدحسن؛* «مقدمه‌ای بر ماهیت و تقسیم‌بندی تئوریک جرایم رایانه‌ای (سایبری)»، **خبرنامهٔ انفورماتیک**، ش ۸۷، تهران، ۱۳۸۳.

۸. *دلماس مارتی، می‌ری؛* **نظام‌های بزرگ سیاست جنایی**، ترجمه: علی‌حسین نجفی ابرندآبادی، ج ۲، تهران: بنیاد حقوقی میزان، ۱۳۸۷.

۹. *جلالی فراهانی، امیرحسین؛* «پیشگیری وضعی از جرایم سایبر در پرتو موازین حقوق بشر»، **فصلنامهٔ فقه و حقوق**، قم، سال دوم، پاییز ۱۳۸٤.

۱۰. *سازمان ملل؛* **نشریهٔ بین‌المللی سیاست جنایی**، ترجمه: دبیرخانهٔ شورای عالی انفورماتیک، تهران: سازمان برنامه و بودجهٔ کشور، ۱۳۷٦.

۱۱. *عبداللهی ازگمی، محمد؛* **طراحی و پیاده‌سازی سرویس‌های امن برای شبکه‌های رایانه‌ای** (پایان‌نامهٔ کارشناسی ارشد)، تهران: دانشگاه صنعتی شریف، ۱۳۷۵.

۱۲. *قاجار قیونلو، سیامک؛* «ابعاد حقوقی کاربرد رایانه، حریم خصوصی، حمایت از داده»؛ **خبرنامهٔ انفورماتیک**، ش ۷٤، سال پانزدهم، تهران، اردیبهشت ۱۳۷۹.
۱۳. *قاجار قیونلو، سیامک؛* «ادلهٔ اثبات در محیطهای دیجیتال»؛ **شورای عالی انفورماتیک کشور**، تهران: چاپ محدود، ۱۳۷٤.
۱٤. *صدرزاده افشار، سیدمحسن؛* **ادلهٔ اثبات دعوی در حقوق ایران**؛ ۱۳۷۳.
۱۵. *هاشمیان، وحید؛* **روش‌های رمزنگاری اطلاعات**؛ تهران: رایانهٔ شریف، ۱۳۷۹.
۱٦. *یزدی، ابراهیم؛* **دکترین امنیت ملی**، چاپ اول، انتشارات سرایی، ۱۳۸٤.
17. "[ITU] WSIS Thematic Meeting on Cybersecurity Document: CYB/05 10" June 2005.
18. "97/66/EC of the European Parliament," concerning the processing of personal data and the protection of privacy in the telecommunications sector. Council of 15 December 1997.
19. "Civil evidence act" 1968.
20. "Computers & Security" Electronic version in Elsevier Database, 22 (4), 299 ـ 307, 2006.
21. "Directive 2002/58/EC of the European Parliament" concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Council of 12 July 2002.
22. "Directive 96/9/EC of the European Parliament and of the Council of on the legal protection of databases" 11 March 1996
23. "Measures to Combat Computer ـــ related Crime" Eleventh United Nations Congress on Crime Prevention and Criminal Justice, A/CONF, 203/14, Vol, Eleventh, Workshop 6, Bangkok: United Nations, 18 ـ 25 April 2005.

24. "Model Law on Electronic Commerce with Guide to Enactmen. s. l." UNCITRAL, 1996.
25. "OECD Guidelines for the Security of Information Systems," 1992.
26. "OECD. Computer ـــ Related Crime: Analysis of Legal Policy, ICCP. s. l.: OECD, 10" 1986.
27. "The ISO 17799 Directory".
28. "The present OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security were adopted as a Recommendation" the OECD Council at its 1037th Session, July 25, 2002.
29. "UNCITRAL Model Law on Electronic Commerce with Guide to Enactment" 1996.
30. "UNCITRAL Model Law on Electronic Signatures with Guide to Enactment", 2001.
31. "UNCITRAL Model Law on Electronic Signatures with Guide to Enactment", 2001.
32. David, Bainbridge, Inroduction to computer law, Fourth Edition, Longman ed, 2002.
33. Gerald, ferrera and others, Cyber law, south ـ western college pub, 2001.
34. Green Paper on Public Sector Information in the Information Society, EUROPEAN COMMISSION COM, 585, 1998.
35. International review of criminal policy ـــ United Nations Manual on the prevention and control of computer ـــ related crime.
36. Kent, Stephen and I. Millett Lynette, Who Goes There? Authentication Through the Lens of Privacy, National Academy Press, 2004.
37. King, C. M., Dalton, C. E., & Osmanoglu, Security

Architecture: Design Deployment and Operations, T. E. London: McGraw _ Hill, 2001.

38. Maiwald, E., & Sieglein, w. Security planning & disaster recovery, Osborne: McGraw _ Hill, 2002.
39. Maiwald, Eric, "Legal Issues in Information Security" In Fundamentals of Network Security, chapter 5. 2004.
40. Michael A. Benoit & Joseph D. Looney, "Recent Federal Privacy Initiatives Affecting The Electronic Delivery of Financial Services".
41. Oppliger, R. Internet & Intranet security, Boston: Artech House, 1998.
42. Pereira, Mario Freire & Manuela, Encyclopedia of Internet Technologies and Applications. Hershey, New York: Information Science reference, 2007.
43. University of, California, Business and Finance Bulletin. IS_3 Electronic Information Security, 2008.
44. Venter, H. S., & Eloff, J. H. P. A taxonomy for information security technologies. 2003.