حفاظت از داده‌های کاربران: رویکردهای جهانی و گونه‌شناسی تنظیم مقررات

کد موضوعی: ۲۸۰
شماره مسلسل: ۱۵۸۶۴
خردادماه ۱۳۹۷

معاونت پژوهش‌های زیربنایی و امور تولیدی
دفتر: مطالعات ارتباطات و فناوری‌های نوین

به نام خدا

فهرست مطالب

حفاظت از داده‌های کاربران: رویکردهای جهانی و گونه‌شناسی تنظیم مقررات

چکیده

فضای مجازی زندگی انسان را بیشتر از هر چیز دیگری دستخوش تغییرات ساخته است. هرچند بسیاری از این تغییرات موجب بهبود زندگی انسان شده‌اند، اما پیامدهای استفاده از فضای مجازی همیشه مثبت و مفید نبوده‌اند. حریم خصوصی افراد را می‌توان به دیواری تشبیه کرد که سرتاسر زندگی آنان را دربر گرفته است و تنها خود آنها و نزدیکانشان از داخل آن اطلاع دارند؛ یکی از مهمترین پیامدهای استفاده از فضای مجازی و عصر دیجیتال این است که این دیوار را شفاف و شفاف‌تر ساخته است؛ به‌نحوی که بسیاری از جنبه‌های پنهان زندگی آنان قابل رؤیت شده است. با وجود این قانونگذاری و تنظیم مقررات در عرصه حفاظت از داده‌های کاربران با توجه به نفوذ فناوری اطلاعات در کاربردهای مختلف و توسعه فضای مجازی اهمیت زیادی یافته و نیازمند اقدامات سیاستی است. در این گزارش با بررسی اسناد و مدارک بین‌المللی و منطقه‌ای حریم خصوصی و حفاظت از داده‌های کاربران به رویکردهای جهانی در عرصه قانونگذاری و گونه‌شناسی تنظیم مقررات در این عرصه پرداخته می‌شود.

مقدمه

تغییر زندگی شهروندان از «زندگی خصوصی» به «زندگی عمومی» از مهمترین پیامدهای عصر اطلاعات است. امروزه سازمان‌های عمومی و خصوصی صاحب‌نفوذ، سازمان‌های اطلاعاتی و جاسوسی و شرکت‌های بزرگ اینترنتی می‌توانند در کسری از ثانیه داده‌های مربوط به خصوصی‌ترین اطلاعات یک فرد، همچون اطلاعات مربوط به وضعیت سلامت جسم و روان، دارایی‌های مالی و بانکی، سوابق تحصیل، سوابق سفرهای خارج و... دسترسی پیدا کنند. اطلاعاتی که وی حتی از اینکه چه هنگام و توسط چه کسی گردآوری شده یا مورد استفاده قرار گرفته خبردار نیست. تنها راه ممکن برای صیانت از حریم خصوصی کاربران فضای مجازی همانا ضابطه‌مندسازی آن است.

اعلامیه جهانی حقوق بشر در بند «۳» چنین می‌گوید: «هر فردی حق زندگی، آزادی و امنیت شخصی دارد» و در بند «۱۲» نیز آمده است: «نباید در زندگی خصوصی، امور خانوادگی، اقامتگاه یا مکاتبات هیچ‌کس مداخله‌های خودسرانه صورت گیرد یا به شرافت و آبرو و شهرت کسی حمله شود در برابر چنین مداخله‌هایی، برخورداری از حمایت قانون، حق هر شخصی است» (اعلامیه جهانی حقوق بشر، ۱۹۴۸). در اعلامیه حقوق بشر اسلامی مصوب ۱۴ محرم ۱۴۱۱ قمری در قاهره نیز در بند «۱۸» قسمت «ب» در راستای توجه به حریم خصوصی آمده است: «هر انسانی این حق را دارد که در امر زندگی خصوصی خود استقلال داشته باشد و جاسوسی یا نظارت بر او و مخدوش کردن حیثیت او جایز نیست و باید از او در مقابل هرگونه دخالت زورگویانه حمایت شود» (اعلامیه حقوق بشر اسلامی قاهره، ۱۹۹۰).

سابقه حفاظت از داده‌های کاربران در اسناد بین‌المللی به سالیان اخیر بازمی‌گردد. سازمان ملل متحد در دسامبر ۲۰۱۳ میلادی به‌اتفاق آرا، رأی به گنجاندن حق حفظ حریم خصوصی کاربران در فضای مجازی به‌عنوان یکی از بندهای حقوق بشر داده است تا انسان‌ها از حقوق زیر برخوردار شوند: الف) هرگونه ارتباطات برخط آنها مورد احترام قرار گرفته و حفاظت شود؛ ب) از تجاوز به حریم خصوصی آنها جلوگیری شده و قوانین ملی کشورها با حق حفظ حریم خصوصی آنان سازگاری داشته باشد؛ ج) فرآیندها، رویه‌ها و قوانین نظارت بر انتقال اطلاعات و جمع‌آوری داده‌های شخصی باید با حق حفظ حریم خصوصی اطلاعاتی افراد تطابق داشته باشد؛ د) مکانیسم‌هایی برای اطمینان از شفافیت و مناسب بودن اقدامات دولت‌ها در نظارت بر انتقال و جمع‌آوری داده‌های شخصی افراد به‌وجود آید (شیروود،[1] ۲۰۱۳). هرچند حق داشتن حریم خصوصی برای شهروندان در بسیاری از اسناد بین‌المللی ذکر شده و دولت‌های مختلف موافقت خود را با آن اسناد اعلام کرده‌اند، اما بسیاری از کشورهای جهان در عمل، در قوانین داخلی خود چنین حقی را برای شهروندان خود قائل نشده‌اند. در این گزارش با بررسی استاد بین‌المللی و منطقه‌ای در حوزه حمایت از داده‌های کاربران در فضای مجازی به رویکردهای جهانی متداول و گونه‌شناسی رفتار کشورها در زمینه قانونگذاری پرداخته می‌شود.

1. Sharwood

۱. حفظ حریم خصوصی شهروندان و حفاظت از داده‌های کاربران در اسناد منطقه‌ای و بین‌المللی

حفظ حریم خصوصی شهروندان و حفاظت از داده‌های کاربران در اسناد منطقه‌ای و بین‌المللی بسیار مورد توجه قرار گرفته است. برخی از اسناد بین‌المللی عبارتند از: ۱. اعلامیه جهانی حقوق بشر[1] (۱۰ دسامبر ۱۹۴۸)؛[2] ۲. کنوانسیون اروپایی حمایت از حقوق بشر و آزادی‌های اساسی[3] (۴ نوامبر ۱۹۵۰) (گریر،[4] ۲۰۰۶)؛ ۳. عهدنامه بین‌المللی حقوق مدنی و سیاسی[5] (۱۶ دسامبر ۱۹۶۶)؛[6] ۴. اعلامیه تهران یا کنفرانس بین‌المللی حقوق بشر (۱۳ می ۱۹۶۸)؛[7] ۵. کنوانسیون آمریکایی حقوق بشر[8] (۲۲ نوامبر ۱۹۶۹) (پائول،[9] ۲۰۱۱)؛ ۶. کنوانسیون حقوق کودک[10] (۲۰ نوامبر ۱۹۸۹)؛[11] ۷. اعلامیه اسلامی حقوق بشر قاهره[12] (۵ اوت ۱۹۹۰)؛[13] ۸. راهنمای حفاظت از داده اتحادیه اروپا[14] (۱۹۹۵)؛ ۹. دستورالعمل اتحادیه اروپا در حمایت از اشخاص حقیقی در مقابل پردازش داده‌های

1. Universal Declaration of Human Rights
2. http://www. un. org/en/universal-declaration-human-rights/index. html
3. Convention for the Protection of Human Rights and Fundamental Freedoms
4. Greer
5. International Covenant on Civil and Political Rights
6. https://treaties. un. org/Pages/ViewDetails. aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=en
7. http://www. humanrights-iran. ir/news. aspx?id=16611
8. American Convention on Human Rights
9. Paúl
10. Convention on the Rights of the Child
11. http://www. ohchr. org/en/professionalinterest/pages/crc. aspx
12. Cairo Declaration on Human Rights in Islam
13. www. umn. edu/humanrts/instree/cairodeclaration. html
14. EU Data Protection Directive

شخصی و گردش آزاد داده (۱۹۹۵)؛[1] ۱۰. دستورالعمل اتحادیه اروپا در حمایت از حریم خصوصی و ارتباطات الکترونیک (۲۰۰۲)؛[2] ۱۱. دستورالعمل نگهداری داده‌های شخصی تولید و پردازش شده در چارچوب تأمین خدمات ارتباطی الکترونیکی(۲۰۰۶)؛[3] ۱۲. اعلامیه حقوق بشر سازمان ملل (بازبینی در سال ۲۰۱۳).

۱-۱. اعلامیه جهانی حقوق بشر[4] (۱۰ دسامبر ۱۹۴۸)

مهمترین اعلامیه‌ای که حق حفظ حریم خصوصی شهروندان را به رسمیت شناخته است، اعلامیه جهانی حقوق بشر است که در دهم دسامبر ۱۹۴۸ در مجمع عمومی سازمان ملل متحد مورد تصویب قرارگرفته است. در این اعلامیه در دو ماده به مبحث حفظ حریم خصوصی شهروندان پرداخته شده است:

ماده (۱) ــ همه انسان‌ها آزاد به دنیا می‌آیند و از نظر حیثیت و حقوق با یکدیگر برابرند؛ همه دارای عقل و وجدان بوده و باید نسبت به همه با روح برادری رفتار نمایند.

ماده (۱۲) ــ هیچ‌کس نباید در زندگی شخصی، امور خانوادگی، محل زندگی یا مکاتبات خود مورد دخالت‌های خودسرانه قرار گیرد و آبرو و حیثیتش مورد تعرض قرار گیرد. همه انسان‌ها حق دارند در برابر چنین مداخله‌ها و تعرضاتی مورد حمایت قانون قرار گیرند.[5]

1. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046
2. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002L0058
3. http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32006L0024
4. Universal Declaration of Human Rights
5. http://www. un. org/en/universal-declaration-human-rights/index. html

۲-۱. کنوانسیون اروپایی حمایت از حقوق بشر و آزادی‌های اساسی[1] (۴ نوامبر ۱۹۵۰)

این کنوانسیون در تاریخ ۴ نوامبر ۱۹۵۰ مورد تصویب کشورهای اروپایی قرار گرفت. در ماده (۸) این کنوانسیون آمده است:

۱. هر فردی حق دارد تا حریم زندگی خصوصی و خانوادگی، منزل و مکاتباتش حفظ شود.

۲. مرجع عمومی نباید هیچ‌گونه مداخله‌ای در اعمال این حق کند مگر آنچه طبق قانون بوده و در حفظ نظم و پیشگیری از جرائم، حمایت از حقوق و آزادی‌های افراد (جامعه) ضروری باشد (گریر،[2] ۲۰۰۶).

۳-۱. عهدنامه بین‌المللی حقوق مدنی و سیاسی[3] (۱۶ دسامبر ۱۹۶۶)

این میثاق بین‌المللی در تاریخ ۱۶ دسامبر ۱۹۶۶ به تصویب مجمع عمومی سازمان ملل رسید. در ماده (۱۷) این میثاق آمده است:

۱. هیچ‌کس نباید در زندگی خصوصی و خانواده، محل زندگی یا مکاتبات مورد مداخله غیرقانونی (بدون داشتن مجوز قانونی) قرار گیرد و نیز آبرو و اعتبار وی نباید مورد تعرض غیرقانونی واقع شود.

۲. هرکس حق دارد در برابر چنین مداخله‌ها یا تعرضاتی مورد حمایت قانون قرار گیرد.[4]

---

1. Convention for the Protection of Human Rights and Fundamental Freedoms
2. Greer
3. International Covenant on Civil and Political Rights
4. https://treaties. un. org/Pages/ViewDetails. aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=en

۱-۴. اعلامیه تهران یا کنفرانس بین‌المللی حقوق بشر (۱۳ می ۱۹۶۸)

این کنفرانس در تاریخ ۱۳ می ۱۹۶۸ در تهران برگزار شد. در بند «۱۸» این اعلامیه آمده است: «درحالی‌که اکتشافات علمی و پیشرفت‌های فناوری موجب گشوده شدن افق‌های وسیعی برای پیشرفت‌های اقتصادی و اجتماعی و فرهنگی شده است، امکان دارد که همین پیشرفت‌ها، حقوق و آزادی‌های افراد را به مخاطره افکند، لذا باید مورد توجه مداوم قرار گیرد».[1]

۱-۵. کنوانسیون آمریکایی حقوق بشر[2] (۲۲ نوامبر ۱۹۶۹)

کنوانسیون آمریکایی حقوق بشر در تاریخ ۲۲ نوامبر ۱۹۶۹ در کاستاریکا به تصویب رسید. در ماده (۱۱) این کنوانسیون بر موضوع حفظ حریم خصوصی افراد تأکید شده است:

۱. هر فردی حق دارد که شرافتش حفظ شده و حیثیتش به رسمیت شناخته شود.

۲. نباید در زندگی خصوصی، خانوادگی، منزل یا مکاتبات افراد دخالت خودسرانه شده یا به آبرو و حیثیت افراد به‌صورت غیرقانونی تعرض کرد.

۳. همه افراد حق دارند در برابر چنین مداخله‌هایی یا تعرضاتی مورد حمایت قانون قرار گیرند (پاول،[3] ۲۰۱۱).

1. http://www. humanrights-iran. ir/news. aspx?id=16611
2. American Convention on Human Rights
3. Paúl

۶-۱. کنوانسیون حقوق کودک[1] (۲۰ نوامبر ۱۹۸۹)

در این کنوانسیون حق حفظ حریم خصوصی کودکان و نوجوانان به رسمیت شناخته شده است. طبق ماده (۱۶) این کنوانسیون:

۱. در امور خصوصی، خانوادگی یا مکاتبات هیچ کودکی نمی‌توان خودسرانه یا غیرقانونی دخالت یا تعرض کرد.

۲. کودک باید در مقابل چنین دخالت‌ها یا تعرضاتی مورد حمایت قانون واقع شود.[2]

۷-۱. اعلامیه اسلامی حقوق بشر قاهره[3] (۵ اوت ۱۹۹۰)

این اعلامیه را اعضای سازمان کنفرانس اسلامی در سال ۱۹۹۰ در قاهره مصر تنظیم کردند. طبق ماده (۱۸) این اعلامیه:

الف) هر انسانی حق دارد که نسبت به جان و دین و خانواده و ناموس و مال خویش در آسودگی زندگی کند.

ب) هر انسانی حق دارد که در امور زندگی خصوصی خود (مسکن، خانواده، مال و ارتباطات) استقلال داشته باشد. جاسوسی یا نظارت بر وی یا مخدوش کردن حیثیت او جایز نیست و باید از شئونات او در مقابل هرگونه دخالت زورگویانه حمایت شود.

ج) مسکن در هر حالی حرمت دارد و نباید بدون اجازه ساکنان آن یا به‌صورت غیرمشروع وارد آن شده و نباید آن را خراب یا مصادره و یا ساکنینش را آواره کرد.[4]

---

1. Convention on the Rights of the Child
2. http://www. ohchr. org/en/professionalinterest/pages/crc. aspx
3. Cairo Declaration on Human Rights in Islam
4. www. umn. edu/humanrts/instree/cairodeclaration. html

۸-۱. راهنمای حفاظت از داده اتحادیه اروپا[1]

راهنمای حفاظت از داده اتحادیه اروپا، دستورالعملی است که اتحادیه اروپا آن را در سال ۱۹۹۵ تصویب کرده است. این راهنما، نحوه تدوین قوانین در حوزه پردازش داده‌های شخص شهروندان را در کشورهای عضو اتحادیه اروپا مشخص می‌کند و به‌نوعی راهنمای قانونگذاران اروپایی شناخته می‌شود. این راهنما با بند «۸» کنوانسیون اروپایی حمایت از حقوق بشر و آزادی‌های اساسی هماهنگی داشته و حق افراد را «برای داشتن زندگی خصوصی شخصی و خانوادگی» به رسمیت می‌شناسد. راهنمای حفاظت از داده اتحادیه اروپا برای پیروی از اصول حفاظت از داده سازمان همکاری و توسعه اقتصادی (OECD)[2]، تمامی اصول پیشنهادی را در راهنمای خود گنجانده است. با وجود این، در ایالات متحده آمریکا هیچ تلاشی برای گنجاندن این اصول در قوانین ملی صورت نگرفته است (شینامک،[3] ۲۰۰۱).

راهنمای حفاظت از داده اتحادیه اروپا سه اصل کلی را برای قانونگذاری به کشورهای عضو اتحادیه اروپا پیشنهاد کرده است: ۱. شفافیت،[4] ۲. هدف مشروع،[5] ۳. تناسب.[6] طبق اصول پیشنهادی، پردازش داده‌های شخصی نباید اصلاً انجام گیرد، مگر شرایط مشخص شده در اصول حاصل شده باشد.

1. EU Data Protection Directive
2. Organization for Economic Cooperation and Development
3. Shimanek
4. Transparency
5. Legitimate purpose
6. Proportionality

۱. شفافیت: شهروند[1] این حق را دارد که هنگام پردازش داده‌های شخصی‌اش از این موضوع مطلع شود. همچنین متولی (کنترل‌گر)[2] باید نام، آدرس و هدف پردازش و نیز دریافت‌کنندگان احتمالی اطلاعات را برای اطمینان از منصفانه بودن پردازش در اختیار شهروند قرار دهد.

۲. هدف مشروع: داده‌های شخصی باید برای اهداف مشخص و مشروعی پردازش شوند و برای اهدافی ناسازگار با آن هدف پردازش نشوند.

۳. تناسب: داده‌های شخصی باید تنها تا حد کفایت برای اهدافی پردازش شوند که برای آن گردآوری شده‌اند. داده‌ها باید دقیق بوده و هنگام ضرورت به‌روزرسانی شوند. تمامی اقدامات لازم برای اطمینان از اینکه حذف یا اصلاح داده‌های غیردقیق باید صورت گیرد. داده‌ها نباید بیش از زمان مورد نیاز نگهداری شوند (شینامک،[3] ۲۰۰۱).

۹-۱. دستورالعمل اتحادیه اروپا در حمایت از اشخاص حقیقی در مقابل پردازش داده‌های شخصی و گردش آزاد داده (۱۹۹۵)

اتحادیه اروپا در دوره‌های زمانی مختلف، نسخه‌های جدیدی را به راهنمای حفاظت داده اروپا افزود. در ۲۴ اکتبر ۱۹۹۵، اتحادیه اروپا دستورالعمل حمایت از اشخاص حقیقی در مقابل پردازش داده‌های شخصی و گردش آزاد داده[4] را مصوب کرد. طبق این دستورالعمل، کشورهای عضو اتحادیه اروپا موظفند تا شهروندان خود را در برابر مسائل مرتبط با حقوق

1. Data Subject
2. Controller
3. Shimanek
4. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046

بنیادین شهروندی و آزادی‌های فردی خصوصاً در مورد حق حریم خصوصی پردازش داده‌های شخصی‌شان محافظت کنند (ماده (۱)). همچنین، اعضای اتحادیه اروپا طبق این دستورالعمل نباید جریان آزاد داده‌های شخصی شهروندانشان را میان اعضای این اتحادیه منع یا محدود سازند (ماده (۲)). اصول حفاظت از داده مطرح شده در این دستورالعمل به‌شرح زیر هستند:

۱. منصفانه بودن پردازش داده‌های شخصی؛

ـ لزوم اخذ رضایت شهروند برای پردازش داده‌های شخصی؛

ـ پردازش بدون رضایت در صورت ضروری بودن پردازش طبق قرارداد میان شهروند و متولی؛

ـ پردازش بدون رضایت، در صورت ضروری بودن پردازش، بنا به الزام قانونی متوجه کنترل‌گر؛

ـ پردازش بدون رضایت، در صورت ضروری بودن پردازش، برای حفاظت از دارایی‌های مهم شهروند؛

ـ پردازش بدون رضایت، در صورت ضروری بودن پردازش، برای انجام وظیفه‌ای در جهت منافع عمومی توسط کنترل‌گر یا نهاد ثالث رسمی؛

ـ پردازش بدون رضایت، در صورت ضروری بودن پردازش، برای پیگیری منافع مشروع کنترل‌گر یا دریافت‌کننده داده با شرط پایمال نشدن حقوق شهروند یا آزادی‌های وی.

۲. مشروع بودن پردازش داده‌های شخصی (ماده (۶)).

طبق ماده (۱۰) همین دستورالعمل، متولیان داده‌های شخصی باید اطلاعات زیر را در اختیار شهروند قرار دهند:

ـ هویت کنترل‌گر یا نماینده قانونی وی؛

ـ اهداف پردازش داده‌ها؛

ـ هر نوع اطلاعات اضافی شامل:

- دریافت‌کنندگان داده یا بخش‌های داده که به آنها افشا می‌شود؛
- این موضوع که پاسخ دادن به سؤالات توسط شهروندان اجباری است یا اختیاری و نیز عواقب احتمالی عدم پاسخ به سؤالات توسط شهروند؛
- حق دسترسی و نیز اصلاح داده‌های شخصی برای شهروند؛

این دستورالعمل ۳۴ ماده دارد که مسائلی همچون پردازش داده‌های شخصی کسب شده از خود شهروند، پردازش داده‌های کسب شده از فردی غیر از خود شهروند، حق دسترسی شهروند به داده، حق اعتراض شهروند به پردازش داده‌ها، محرمانگی و امنیت پردازش داده‌ها، پردازش داده‌های شخصی خاص، اطلاع‌رسانی به نهادهای بالادستی و موارد این‌چنینی را شامل می‌شود.

۱۰-۱. دستورالعمل اتحادیه اروپا در حمایت از حریم خصوصی و ارتباطات الکترونیک (۲۰۰۲)

دستورالعمل اتحادیه اروپا[1] در حمایت از حریم خصوصی و ارتباطات الکترونیک[2] که به‌عنوان دستورالعمل حریم خصوصی الکترونیکی[3] نیز شهرت دارد، تکمیل‌کننده دستورالعمل‌های قبلی این اتحادیه در زمینه حفاظت از حریم خصوصی اطلاعاتی است که مبحث حریم خصوصی ارتباطاتی نیز به آن افزوده شده است. مسائلی همچون محرمانگی اطلاعات

1. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002L0058
2. Privacy and Electronic Communications Directive
3. E-Privacy Directive

شخصی، ترافیک داده اینترنتی، هرزنامه‌های اینترنتی و کوکی‌ها ازجمله موارد مطرح شده در این دستورالعمل است. ازآنجایی‌که در دستورالعمل قبلی مسائل مطرح شده بیشتر مربوط به حریم خصوصی اطلاعاتی هستند، در این دستورالعمل مسائل مرتبط با حریم خصوصی ارتباطاتی بیشتر مورد توجه قرارگرفته است.

این دستورالعمل دو هدف عمده دارد:

- اول فراهم کردن امنیت برای خدمات که این بخش از راهنما مربوط به فراهم‌کنندگان خدمات ارتباطی الکترونیکی همچون رساها (آی اس پی ها) است.
- دوم پیشگیری از نظارت و پایش اطلاعات افراد توسط اعضای اتحادیه اروپا از طریق شنود مکالمات، نظارت ویدیوئی و سایر شکل‌های جاسوسی.

طبق ماده (۵) این دستورالعمل، در صورت استفاده از کوکی‌های اینترنتی، به‌عنوان مثال در خریدهای آنلاین که کاربر از کالاهای مختلف بازدید می‌کند و فروشگاه اینترنتی به رصد کردن فعالیت‌های کاربر در وب‌سایت و ذخیره اطلاعات در پایگاه داده اقدام می‌کند، اعضای اتحادیه اروپا ملزم شده‌اند تا قوانینی را برای جلوگیری از ذخیره خودکار داده‌های کوکی‌های اینترنتی توسط وب‌سایت‌ها تنظیم کنند تا تنها درصورتی‌که رضایت کاربر برای این کار جلب شده باشد، این اقدام صورت گیرد.

طبق ماده (۶) این دستورالعمل، فراهم‌کنندگان خدمات اینترنتی ملزم شده‌اند تا به پاک کردن داده‌های مربوط به ترافیک اینترنتی کاربران اقدام کنند یا لااقل این نوع داده‌ها را گمنام ذخیره کنند.

طبق ماده (۱۳) این دستورالعمل، استفاده از ایمیل‌های شخصی افراد برای مقاصد بازاریابی غیرمجاز تلقی شده است و باید به شهروندان این امکان داده شود تا بتوانند با

استفاده از روش به‌اصطلاح آپت ـ این[1] (ثبت مشخصات ایمیلی توسط خود فرد جهت اعلام رضایت برای دریافت ایمیل‌های تبلیغاتی) دریافت ایمیل‌های تبلیغاتی را کنترل کنند. همچنین در این ماده ارسال سایر شکل‌های پیغام‌های تبلیغاتی همچون پیامک نیز مشابه ایمیل تلقی شده است.

۱۱-۱. دستورالعمل نگهداری داده‌های شخصی تولید و پردازش شده در چارچوب تأمین خدمات ارتباطی الکترونیکی (۲۰۰۶)

دستورالعمل نگهداری داده‌های شخصی تولید و پردازش شده در چارچوب تأمین خدمات ارتباطی الکترونیکی[2] در ۱۵ مارس ۲۰۰۶ به تصویب اتحادیه اروپا رسید.[3] این دستورالعمل علاوه‌بر راهنمایی‌های جدید برای حفظ حریم خصوصی ارتباطاتی افراد در مورد مسائل نگهداری داده‌های شخصی، اصلاحاتی برای دستورالعمل پیشین این اتحادیه در سال ۲۰۰۲ نیز محسوب می‌شود. این دستورالعمل شامل ۱۷ ماده است که مهمترین مسائل مطرح شده در آن عبارتند از:

ـ توصیف داده‌هایی که قابلیت نگهداری دارند،

ـ دوره نگهداری داده‌های شخصی، نیازمندی‌های نگهداری داده‌های شخصی،

ـ وظایف نهاد بالادستی در نظارت بر نگهداری داده‌های شخصی،

---

1. Opt-in
2. DIRECTIVE 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks
3. http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32006L0024

ـ جرائم نقض حریم خصوصی در ارتباط با نگهداری داده‌های شخصی.

از آنجایی که در دستورالعمل‌های قبلی این اتحادیه، موضوع نگهداری داده‌های شخصی دارای ضعف‌هایی تشخیص داده شده بود، در دستورالعمل جدید غالباً این موضوع مورد توجه قرار گرفته است. براساس ماده (۶) این دستورالعمل، کشورهای عضو باید داده‌های مطرح شده در زیر را حداقل ۶ ماه و حداکثر دو سال نگهداری کنند:

ـ داده‌های ضروری برای ردیابی هویت و منبع ارتباط تلفنی شامل:

- شماره تلفن تماس‌گیرنده،
- نام و آدرس مشترک خدمات مخابراتی یا کاربر ثبت‌نام کرده،

ـ در مورد دسترسی اینترنتی، ایمیل و تلفن اینترنتی:

- اطلاعات آی. دی. (ID) کاربر،
- اطلاعات آی. دی. کاربر و شماره تلفن اختصاص‌یافته به تماس ورودی از طریق شبکه تلفن عمومی،
- نام و آدرس کاربر ثبت‌نام شده‌ای که آدرس آی پی (IP) به وی اختصاص پیدا کرده یا شماره تلفن در زمان برقراری ارتباط،

ـ داده‌های ضروری برای تشخیص تاریخ، زمان و طول یک مکالمه:

- در مورد تلفن ثابت یا همراه: تاریخ و زمان شروع و پایان ارتباط،
- درباره ارتباطات اینترنتی شامل ایمیل و تلفن اینترنتی:

الف) تاریخ و زمان ورود به و خروج از خدمات دسترسی اینترنتی برمبنای منطقه زمانی و آدرس آی. پی،

ب) تاریخ و زمان ورود و خروج از خدمات ایمیلی یا خدمات تماس تلفنی اینترنتی

براساس منطقه زمانی،

ـ داده‌های ضروری برای شناسایی نوع ارتباط:

- در مورد تلفن ثابت و همراه نوع خدمات تلفنی مورد استفاده،
- درباره خدمات اینترنتی و ایمیلی، نوع خدمات اینترنتی مورد استفاده،

ـ داده‌های ضروری برای شناسایی تجهیزات ارتباطی کاربر:

- در مورد تلفن ثابت شماره تماس‌گیرنده و پذیرنده تماس،
- در مورد تلفن همراه:

الف) شماره تماس‌گیرنده و پذیرنده تماس،

ب) هویت مشترک خدمات تلفن همراه بین‌المللی ایجادکننده تماس،

ج) هویت فراهم‌کننده خدمات تلفن همراه بین‌المللی تماس‌گیرنده،

د) هویت مشترک خدمات تلفن همراه بین‌المللی دریافت‌کننده تماس،

هـ) هویت فراهم‌کننده خدمات تلفن همراه بین‌المللی تماس‌گیرنده،

و) در مورد خدمات گمنام، زمان و تاریخ برقراری خدمت و مکان برقراری تماس.

- در مورد خدمات اینترنتی و ایمیلی:

الف) تلفن تماس کاربر در خدمات دایال آپ (Dial-Up)،

ب) شماره خط مشترک دیجیتال (DSL[1]) یا نقطه انتهایی مبدأ ارتباط،

ـ داده‌های ضروری برای شناسایی مکان تجهیزات ارتباطی همراه شامل:

- مکان سلول مخابراتی شروع ارتباط،
- داده‌ها نشان‌دهنده مکان جغرافیایی سلول‌ها در طول دوره‌های برقراری تماس که

1. Digital Subscriber Line

در آنها داده‌های تماس ذخیره‌سازی شده است (ماده (۵)).

همچنین طبق ماده (۷) این راهنما، حداقل نیازمندی‌های امنیتی برای حفاظت از داده‌های مخابراتی ذخیره‌سازی شده مطرح شده است. این راهنما بیشتر داده‌هایی را مورد توجه قرار داده است که مربوط به ارتباطات تلفنی و اینترنتی هستند. به‌نظر می‌رسد هدف اصلی از این راهنما پیگرد جرائم اینترنتی و مزاحمت‌های تلفنی، هرزنامه‌های ایمیلی و مسائل مرتبط با تروریسم باشد.

۱۲-۱. اعلامیه حقوق بشر سازمان ملل (بازبینی در سال ۲۰۱۳)

سازمان ملل متحد در دسامبر ۲۰۱۳ میلادی به‌اتفاق آرا رأی به گنجاندن حق حفظ حریم خصوصی اطلاعاتی افراد به‌عنوان یکی از بندهای حقوق بشر داده است تا انسان‌ها از حقوق زیر برخوردار باشند:

الف) هرگونه ارتباطات آنلاین آنها مورد احترام قرار گرفته و حفاظت شود؛

ب) از تجاوز به حریم شخصی آنها جلوگیری شده و قوانینی ملی کشورها با حق حفظ حریم شخصی آنان سازگاری داشته باشد؛

ج) فرآیندها، رویه‌ها و قوانین نظارت بر انتقال اطلاعات و جمع‌آوری داده‌های شخصی باید با حق حفظ اطلاعات حریم شخصی افراد تطابق داشته باشد؛

د) مکانیسم‌هایی برای اطمینان از شفافیت و مناسب بودن اقدامات دولت‌ها در نظارت بر انتقال و جمع‌آوری داده‌های شخصی افراد به‌وجود آورد (شیروود،[1] ۲۰۱۳).

1. Sharwood

۲. اصول حاکم بر حفاظت از داده‌های کاربران

مهمترین اصول حاکم بر حفاظت از داده‌های کاربران که به‌عنوان سنگ زیرین قوانین کشورهای پیشرفته دنیا در این خصوص شناخته می‌شوند، عبارتند از: اصول HEW، اصول OECD، اصول APEC و اصول بندرگاه ایمن.

۲-۱. اصول HEW

از دهه ۱۹۶۰، با رشد سامانه‌های دیجیتالی ذخیره و بازیابی اطلاعات، اصول مدیریت و جمع‌آوری اطلاعات توسط نهادهای دولتی و بین‌المللی نیز توسعه پیدا کرد. در سال ۱۹۷۳ اداره بهداشت، آموزش و رفاه ایالات متحده[1] (HEW)، گزارشی را به کنگره ارسال کرد که در آن به کنگره پیشنهاد شده بود قوانینی را در زمینه سامانه‌هایی که داده‌های شخصی افراد را نگهداری می‌کنند وضع کند، این اصول حفظ حریم خصوصی در فضای مجازی که در سال ۱۹۷۴ با نام قانون محرمانگی به تصویب رسید به‌شرح زیر هستند (سولو و هوفناگل،[2] ۲۰۰۶):

- نباید هیچ‌گونه سیستم ذخیره داده‌های شخصی وجود داشته باشد که ماهیت وجودی آن محرمانه باشد.
- باید راهی برای فرد وجود داشته باشد تا بتواند با استفاده از اطلاعات بدون رضایت وی برای هدفی غیر از هدف اولیه که به همان منظور گردآوری شده، جلوگیری نماید.

1. Health, Education and Welfare
2. Solove and Hoofnagle

- باید راهی برای هر فرد وجود داشته باشد تا بتواند اطلاعات قابل شناسایی در مورد خودش را اصلاح کرده، تغییر داده یا ضبط کند.
- هر سازمانی که داده‌های قابل‌شناسایی افراد را ایجاد، نگهداری، استفاده، یا منتشر می‌کند باید از قابلیت اطمینان داده‌ها در جهت هدف اولیه گردآوری اطمینان یافته و اقدامات احتیاطی را برای جلوگیری از سوءاستفاده از داده‌ها انجام دهد.

این قانون به افراد این امکان را می‌داد که از دولت به‌خاطر نقض حقوق حریم خصوصی آنها در فضای مجازی شکایت کنند. همچنین علاوه‌بر قانون محرمانگی که مورد هدفش دولت بود، قانون اف. سی. آر. ای.[1] چارچوبی را برای حفاظت از حریم خصوصی در شرکت‌های خصوصی و غیردولتی فراهم می‌آورد. در پیروی از این قانون در آمریکا، بسیاری از کشورها و نهادهای بین‌المللی (همچون اتحادیه اروپا، سازمان ملل و...) به تکاپو افتادند تا اصولی را برای محرمانگی اطلاعات وضع کنند.

۲-۲. اصول OECD

یکی از شناخته‌شده‌ترین دسته‌بندی‌های اصول حفظ حریم خصوصی در فضای مجازی می‌توان به اصول مطرح شده توسط سازمان همکاری و توسعه اقتصادی (OECD[2]) اشاره کرد. این اصول برای کشورهای عضو این سازمان به‌عنوان راهنمایی برای تدوین قوانین درون‌مرزی برای حفاظت از حریم خصوصی شهروندان در فضای مجازی پیشنهاد شده‌اند. این اصول عبارتند از:

1. FCRA
2. Organization for Economic Cooperation and Development

۱. اصل محدودیت جمع‌آوری:[1] باید محدودیت‌هایی در جمع‌آوری داده‌های شخصی وجود داشته باشد. همچنین تمامی داده‌های شخصی تنها باید توسط ابزارهای قانونی و منصفانه و با اطلاع و رضایت افراد به‌دست آیند.

۲. اصل کیفیت اطلاعات:[2] داده‌های شخصی باید مربوط به اهدافی باشند که در آن زمینه مورد استفاده واقع می‌شوند؛ همچنین تا حدی که برای این اهداف مورد نیاز است، باید دقیق، کامل، و به‌روز باشند.

۳. اصل مشخص بودن هدف:[3] اهدافی که در جهت آنها داده‌های شخصی جمع‌آوری می‌شوند، باید درست هنگام جمع‌آوری داده‌ها مشخص شوند و نیز استفاده‌های بعدی نیز باید محدود به برآورده کردن همان اهداف، یا اهدافی سازگار با اهداف اولیه باشند.

۴. اصل محدودیت استفاده:[4] داده‌های شخصی نباید در جهت اهدافی غیر از اهداف مشخص‌شده، آشکار شده، در دسترس قرار گرفته، یا مورد استفاده قرار گیرند، مگر در شرایطی با رضایت صاحب داده‌ها یا نهاد قانونی صاحب اختیار.

۵. اصل تدابیر حفاظتی امنیتی:[5] تدابیر حفاظتی ایمنی معقولی باید برای حفاظت از داده‌های شخصی در مقابل ریسک‌هایی چون از دست دادن یا دسترسی، تخریب، استفاده، اصلاح، یا افشای غیرمجاز داده‌ها به‌کار گرفته شوند.

۶. اصل گشودگی[6] **(یا شفافیت)**: باید سیاستی کلی برای گشودگی (صراحت) در

---

1. Collection Limitation Principle
2. Data Quality Principle
3. Purpose Specification Principle
4. Use limitation Principle
5. Security Safeguards Principle
6. Openness Principle

مورد توسعه، روش‌ها و سیاست‌های مربوط به داده‌های شخصی وجود داشته باشد. ابزارهای استقرار وجود و ماهیت داده‌های شخصی و اهداف اصلی استفاده از آنها باید در دسترس عموم قرار گرفته و نیز باید هویت نهاد کنترل‌کننده و در اختیار دارنده داده‌ها به‌طور شفاف بیان شود.

۷. اصل مشارکت فردی:[1] هر فرد باید این حق را داشته باشد که:

تصدیقی از کنترل‌کننده داده‌ها به‌دست آورد که کنترل‌کننده داده‌ها مربوط به وی را در اختیار دارد یا خیر.

ـ این داده‌ها را در زمان منطقی و نیز:

- با (پرداخت هر) هزینه‌ای که بیش‌ازحد نباشد،
- به طریقی منطقی،
- به صورتی قابل فهم کسب کند.

ـ به وی دلایلی داده شود که چرا تقاضای وی در موارد ۱ و ۲ رد شده و قادر باشد تا چنین عدم پذیرش درخواستی را (به‌صورت قانونی) به چالش بکشد.

ـ داده‌های مربوط را (به‌صورت قانونی) به چالش کشیده و اگر پیگرد قانونی موفقیت‌آمیز بود، بتواند داده‌ها را اصلاح کرده، کامل کرده، تغییر دهد یا حذف کند.

۸. اصل پاسخگویی:[2] یک کنترل‌کننده داده باید پاسخگوی تطابق با سنجه‌ها (معیارها)یی باشد که اصول فوق‌الذکر را عملی می‌سازند.[3]

---

1. Individual Participation Principle
2. Accountability Principle
3. http://www. oecd. org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata. htm#part2

۳-۲. اصول APEC[1]

اصول حفاظت از حریم خصوصی در فضای مجازی آپک (APEC) یا سازمان همکاری‌های اقتصادی آسیا و اقیانوسیه، نیز همچون اصول OECD اصولی را برای حفاظت از داده‌های شخصی شهروندان کشورهای عضو پیشنهاد داده است. این اصول در سال ۲۰۰۳ مطرح شد و در سال ۲۰۰۵ توسط کشورهای عضو لازم‌الاجرا تلقی شد. برخلاف اصول OECD که به‌عنوان به‌اصطلاح کف شناخته می‌شوند و کشورهای عضو می‌توانند با تدوین قوانین جداگانه، این اصول را ارتقا دهند، در اصول APEC، در هیچ کجا بیان نشده است که کشورهای عضو می‌توانند با تصویب قوانین تقویتی، این اصول استاندارد را ارتقا دهند. بنابراین به‌نظر می‌رسد در چارچوب پیشنهادی APEC برای حفاظت از حریم خصوصی اطلاعاتی سقف تعیین شده است (گرینلیف،[2] ۲۰۰۹). اصول ۹ گانه APEC به‌شرح زیر هستند:

۱. اصل پیشگیری از ضرر:[3] اصول حفاظت از حریم خصوصی اطلاعاتی باید برمبنای جلوگیری از ضرر افراد طراحی شوند.

۲. اصل اطلاع‌رسانی:[4] افراد باید در مواقع لزوم از اطلاعاتی همچون موارد زیر آگاه شود:

- اهداف گردآوری،
- احتمال افشای داده‌های شخصی،
- جزئیات مربوط به مشخصات کنترل‌گر داده‌های شخصی،[5]

1. Asia-Pacific Economic Cooperation
2. Greenleaf
3. Preventing Harm
4. Notice
5. Data Controller

ـ روش‌هایی که فرد می‌تواند استفاده از داده‌های شخصی خود را محدود کند،

ـ راه‌های اصلاح داده‌های شخصی توسط فرد،

ـ روش‌های دسترسی به داده‌های شخصی توسط فرد.

۳. اصل محدودیت گردآوری:[1] داده‌های شخصی باید مرتبط با اهداف گردآوری باشند و باید حداقل اطلاعات در مورد افراد گردآوری شود.

۴. اصل (محدودیت) استفاده از داده‌های شخصی:[2] استفاده از داده‌های شخصی افراد باید سازگار با اهداف مرتبط با گردآوری بوده و همراه با جلب رضایت فرد انجام گیرد.

۵. اصل انتخاب:[3] افراد باید بتوانند درخصوص گردآوری، استفاده و افشای داده‌های شخصی خود از حق انتخاب برخوردار باشند.

۶. اصل یکپارچگی اطلاعات شخصی:[4] اطلاعات شخصی افراد باید تا حد موردنیاز برای اهداف استفاده، دقیق، کامل و به‌روز باشد.

۷. اصل تدابیر حفاظتی امنیتی:[5] کنترل‌گرهای داده باید تدابیر حفاظتی امنیتی کافی را برای جلوگیری از ریسک‌های داده‌های شخصی متناسب با شدت ریسک و حساسیت اطلاعات به‌کار گیرند.

۸. اصل دسترسی و اصلاح:[6] افراد باید بتوانند به داده‌های شخصی مربوط به خود دسترسی داشته باشند و در صورت غیرصحیح بودن، بتوانند آنها را اصلاح کنند.

---

1. Collection Limitation
2. Uses of Personal Information
3. Choice
4. Integrity of Personal Information
5. Security Safeguards
6. Access and Correction

۹. اصل مسئولیت‌پذیری:[1] کنترل‌گر داده‌های شخصی مسئولیت تطابق با اصول مطرح شده فوق را دارد و در صورت انتقال داده‌های شخصی به شخص یا کشور ثالث باید از قبل رضایت فرد را جلب کرده باشد.[2]

۴-۲. اصول بندرگاه ایمن

با توجه به اختلاف میان قوانین آمریکا و اتحادیه اروپا در زمینه حریم خصوصی در فضای مجازی، شرکت‌های آمریکایی که قصد انجام تجارت الکترونیکی با کشورهای اتحادیه اروپا را دارند، باید از اصول حفظ حریم خصوصی در فضای مجازی موسوم به بندرگاه ایمن[3] که در سال ۲۰۰۰ مصوب شده است، تبعیت کنند. این اصول نیز به‌عنوان اصول هشت‌گانه حفظ حریم خصوصی در تجارت الکترونیک شناخته می‌شوند. این اصول به‌شرح زیر هستند:

۱. اصل اطلاع:[4] افراد باید از این موضوع که داده‌های شخصی آنها گردآوری می‌شود و نحوه استفاده از آنها مطلع شوند. به آنها باید اطلاعاتی درخصوص نحوه تماس با سازمان (گردآوری‌کننده داده‌های شخصی) برای پرسش سؤال‌ها یا مطرح کردن شکایاتشان تدارک دیده شود.

۲. اصل انتخاب:[5] برای افراد باید این گزینه انتخابی وجود داشته باشد که بتوانند داده‌های شخصی خود را از فرآیند گردآوری یا انتقال بعدی به نهادها (یا اشخاص) ثالث

1. Accountability
2. http: //www. apec. org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk. ashx
3. Safe Harbor Privacy Principles
4. Notice Principle
5. Choice Principle

خارج کنند.

۳. اصل (محدودیت) انتقال بعدی:[۱] انتقالات داده‌ها به نهادها (یا اشخاص) ثالث باید تنها هنگامی رخ دهد که این عملیات از اصول کافی حفاظت از داده تبعیت کند.

۴. اصل امنیت:[۲] تلاش‌های معقولی باید برای جلوگیری از دست رفتن داده‌های گردآوری شده[۳] انجام گیرد.

۵. اصل یکپارچگی داده‌ها:[۴] داده‌ها باید نسبت به اهدافی که گردآوری شده‌اند مربوط[۵] و قابل اعتماد[۶] باشند.

۶. اصل دسترسی:[۷] افراد باید بتوانند به اطلاعاتی که در مورد آنها (توسط یک سازمان) نگهداری می‌شود دسترسی داشته باشند و در صورت غیردقیق بودن، آن را اصلاح یا حذف کنند.

۷. اصل اجرا:[۸] باید روش‌های مؤثری برای اجرای این قوانین وجود داشته باشد.[۹]

---

1. Onward Transfer
2. Security Principle
3. Loss of Collected Information
4. Data Integrity Principle
5. Relevant
6. Reliable
7. Access Principle
8. Enforcement Principle
9. European Court of Justice 2000/520/EC: Commission Decision of 26 July 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce (Notified Under Document Number C (2000) 2441) (Text with EEA Relevance) 25 August 2000.

۳. رویکردهای جهانی پیرامون حفاظت از داده‌های کاربران

در تحقیق بلمان و همکاران[1] (۲۰۱۴) سه رویکرد قانونگذاری در کشورهای دنیا برای حفظ حریم خصوصی اطلاعاتی شناسایی شده است: ۱. کشورهای فاقد قوانین مدون، ۲. کشورهای دارای قانونگذاری بخشی،[2] ۳. کشورهای دارای قانونگذاری یکپارچه[3] (جدول).

جدول رویکردهای قانونگذاری در حوزه حفظ حریم خصوصی اطلاعاتی

رویکرد قانونگذاری در حوزه حفظ حریم خصوصی اطلاعاتی	کشورها
کمبود قوانین مدون	پاکستان، گواتمالا، هند، ترکیه، مالزی، مکزیک، فیلیپین، سنگاپور، ونزوئلا و...
قانونگذاری بخشی	ایالات متحده آمریکا و ژاپن
قانونگذاری یکپارچه	کره جنوبی، استرالیا، کانادا، اتریش، بلژیک، فرانسه، ایتالیا، کانادا، دانمارک، فنلاند، آلمان، یونان، بلژیک، نروژ، ایرلند، پرتغال، اسپانیا، سوئد، سوئیس و انگلستان و...

به‌نظر می‌رسد دنیای حفاظت از حریم خصوصی کاربران در فضای مجازی دوقطبی شده است. در یک سوی این معادله، ایالات متحده آمریکا قرار دارد و در سوی دیگر، دیدگاه اروپایی دیده می‌شود. ایالات متحده آمریکا در فناوری اطلاعات و اینترنت هم از نظر فنی و زیرساختی و هم ازنظر قانونگذاری پیشتازتر از سایر کشورها بوده است، اما

1. Bellman et al.
2. Sectoral
3. Omnibus

به‌نظر می‌رسد سیاست‌ها و قوانین این کشور دارای خلأهای زیادی در حوزه حفاظت از حریم خصوصی کاربران در فضای مجازی است. ایالات متحده آمریکا به‌دلیل اتخاذ روش موردی برای قانونگذاری درخصوص حریم خصوصی و رویکرد خودتنظیمی در بخش‌های مختلف این موضوع، فاقد قانونی جامع در این زمینه است. در زمینه حریم خصوصی داده‌ها مواضع این کشور دربردارنده نکات زیر است:

- داده‌های مرتبط با اشخاص که توسط بنگاه‌ها و دولت جمع‌آوری شده‌اند، مورد حمایت قرار نمی‌گیرند؛
- وجود دیدگاه بازارگرایی و مصرفی، بدین معنا که مردم مصرف‌کننده‌اند و داده، کالایی مصرفی و قابل فروش و متعلق به شرکت است؛
- محدود نبودن جریان داده‌ها بین شرکت‌ها؛
- اتکا به قانون‌شناسی و پایبندی شرکت‌ها به حریم خصوصی افراد؛
- تبعیت از قانون‌های متفرق که هریک تنها ناظر بر جنبه خاصی از حریم خصوصی هستند نه کل آن (نوری و نخجوانی، ۱۳۸۲: ۱۰۶).

نقطه مقابل رویکرد آمریکایی در باب حفاظت از داده‌های کاربران ، رویکرد اروپایی است. رهیافت اروپایی درباره حریم خصوصی کاربران در فضای مجازی رهیافت جامع‌نگر یا کل‌نگر است. در این رویکرد، قوانین جامع و فراگیر در زمینه حمایت از داده‌ها، تعیین مراجع عمومی برای ثبت داده‌ها، پایگاه داده، حل اختلاف، اخذ رضایت قبلی در مورد پردازش برخی داده‌ها و... مدنظر قرار می‌گیرد (محسنی، ۱۳۹۴: ۵۴۰). بسیاری از کشورهای غیراروپایی همچون استرالیا، کانادا، کره جنوبی، ژاپن و... نیز به تأسی از دیدگاه اروپایی، به تدوین قانونی جامع برای حفاظت از داده‌های کاربران پرداخته‌اند و در آن،

برخلاف ایالات متحده آمریکا، از داده‌های شخصی گردآوری شده توسط نهادهای دولتی نیز حمایت کرده‌اند.

مشکلی که به‌علت دوقطبی شدن حریم خصوصی اطلاعاتی در دنیا وجود دارد، به‌وجود آمدن مشکل در انتقالات بین‌المللی داده‌های شخصی افراد میان کشورهای خصوصاً اروپایی و آمریکا وجود دارد. بنابراین میان سال‌های ۱۹۹۸-۲۰۰۰ وزارت بازرگانی ایالات متحده طی یک همکاری مشترک با کمیسیون اروپا مقررات «بندرگاه ایمن»[1] را تدوین کردند که در همان سال مورد تأیید اتحادیه اروپا قرار گرفت. این مقررات برای جلوگیری از دست رفتن یا افشای تصادفی داده‌های مشتریان که توسط شرکت‌های خصوصی در کشورهای عضو اتحادیه اروپا یا ایالات متحده آمریکا نگهداری می‌شوند، تدوین شدند. در سال ۲۰۰۰ نیز اتحادیه اروپا چنین مصوب کرد که شرکت‌های آمریکایی که قصد انجام تجارت الکترونیک با کشورهای اروپایی را دارند، باید نام خود را در به‌اصطلاح «لیست بندرگاه ایمن»[2] ثبت کنند و متعهد به تبعیت از اصول «بندرگاه ایمن» باشند.[3] در ۲ فوریه سال ۲۰۱۶ نیز اتحادیه اروپا تصمیم گرفت تا از طریق همکاری بیشتر میان نهادهای حفاظت از داده اروپایی، بر نقل و انتقالات داده‌های شخصی شهروندان میان کشورهای عضو اتحادیه اروپا و ایالات متحده آمریکا نظارت بیشتر و قوی‌تری داشته باشد. همچنین طبق مصوبه اخیر اتحادیه اروپا، دولت آمریکا باید تعهد کند تا شرایط و محدودیت‌های دسترسی نهادهای دولتی به داده‌های شخصی منتقل شده از اروپا به آمریکا

1. Safe Harbor
2. Safe Harbor List
3. http://web. archive. org/web/20150910175747/http://export. gov/safeharbor/eu/eg_main_018493. asp

و بالعکس را به‌صورت روشن بیان کرده و از دسترسی عمومی آنها به چنین داده‌هایی جلوگیری به‌عمل آورد. همچنین حق کشورهای اروپایی برای طرح هرگونه شکایت علیه نقض حریم خصوصی کاربران اروپایی در فضای مجازی توسط دولت آمریکا محفوظ است.[۱]

امروزه ایالات متحده آمریکا به‌عنوان بزرگ‌ترین ناقض حریم خصوصی کاربران در فضای مجازی شناخته می‌شود. پس از افشاگری‌های ادوارد اسنودن،[۲] کارمند سابق سازمان امنیت ملی آمریکا[۳] (NSA)، که اطلاعات محرمانه این سازمان را در سال ۲۰۱۳ منتشر کرد، مشخص شد که سازمان امنیت ملی آمریکا به‌صورت نظام‌مند اقدام به شنود اطلاعات شخصی شهروندان آمریکایی و حتی شنود اطلاعات شهروندان و حتی مقامات دولتی سایر کشورها می‌کند. وی بنا به افشای اسرار دولتی و اسناد محرمانه توسط دولت ایالات متحده مورد پیگرد قانونی قرار گرفت و محکوم شد، اما توسط کشورهایی که به آنها پناهنده شده بود هرگز به آمریکا تحویل داده نشد.[۴] با وجود افشاگری‌های اسنودن، نهادهای امنیتی آمریکا به بهانه‌های مختلفی همچون حفاظت از امنیت ملی و مبارزه با تروریسم، حق حریم خصوصی کاربران در فضای مجازی را زیر پا گذارده و برنامه‌های شنود اینترنتی گسترده خود را متوقف نکرده‌اند. «هر مکالمه‌ای که شهروندان آمریکایی در خاک آمریکا با هم انجام می‌دهند، با یا بدون حکم دادگاهی ثبت و ضبط می‌شود» همچنین «سامانه‌های گردآوری در آژانس امنیت ملی آمریکا ۷/۱ میلیارد ایمیل، مکالمات تلفنی و سایر اشکال مکالمات را ذخیره می‌کنند» (گرینوالد،[۵] ۲۰۱۳).

1. http://europa. eu/rapid/press-release_IP-16-216_en. htm
2. Edward Snowden
3. National Security Agency

٤. وی ابتدا به هنگ کنگ و سپس به روسیه سفر کرد و درحال حاضر به روسیه پناهنده شده است.

5. Greenwald

۴. گونه‌شناسی[1] تنظیم مقررات حفاظت از داده‌های کاربران در فضای مجازی

در دنیا دو نوع گونه‌شناسی در مورد تنظیم مقررات حفاظت از داده‌های کاربران در فضای مجازی مشاهده می‌شود: مدل موردی[2] یا خودتنظیمی[3] (شکل ۱) و مدل جامع‌نگر[4] (شکل ۲).

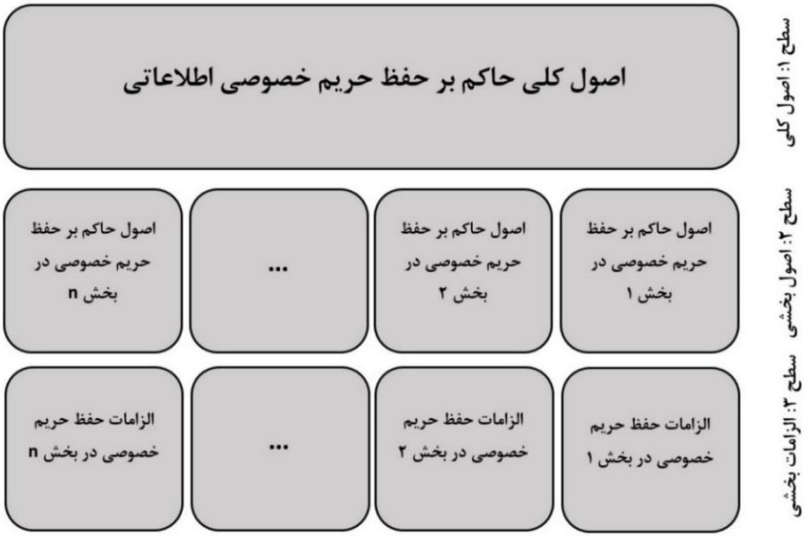
۴-۱. مدل خودتنظیمی تنظیم مقررات حفظ حریم خصوصی اطلاعاتی

در مدل خودتنظیمی تنظیم مقررات حریم خصوصی اطلاعاتی که از رویکرد آمریکایی تنظیم مقررات حریم خصوصی اطلاعاتی نشئت می‌گیرد، سه سطح مشاهده می‌شود. در سطح اول که بالاترین سطح است، اصول کلی حفظ حریم خصوصی وجود دارد که بدون توجه به بخش خاص، در تمامی بخش‌ها باید رعایت شوند. این اصول را می‌توان همان اصول حاکم بر حریم خصوصی دانست که یک کشور خود را ملزم به رعایت آنها می‌کند. به‌عنوان مثال اصول HEW، اصول OECD، اصول APEC و غیره. در سطح دوم که سطح اصول حاکم بر بخش خاص است، اصول حریم خصوصی که فراتر از اصول کلی هستند و تنها مختص یک بخش خاص مثل بخش بهداشت و درمان، بخش مالی و بانکی، بخش قضایی و غیره هستند به چشم می‌خورند. باید توجه داشت که اصول هر بخش ممکن است تفاوت‌هایی با سایر بخش‌ها داشته باشند. مثلاً ممکن است بخش بهداشت و درمان اصول HEW را رعایت کند و بخش مالی و بانکی اصول HEW و اصول OECD را رعایت کند. در سطح

1. Taxonomy
2. Sectorial Approach
3. Self. Regulation
4. Comprehensive Approach

سوم که مهمترین سطح حفاظت از حریم خصوصی است، الزامات لازم‌الرعایه که باید توسط سازمان‌های مختلف هر بخش (مثلاً بیمارستان‌ها و کلینیک‌های بهداشتی، مراکز مشاوره پزشکی و ژنتیکی، مراکز ترک اعتیاد و غیره در بخش بهداشت و درمان، بانک‌ها و مؤسسات مالی و اعتباری و غیره در بخش مالی و سایر سازمان‌های بخش‌های مختلف) اجرا شوند براساس اصول حاکم کلی و اصول خاص بخشی به چشم می‌خورند.

شکل ۱. مدل خودتنظیمی تنظیم مقررات حریم خصوصی اطلاعاتی



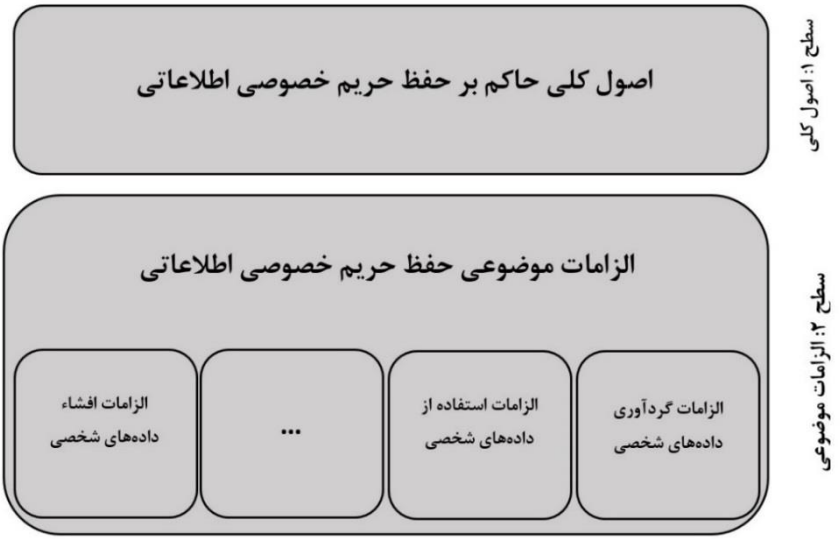
مأخذ: محسنی، ۱۳۹۴، ص ۵۴۰.

۲-۴. مدل جامع‌نگر تنظیم مقررات حریم خصوصی اطلاعاتی

در مدل جامع‌نگر تنظیم مقررات حریم خصوصی اطلاعاتی که از رویکرد اروپایی تنظیم

مقررات حریم خصوصی اطلاعاتی نشئت می‌گیرد، دو سطح وجود دارد. در سطح اول که اصول کلی نام دارد، مشابه مدل خودتنظیمی یکسری اصول اساسی حاکم بر حفظ حریم خصوصی اطلاعاتی به چشم می‌خورد. برخلاف مدل خودتنظیمی، در مدل جامع‌نگر، تنها یکسری اصول کلی وجود دارد و بخش‌های مختلف دولتی و خصوصی به‌صورت جداگانه اصول بخشی ندارند. به‌عبارت دیگر تنها یک سطح برای اصول حاکم وجود دارد. بدین‌ترتیب امکان تشتت در اصول و الزامات حفظ حریم خصوصی در بخش‌های مختلف به حداقل ممکن رسیده و تمامی بخش‌ها به‌صورت یکپارچه و هماهنگ ملزم به رعایت اصول خاصی هستند. در سطح دوم الزامات موضوعی با توجه به اصول کلی وجود دارد. این الزامات برای تمامی بخش‌ها به‌صورت یکپارچه تدوین شده و در قوانین حفظ حریم خصوصی اطلاعاتی مشخص شده‌اند. الزامات حفظ حریم خصوصی برای موضوعات مختلف مرتبط با پردازش داده‌های شخصی شهروندان همچون گردآوری، نگهداری، استفاده و... و سایر موضوعات همچون مسائل مربوط به انتقال بین‌المللی داده‌های شخصی، حقوقی که شهروند (کاربر دولت الکترونیک) از آنها برخوردار است و مسائل فنی مرتبط با حفظ امنیت و محرمانگی داده‌ها در قوانین حریم خصوصی اطلاعاتی تدوین شده است.

شکل ۲. مدل جامع‌نگر تنظیم مقررات حریم خصوصی اطلاعاتی



مأخذ: همان.

جمع‌بندی

براساس نظر بسیاری از صاحبنظران و به‌ویژه مبتنی‌بر تحقیق میلبرگ و همکاران[1] (۲۰۰۰) که در چندین کشور به انجام رسیده است، مدل خودتنظیمی[2] تنظیم مقررات حریم خصوصی اطلاعاتی، نمی‌تواند به‌عنوان مدلی که حافظ حق حریم خصوصی کاربران در فضای مجازی است، برای بلندمدت موفق عمل کند. آنها معتقدند، این مدل شاید برای کوتاه‌مدت جواب بدهد، اما در بلندمدت نمی‌تواند موجب حفظ حریم خصوصی کاربران

1. Milberg et al.
2. Self-Regulatory

در فضای مجازی شود. ازآنجایی‌که در مدل خودتنظیمی، قانونگذار اختیار قانونگذاری برای تمامی بخش‌ها را ندارد و هر بخش با توجه به نیاز خود اقدام به تدوین دستورالعمل‌هایی برای حفظ حریم خصوصی اطلاعاتی می‌کند که ممکن است با الزامات حفظ حریم خصوصی اطلاعاتی در سایر بخش‌ها تداخل‌ها و تعارض‌های زیادی داشته باشد، ازاین‌رو نمی‌توان به چارچوب جامعی برای حفظ حریم خصوصی کاربران در فضای مجازی دست یافت. اگر قبول کنیم که در دولت الکترونیک، حرکت سازمان‌های دولتی باید به سمت تعامل بیشتر و یکپارچگی باشد، بنابراین نمی‌توان با اتخاذ این نوع طبقه‌بندی به چارچوبی یکپارچه برای حفظ حریم خصوصی کاربران در فضای مجازی دست یافت. به‌عنوان مثال، اگر قرار باشد اصول و الزامات حفظ حریم خصوصی اطلاعاتی در بخش‌های مختلف با هم تفاوت داشته باشد، عملاً استقرار دولت الکترونیک به‌عنوان یک پنجره واحد که شهروندان از آن طریق خدمات دولتی را دریافت می‌کنند ناممکن خواهد بود؛ زیرا سازمان‌های مختلف بنا به تفاوت در الزامات حفاظت از داده‌های کاربران، تبادل داده‌های شخصی را مغایر با قوانین بخشی خود می‌بینند. ازاین‌رو، آمریکا قانون حفظ حریم خصوصی اطلاعاتی سازمان‌های دولتی را شامل نمی‌شود و تنها بخش خصوصی و غیردولتی را شامل می‌شود. بدین طریق بخش‌های دولتی بدون هیچ‌گونه نگرانی برای نقض حریم خصوصی کاربران در فضای مجازی باهم به تبادل داده‌های شخصی آنان می‌پردازند و دولت الکترونیک در آمریکا مستقر می‌شود. در نقطه مقابل، مدل جامع‌نگر به‌نظر می‌رسد که مناسب‌ترین راهکار برای حفظ حریم خصوصی کاربران در فضای مجازی باشد. در این طبقه‌بندی، اصول و الزامات براساس بخش‌های مختلف شاخه‌شاخه شوند، یکپارچه شده و موجب هماهنگی در میان سازمان‌های مختلف می‌شوند. به‌عنوان مثال، سازمان امور مالیاتی به

رعایت همان اصول و الزاماتی ملزم است که شهرداری به رعایت آنها ملزم است. در این صورت نه‌تنها برخلاف مدل خودتنظیمی پیاده‌سازی دولت الکترونیک ناممکن نمی‌شود، بلکه استقرار دولت الکترونیک به‌دلیل یکپارچگی الزامات حفظ حریم خصوصی کاربران در فضای مجازی تسهیل می‌شود. همچنین متخصصان حفظ حریم خصوصی کاربران در فضای مجازی در سازمان‌های دولتی به این دلیل که دارای یک راهنمای واحد قانونی هستند، بهتر می‌توانند به حفاظت از داده‌های کاربران بپردازند. همچنین شهروندان به این دلیل که دارای حقوق شهروندی یکسانی در مواجهه با سازمان‌های دولتی مختلف هستند، از سردرگمی درآمده و به حفظ حریم خصوصی اطلاعاتی خود امیدوارتر می‌شوند. از همه مهمتر ساده‌تر شدن تدوین، بازنگری، اصلاح و نظارت بر اجرای قوانین حفظ حریم خصوصی اطلاعاتی توسط مجالس قانونگذاری و سازمان‌های دیده‌بان حریم خصوصی است که به‌دلیل جامع بودن اصول و الزامات حفظ حریم خصوصی اطلاعاتی بسیار ساده‌تر می‌شود. با توجه به اینکه در مدل جامع‌نگر، رویکرد بهتری به حفاظت از داده‌های کاربران پیگیری شده است، این طبقه‌بندی منطقی‌تر به‌نظر می‌رسد.

منابع و مآخذ

۱. چارچوب تعامل‌پذیری دولت الکترونیک جمهوری اسلامی ایران (۱۳۹۵)، آدرس اینترنتی:
http://smart.gov.ir/portal/file/?80990/IReGIF—v0.2-under-development.pdf

۲. ضوابط فنی اجرایی توسعه دولت الکترونیکی، (۱۳۹۳)، دبیرخانه شورای عالی فناوری اطلاعات، آدرس اینترنتی:
http://kb.mporg.ir/FileSystem/View/File.aspx?FileId=8d109781-be56-407d-be23-ce42b3ac252f

۳. فقیهی، مهدی، معمارزاده، غلامرضا و رفوگر آستانه، حسین. حفظ حریم خصوصی بیماران، پیش‌نیاز توسعه سلامت الکترونیک، فصلنامه اخلاق پزشکی، دوره ۴، ش ۱۲، ۱۳۸۹.

۴. حسنی، فرید. حریم خصوصی اطلاعات: مطالعه کیفری در حقوق ایران، ایالات متحده آمریکا و فقه امامیه، تهران، انتشارات دانشگاه امام صادق (ع)، ۱۳۹۴.

۵. نوری، محمدعلی و نخجوانی، رضا. حقوق تجارت الکترونیکی، تهران: گنج دانش، ۱۳۸۲.

6. Boardman, R. (2015). Data protection in UK: overview, [Online], Retreived from: uk. practicallaw. com/1-502-1544?source=relatedcontent [3/5/2016]

7. Bourbeau, J. , & Lindell, R. (2014). Thousands of Canadians compromised by government information breaches. [Online], Retreived from: http://www. globalnews. ca/news/1237845/thousands-of-canadians-compromised-by-government-information-breaches. [2/8/2016]

8. Creswell, J. W. (I) (2013). Research design: Qualitative, quantitative, and mixed methods approaches. Sage publications.

9. Creswell, J. W. (II) (2013). Philosophical assumptions and intrepretive frameworks. Qualitiative inquiry and research design: Choosing among five approaches, 15-41.

10. Cuatrecasas, G. P. (2015). Data protection in Spain: overview, [Online], Retreived from: uk. practicallaw. com/1-520-8264 [1/5/2016]

11. Cuhls, K. (2003). Delphi method. Fraunhofer Institute for Systems and Innovation Research.
12. D'hulst, T. (2016). Data protection in Belgium: overview. [Online], Retreived from: uk. practicallaw. com/2-502-2977# [4/5/2016]
13. DLA. (2016). Piper's Data Protection. Privacy and Security group, [Online], Retreived from: http://www. dlapiperdataprotection. com [1/3/2016]
14. Douglas, R. (2014). Identity Theft Victim Statistics. Retreived from www. identitytheft. info/about. aspx.
15. Electronic Frontier Foundation. (2016). NSA Spying. [Online], Retrieved from: https://www. eff. org/nsa-spying [3/11/2016]
16. Greenleaf, G. , & Park, W. I. (2012). Korea's new Act: Asia's toughest data privacy law. Privacy Laws & Business International Report, (117), 1-6.
17. Greenwald, G. (2013). Are all telephone calls recorded and accessible to the US government? The Guardian, [Online], Retreived from: www. theguardian. com/commentisfree/2013/may/04/ telephone-calls-recorded-fbi-boston [4/26/2016]
18. Greenwald, G. (2014). Edward Snowden: the whistleblower behind the NSA surveillance revelations. New York: The Guardian. . [Online], Retreived from: http://www. theguardian. com/world/2013/ jun/09/edward-snowden-nsa-whistleblower-surveillance.
19. Guilayn, A. A. & Sala, A. N. (2015). Data protection in Spain: overview. [Online], Retreived from:uk. practicallaw. com/1-520-8264 [4/26/2016]
20. HIHD. (2014). Pan-Canadian Health Information Privacy and Confidentiality Framework. Retreived from http://www. hc-sc. gc. ca/ahc-asc/activit/atip-aiprp/priv-prot/index-eng. php.
21. Hiller, J. S. , & Belanger, F. (2001). . Privacy Strategies for Electronic Government. North America: Rowman and Littlefield Publishers.
22. Holloway, I. , & Wheeler, S. (2013). Qualitative research in nursing

and healthcare. John Wiley & Sons.
23. Hutcheon, M. L. (2015). The Government Does Not Take an Oath of Privacy. American journal of therapeutics, 22(4), 318-319.
24. Häger, E. W. (2015). Data protection in Sweden: overview. [Online], Retrieved from: uk. practicallaw. com/8-502-0348 [4/17/2016]
25. Milberg, S. J. , Smith, H. J. , & Burke, S. J. (2000). Information privacy: Corporate management and national regulation. Organization science, 11(1), 35-57.
26. OECD. (2013). OECD Guidelines on the Protection of Privacy and Trans border Flows of Personal Data. [Online], Retrieved from: http://www. oecd. org/sti/ieconomy/oecdguidelinesontheprotectionof privacyandtransborderflowsofpersonaldata. htm#part2 [4/26/2016]

مرکز پژوهش‌ها
مجلس شورای اسلامی

شناسنامه گزارش	شماره مسلسل: ۱۵۸۶۴

عنوان گزارش: حفاظت از داده‌های کاربران: رویکردهای جهانی و گونه‌شناسی تنظیم مقررات

نام دفتر: مطالعات ارتباطات و فناوری‌های نوین

تهیه و تدوین‌کنندگان: مهدی فقیهی، محمدجواد جمشیدی

ناظر علمی: حسین افشین

متقاضی: معاونت پژوهش‌های زیربنایی و امور تولیدی

ویراستار تخصصی: ـــــ

ویراستار ادبی: ـــــ

واژه‌های کلیدی: ـــــ

تاریخ انتشار: ۱۳۹۷/۳/۲