بررسی قوانین حفاظت از داده‌های کاربران در کشورهای منتخب

کد موضوعی: ۲۸۰
شماره مسلسل: ۱۵۸۷۷
خردادماه ۱۳۹۷

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

به‌نام خدا

فهرست مطالب

بررسی قوانین حفاظت از داده‌های کاربران در کشورهای منتخب

چکیده

حفاظت از داده‌های کاربران با توجه به توسعه فناوری اطلاعات و ارتباطات و فضای مجازی به یکی از اولویت‌های سیاستی و قانونگذاری کشورها تبدیل شده است، به نحوی که اغلب کشورهای توسعه‌یافته به تصویب قوانین بخشی یا یکپارچه در این زمینه اقدام کرده‌اند. با وجود نیاز به این زیرساخت قانونی در کشور، مطالعه وضعیت تصویب قوانین موضوعه مفید و ضروری به‌نظر می‌رسد. در این گزارش به بررسی قوانین، نحوه قانونگذاری، ساختار اجرایی و نظارتی حریم خصوصی در فضای مجازی در ۱۱ کشور توسعه‌یافته پرداخته می‌شود تا با توجه به اسناد و سیاست‌های ملی در سیاستگذاری و قانونگذاری حفاظت از داده‌های کاربران کشور مورد بهره‌برداری قرار گیرد.

مقدمه

براساس گزارش قبلی مرکز پژوهش‌های مجلس با عنوان حفاظت از داده‌های کاربران: بررسی رویکردها و گونه‌شناسی کشورها سه رویکرد قانونگذاری برای حفظ حریم خصوصی اطلاعاتی شناسایی شد: ۱. کشورهای فاقد قوانین مدون؛ ۲. کشورهای دارای قانونگذاری بخشی[1] و ۳. کشورهای دارای قانونگذاری یکپارچه.[2] کشورهای همچون پاکستان، گواتمالا، هند، ترکیه، مالزی، مکزیک، فیلیپین، سنگاپور، ونزوئلا دارای کمبود قوانین در این حوزه هستند، ایالات متحده آمریکا و ژاپن دارای رویکرد قانونگذاری بودند و کره جنوبی، استرالیا، کانادا، اتریش، بلژیک، فرانسه، ایتالیا، کانادا، دانمارک، فنلاند، آلمان، یونان، بلژیک، نروژ، ایرلند، پرتغال، اسپانیا، سوئد، سوئیس و انگلستان ازجمله کشورهایی بودند که دارای قانونگذاری یکپارچه در عرصه حفاظت از داده‌های کاربران بودند. براساس مطالعه رویکردها، دو رویکرد متفاوت در فضای حفاظت از داده‌های کاربران وجود دارد که یکی از آنها رویکرد ایالات متحده آمریکاست و دیگری رویکرد اروپایی است. ایالات متحده آمریکا در فناوری اطلاعات و اینترنت هم از نظر فنی و زیرساختی و هم از نظر قانونگذاری پیشتازتر از سایر کشورها بوده است، اما 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

1. Sectoral
2. Omnibus

قانونگذاری درخصوص حریم خصوصی و رویکرد خودتنظیمی در بخش‌های مختلف این موضوع، فاقد قانونی جامع در این زمینه است. رویکرد اروپایی در مورد حریم خصوصی کاربران در فضای مجازی رویکردی جامع 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... مد نظر 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 حریم خصوصی کاربران در فضای مجازی پرداخته‌اند و در آن، برخلاف ایالات متحده آمریکا، از داده‌های شخصی گردآوری شده توسط نهادهای دولتی نیز حمایت کرده‌اند. با توجه به این موضوع، در این گزارش به مطالعه قوانین کشورهای منتخب با رویکرد اروپایی که دارای قانون جامع و یکپارچه هستند، پرداخته شده است. بر این اساس در ادامه قوانین، نحوه قانونگذاری، ساختار اجرایی و نظارتی حریم خصوصی در فضای مجازی در کشورهای ۱۱ گانه منتخب (کره جنوبی، فرانسه، انگلستان، کانادا، اسپانیا، نروژ، سوئد، آلمان، ایرلند، ایتالیا و بلژیک) بررسی شده است.

۱. کره جنوبی

«قانون حمایت از اطلاعات شخصی»[1] کره جنوبی در ۲۹ مارس ۲۰۱۱ به تصویب مجلس قانونگذاری این کشور رسید و در ۳۱ مارس ۲۰۱۲ توسط دولت این کشور اجرایی شد. این قانون سختگیرانه‌ترین و جامع‌ترین قانون حفاظت از حریم خصوصی کاربران در فضای مجازی در میان کشورهای دنیا شناخته می‌شود (گرینلیف و پارک،[2] ۲۰۱۲). قانون حمایت از حریم خصوصی کاربران در فضای مجازی در کره جنوبی به‌اختصار با عنوان PIPA شناخته می‌شود. این قانون شامل هشت فصل و یک پیوست است که درمجموع دارای ۸۱ بند هستند. قانون قبلی کره جنوبی اشکالات زیادی دارد. یکی از این اشکالات، محدود بودن حوزه قانون در بخش خصوصی تنها به شرکت‌های خدمات‌دهنده خدمات ارتباط از راه دور بود. اما در قانون جدید این مشکل برطرف شده است. همچنین حوزه قانون جدید، شامل تمامی سازمان‌های بخش دولتی نیز می‌شود. «قانون جدید حفاظت از داده در کره جنوبی علاوه‌بر جامع بودن، ویژگی‌های زیر را نیز داراست:

- کمیسیون حفاظت از اطلاعات شخصی که ۱۵ عضو مستقل دارد،
- الزام بنگاه‌های تجاری و سازمان‌های دولتی به نصب مأموران حافظ انطباق با قوانین حریم خصوصی،[3]
- لزوم اطلاع‌رسانی به افراد آسیب‌دیده و نیز نهادهای نظارتی در صورت بروز هرگونه مسائل امنیتی و نشر داده‌های شخصی افراد،

1. Personal Information Protection Act
2. Greenleaf & Park
3. Privacy Compliance Officers

- لزوم انجام ارزیابی آثار حریم خصوصی[1] برای سامانه‌های بخش دولتی آسیب‌پذیر،
- الزام سازمان‌ها به اخذ رضایت آشکار افراد برای مقاصد بازاریابی با استفاده از پایگاه‌های داده خود سازمان‌ها» (گرینلیف و پارک، ۲۰۱۲).

نهاد ناظر بر حسن اجرای قوانین حمایت از حریم خصوصی کاربران در فضای مجازی در کره جنوبی برعهده سازمانی با عنوان «کمیسیون حفاظت از اطلاعات شخصی»[2] است. این کمیسیون تحت نظر نهاد ریاست‌جمهوری کره جنوبی تشکیل می‌شود و وظیفه حل‌وفصل تمامی مسائل مرتبط با حریم خصوصی کاربران در فضای مجازی را دارد. ریاست این کمیسیون را رئیس‌جمهور کره جنوبی و از میان چهره‌های غیروابسته به دولت منتصب می‌کند. همچنین قائم‌مقام ریاست کمیسیون نیز توسط رئیس‌جمهور و از میان چهره‌های سیاسی دولتی انتخاب می‌شود. از میان حداکثر ۱۵ عضو این کمیسیون، ۵ نفر از منتخبین مردم در مجلس شورای ملی انتخاب می‌شوند و ۵ نفر دیگر توسط ریاست قوه قضائیه (دادگاه عالی کره جنوبی) انتخاب می‌شوند. این افراد از میان خبرگان معرفی شده توسط گروه‌های حمایت از مشتریان، نهادهای مردمی و سازمان‌های مردم‌نهاد مرتبط با حقوق حریم خصوصی شهروندان، اتحادیه‌های تجاری پردازشگر (پیمانکار)ان داده‌های شخصی و سایر نخبگان دانشگاهی با دانش مرتبط با اطلاعات خصوصی کافی انتخاب می‌شوند. ریاست کمیسیون حفاظت از اطلاعات شخصی در کره جنوبی حداکثر سه‌سال بوده و می‌تواند تنها یک بار برای یک دوره سه‌ساله دیگر تمدید شود. رأی‌گیری‌های انجام شده در این کمیسیون، پیرامون مسائل مرتبط با حریم خصوصی کاربران در فضای مجازی با رأی حداقل نیمی از اعضا وجهه قانونی پیدا کرده و اجرای آنها برای سازمان‌های مختلف ضروری است. یکی از مهمترین وظایف این کمیسیون رسیدگی به برنامه‌ریزی برای حمایت از حریم خصوصی اطلاعات است که با عنوان «طرح اولیه»[3] شناخته می‌شود. طرح اولیه هر سه‌سال یک بار توسط وزارت مدیریت عمومی و امنیت[4] تدوین و در اختیار کمیسیون حفاظت از اطلاعات شخصی قرار می‌گیرد تا این کمیسیون آن را بازبینی و برای اجرا نهایی سازد. این برنامه شامل موارد زیر است:

- اهداف اولیه و چشم‌انداز حفاظت از داده‌ها،
- بهبود سامانه‌ها و قانونگذاری حفاظت از داده،
- اقدامات متقابل[5] برای پیشگیری از نقض حریم خصوصی شهروندان،
- چگونگی تسهیل قانونگذاری در زمینه حفاظت از داده‌های شخصی،
- چگونگی فراهم نمودن برنامه‌های آموزشی و روابط عمومی در زمینه حفاظت از داده،

1. Privacy Impact Assessment
2. The Personal Information Protection Commission
3. Basic Plan
4. Public Administration and Security
5. Countermeasures

- آموزش و پرورش متخصصان در حفاظت از داده،
- و سایر اقدامات لازم در زمینه حفاظت از داده‌های شخصی (قانون حمایت از اطلاعات شخصی کره جنوبی، ۲۰۱۱، بند «۵»).

طرح اولیه اقدامی اساسی است که برای شناسایی نقاط ضعف قوانین حمایت از حریم خصوصی کاربران در فضای مجازی و رفع آنها و بهبود پیوسته این قوانین صورت می‌گیرد.

سازمان‌های دولتی که در کره جنوبی به پردازش داده‌های شخصی شهروندان مشغولند باید تمامی فعالیت‌های خود را (شامل نام فایل‌های شخصی گردآوری یا نگهداری شده، مبانی حقوقی و اهداف نگهداری داده‌های شخصی و نیز مدت‌زمان نگهداری آنها) به «وزارت اجرائیات و امور داخلی دولتی»[1] اعلام کنند. این وزرات نیز به انتشار وضعیت اطلاعات ثبت شده به‌صورت آنلاین برای آگاهی عموم شهروندان از نحوه گردآوری یا نگهداری داده‌های شخصی توسط سازمان‌های دولتی ملزم است. البته سازمان‌های بخش خصوصی برای این کار ملزم نشده‌اند. سازمان‌های مختلف خصوصی و دولتی ملزم شده‌اند تا فردی را به‌عنوان «مأمور ارشد حریم خصوصی»[2] یا افسر ارشد حریم خصوصی تعیین کنند.[3] افسر ارشد باید وظایف زیر را در زمینه حفاظت از حریم خصوصی شهروندان در سازمان خود به انجام رساند:

- تدوین برنامه حفاظت از داده‌های شخصی،
- مطالعه منظم پردازش داده‌های شخصی و ایجاد بهبودهای لازم در این خصوص،
- رسیدگی به شکایات واصله از طرف شهروندان به سازمان،
- استقرار سامانه‌های کنترل درون‌سازمانی برای پیشگیری از نشت داده‌ها[4] و سوءاستفاده احتمالی از آنها،
- نظارت، مدیریت و حفاظت از فایل‌های حاوی اطلاعات شخصی،
- انجام سایر وظایفی که توسط نماینده کمیسیون حفاظت از اطلاعات شخصی تعیین خواهد شد (کیم و همکاران،[5] ۲۰۱۵).

1. Ministry of Government Administration and Home Affarirs
2. Chief Privacy Officer
3. https://clientsites.linklaters.com/Clients/dataprotected/Pages/RepublicofKorea.aspx
4. Data leakage
5. Kim et al.

۲. فرانسه

در فرانسه، قانون حمایت از حریم خصوصی کاربران در فضای مجازی با عنوان «قانون حفاظت از اطلاعات و آزادی: در مورد فناوری اطلاعات، فایل‌های داده و آزادی‌های مدنی»[1] نام دارد. این قانون مشتمل بر ۸ فصل و ۷۲ بند است. این قانون با عنوان قانون حمایت از داده نیز شناخته می‌شود که در ۶ ژانویه سال ۱۹۷۸ به تصویب مجلس قانونگذاری این کشور رسید. این قانون چندین بار اصلاح شد که آخرین بار آن در ۷ اوت سال ۲۰۰۴ بوده است. در قانون فوق میان کنترل‌گر و سازمان‌های پردازشگر (پیمانکار) داده‌های شخصی شهروندان تمایز ایجاد شده است. کنترل‌گر فرد یا سازمانی دولتی یا خصوصی است که تعیین‌کننده اهداف و روش‌های پردازش داده است. در مقابل پردازشگر (پیمانکار) فرد (یا عموماً یک پیمانکار) است که تحت فرمان کنترل‌گر به پردازش داده‌های شخصی براساس دستورالعمل‌های کنترل‌گر اقدام می‌کند. در قانون فرانسه به این علت که متولی اصلی همان کنترل‌گر شناخته می‌شود، اغلب قوانین متوجه کنترل‌گر هستند؛ زیرا نهاد اصلی تصمیم‌گیر در مورد پردازش داده‌های شخصی شهروندان، کنترل‌گر شناخته می‌شود و مسئولیت اصلی حفظ حریم خصوصی کاربران در فضای مجازی، برعهده کنترل‌گر گذارده شده است. طبق بند «۲» این قانون، داده‌های شخصی[2] «هر نوع اطلاعاتی هستند که به یک شخص حقیقی که به‌صورت مستقیم یا غیرمستقیم از طریق ارجاع با یک کد شناسایی یا یک یا چند فاکتور دیگر، قابل شناسایی باشد» اطلاق می‌شود. به‌عنوان مثال، شهروندان می‌توانند به‌صورت مستقیم یا غیرمستقیم از طریق نام، تاریخ تولد، شماره تلفن، آدرس ایمیل، شماره کد ملی و... شناسایی شوند. بنابراین کنترل‌گرها و پردازشگر (پیمانکار)ها باید این موضوع را در نظر داشته باشند که آیا داده‌های شخصی که از شهروندان در اختیار دارند، امکان شناسایی آنان را فراهم می‌آورد یا خیر (قانون حمایت از داده فرانسه،[3] ۲۰۱۴، بند «۲»).

حوزه قانون حمایت از داده در فرانسه شامل آن دسته از کنترل‌گرها و پردازشگر (پیمانکار)هایی می‌شود که دارای یکی از این ویژگی‌ها باشند: ۱. در فرانسه حضور داشته باشند؛ ۲. سرور خدمات هاستینگ[4] آنها در فرانسه مستقر باشد؛ ۳. فراهم‌کننده خدمات خارجی[5] که در خاک فرانسه مستقر باشد (فیلیپه،[6] ۲۰۱۵).

ازآنجاکه بسیاری از خدمات دولت الکترونیک مبتنی‌بر پردازش خودکار داده‌های شخصی شهروندان هستند، در فرانسه همچون برخی کشورهای منتخب، به شهروندان حقی برای آگاهی از منطق پردازش

1. Loi Informatique Et Libertes On Information Technology, Data Files And Civil Liberties
2. Personal Data
3. The French Data Protection Act
4. Hosting Server
5. External Service Provider
6. Philippe

خودکار[1] داده‌های شخصی‌شان داده شده است. در پردازش دستی یا غیرخودکار داده‌های شخصی، داده‌های مربوط به شهروندان توسط انسان با مشایعت یک سیستم رایانه‌ای پردازش می‌شوند، اما در پردازش خودکار داده‌های شخصی، عملیات پردازش تماماً توسط سیستم رایانه‌ای صورت می‌گیرد، بنابراین امکان بروز خطا در عملیات پردازش وجود دارد و ممکن است شهروند از حقوق خود همچون خدمات دولت الکترونیک محروم شود؛ باوجود حق شهروند برای آگاهی از منطق تصمیم‌گیری مبتنی‌بر پردازش خودکار داده‌های شخصی وی، در فرانسه برخلاف برخی کشورهای منتخب، به وی حق درخواست پردازش داده‌ها به‌صورت دستی یا توسط انسان داده نشده است (**همان**).

وظیفه نظارت بر حسن اجرای قانون حمایت از حریم خصوصی کاربران در فضای مجازی در فرانسه برعهده سازمانی به نام «مرجع حمایت از داده فرانسه»[2] است که وظایف آن در قانون حمایت از داده تعریف شده است. اعضای این مرجع حداقل ۱۷ نفر هستند که شامل دو نفر از اعضای مجلس ملی فرانسه، دو نفر از اعضای سنا، دو نفر از اعضای شورای اقتصادی، اجتماعی و محیطی،[3] دو نفر از اعضا یا اعضای ادوار قبلی دادگاه عالی اجرایی فرانسه،[4] دو نفر از اعضا یا اعضای ادوار قبلی دادگاه عالی قضایی فرانسه،[5] دو نفر از اعضا یا اعضای ادوار قبلی دادگاه حسابداری فرانسه،[6] سه نفر از چهره‌های سیاسی با دانش و تخصص مرتبط با فناوری اطلاعات و حقوق شهروندی منتخب رئیس‌جمهوری و دو نفر از چهره‌های سیاسی با دانش و تخصص مرتبط با فناوری اطلاعات و حقوق شهروندی منتخب مجلس ملی فرانسه (و مورد تأیید رئیس‌جمهور و سنای فرانسه) هستند. علاوه‌بر این ۱۷ عضو، بازرس حقوق شهروندان[7] یا نمایندگان وی که حق رأی در این مرجع را دارند باید در جلسات حضور داشته باشند. رئیس و دو نایب رئیس مرجع که تشکیل کمیته اجرایی را می‌دهند با انتخابات درونی انتخاب می‌شوند. طبق این قانون، مهمترین وظایف این مرجع به‌شرح زیر است:

- رسیدگی به درخواست‌های سازمان‌های دولتی و خصوصی در مورد پردازش داده‌های شخصی و تصدیق عملیات پردازش آنها،
- اعطای گواهی تصدیق عملیات پردازش داده‌های شخصی شهروندان به سازمان‌های دولتی یا خصوصی که قصد انجام عملیات پردازش داده‌های شخصی را دارند،
- تدوین استانداردهایی برای ارتقای امنیت سامانه‌های اطلاعاتی که داده‌های شخصی را پردازش می‌کنند،

1. Automatic processing
2. French Data Protection Authority (Commission Nationale Informatique et Libertés (CNIL)
3. Conseil économique, social et environnemental (Economic, Social & Environmental Council)
4. The French Administrative High Court
5. The French Judicial High Court
6. Accounting Court
7. “Défenseur des Droits” (Civil Rights Ombudsman)

- دریافت و رسیدگی به شکایات مربوط به پردازش داده‌های شخصی شهروندان و ابلاغ تصمیم‌گیری‌های اتخاذ شده به افراد و نهادهای درگیر،
- پاسخگویی به سازمان‌های دولتی که قصد ایجاد سامانه‌های پردازش خودکار داده‌های شخصی را دارند،
- تسلیم اطلاعاتی که در اختیار مرجع است به نهادها و مراجع قضایی مرتبط با جرائم رایانه‌ای درخصوص مسائل مرتبط با نقض حریم خصوصی کاربران در فضای مجازی،
- پاسخگویی به سازمان‌های دولتی و خصوصی در زمینه سؤالات آنها در مورد قانون حمایت از داده و اینکه آیا عملیات خاصی از پردازش داده‌های شخصی با این قانون مغایرت دارد یا خیر،
- به‌روزرسانی دانش مرتبط با حوزه فناوری اطلاعات،
- انتشار عمومی ارزیابی‌های انجام شده در مورد نحوه اعطای حقوق شهروندان در زمینه حریم خصوصی کاربران در فضای مجازی و آزادی‌های آنان جهت ایجاد شفافیت بیشتر در این زمینه،
- مشورت‌دهی به کمیسیون‌های مرتبط تعیین شده توسط نهاد ریاست‌جمهوری،
- پیشنهاد الزامات قانونی و تمهیدات امنیتی به دولت برای حفاظت از حریم خصوصی کاربران در فضای مجازی مطابق با آزادی‌های مدنی و پیشرفت‌های صورت گرفته در حوزه پردازش رایانه‌ای،
- مشایعت سایر سازمان‌های دولتی در زمینه حفاظت از داده‌های شخصی شهروندان در صورت تقاضای آنها،
- کمک به مذاکرات بین‌المللی دولت در زمینه حفاظت از داده‌های شخصی شهروندان.

همچنین این مرجع موظف شده است تا علاوه‌بر وظایف فوق، گزارشی را به‌صورت سالیانه تدوین کند که در عملکرد خود را تشریح کرده و به رئیس‌جمهور، نخست‌وزیر و پارلمان فرانسه برساند (وب‌سایت رسمی مرجع حمایت از داده فرانسه[1]).

در قانون فرانسه سازمان‌های دولتی و خصوصی موظف شده‌اند پیش از اقدام به پردازش داده‌های شخصی شهروندان، مراتب را به «مرجع حمایت از داده فرانسه (CNIL)» اطلاع دهند و تنها در صورتی به انجام عملیات پردازش مجاز هستند که این مرجع تصدیق مجاز بودن عملیات پردازش را به آنها بدهد. روند دریافت گواهی تصدیق عملیات پردازش به این‌صورت است که سازمان‌های دولتی یا خصوصی که قصد گردآوری داده‌های شخصی کاربران در فضای مجازی را دارند، باید ابتدا مواردی همچون موارد زیر را به اطلاع آن مرجع برسانند:

- اهداف پردازش داده‌های شخصی،
- هویت و اطلاعات تماس با خود،

1. https://www. cnil. fr/en/home

- ارتباطات احتمالی میان پایگاه‌های داده،
- نوع داده‌هایی که قرار است پردازش شوند،
- دریافت‌کنندگان احتمالی و نوع داده‌هایی که قرار است به آنها افشا شود،
- بازه زمانی که قرار است داده‌های شخصی نگهداری شوند،
- افراد مسئول یا بخش‌های مسئول عملیات پردازش در سازمان،
- کشورهایی که قرار است داده‌های شخصی شهروندان به آنها منتقل شود (درصورتی‌که آن کشورها خارج از اتحادیه اروپا باشند)،
- تمهیدات امنیتی اندیشیده شده برای حفاظت از امنیت داده‌های شخصی.

آگاه‌سازی مرجع حفاظت از داده به‌صورت آنلاین و از طریق وب‌سایت آن سازمان صورت می‌گیرد. سپس مرجع حفاظت از داده ظرف مدت محدودی ـ حدوداً چند روز ـ در صورت صلاحدید گواهی تصدیق عملیات پردازش را به سازمان اعطا می‌کند (قانون حمایت از داده فرانسه،[1] ۲۰۱۴، بندهای «۱۵-۱۲»).

۳. انگلستان

«قانون حمایت از داده انگلستان»[2] برای اولین بار در سال ۱۹۹۸ توسط مجلس قانونگذاری این کشور تصویب و آخرین اصلاحات آن در ۶ نوامبر ۲۰۱۵ به انجام رسیده است و مشتمل بر ۱۶ سرفصل است. در قانون حمایت از داده انگلستان، داده‌های شخصی که مربوط به یک فرد زنده هستند یا از دو طریق زیر یک فرد را قابل شناسایی نمایند به تحت حمایت قرار می‌گیرند: ۱. از طریق خود داده‌ها، ۲. از طریق ترکیب داده‌ها با هر نوع اطلاعاتی که در اختیار کنترل‌گر قرار داشته باشد یا بعداً در اختیار وی قرار گیرد. داده‌های شخصی که موردحمایت قانون فوق قرار می‌گیرند عبارتند از:

- داده‌های شخصی که بر روی سیستم رایانه‌ای ذخیره شده‌اند یا قرار است ذخیره شوند.
- داده‌های شخصی که در یک سیستم فایلینگ[3] ذخیره شده‌اند یا به یک سیستم فایلینگ شکل می‌دهند. این نوع داده‌ها به اطلاعات پردازش شده به‌صورت خودکار که از طریق ابزارهای الکترونیکی گردآوری شده‌اند و ساختارمند هستند اشاره دارد.
- هر نوع داده‌ای که قابل دسترسی باشد شامل:

ـ داده‌های سلامت در اختیار نهادهای حرفه‌ای بهداشتی،

ـ داده‌های آموزشی،

1. The French Data Protection Act
2. The Data Protection Act, 1998.
3. Filing System

ـ داده‌های عمومی در اختیار نهادهای دولتی برای ارائه خدمات دولتی و اجتماعی،

ـ و سایر اشکال داده‌های در اختیار نهادهای دولتی.

مهمترین اصول حمایت از داده‌های شخصی در قانون انگلستان، که به‌عنوان اصول زیربنایی قوانین حمایت از داده شناخته می‌شوند، به‌شرح زیر هستند:

- داده‌های شخصی باید به‌صورت قانونی و منصفانه پردازش شوند؛
- باید تناسبی میان داده‌های شخصی پردازش شده و اهداف پردازش وجود داشته باشد و نباید بیش از آنچه مورد نیاز است اقدام به پردازش کرد؛
- داده‌های شخصی باید دقیق بوده و در صورت ضرورت به‌روزرسانی شوند؛
- نباید داده‌های شخصی را بیش از زمان مورد نیاز برای رسیدن به اهداف نگهداری کرد؛
- پردازش داده‌های شخصی باید سازگار با حقوقی باشد که شهروندان در این خصوص از آنها برخوردارند؛
- داده‌های شخصی باید با تمهیدات فنی و سازمانی مناسب امنیتی، در برابر پردازش‌های غیرمجاز و همچنین از بین رفتن یا تخریب تصادفی محافظت شده باشند؛
- داده‌های شخصی باید در مقابل انتقال به کشورهای ثالثی که دارای سطوح کافی امنیت از حقوق و آزادی‌های شهروندان نیستند، محافظت شوند (قانون حمایت از داده انگلستان، ۲۰۱۵).

در قانون حمایت از داده انگلستان، سازمان‌های دولتی یا خصوصی یا اشخاصی که به‌صورت فردی به گردآوری یا استفاده یا افشای داده‌های شخصی شهروندان اقدام کنند، درصورتی‌که تصمیم‌گیری در مورد اهداف این عملیات پردازش با خود آنها باشد، کنترل‌گر و درصورتی‌که تحت فرامین سازمانی دیگر به این امر مشغول شده باشند، پردازشگر (پیمانکار) داده‌های شخصی نامیده می‌شوند. افراد و سازمان‌های کنترل‌گر به‌عنوان اصلی‌ترین مسئولان حفاظت از حریم خصوصی کاربران در فضای مجازی شناخته می‌شوند. آنها می‌توانند شامل موارد زیر باشند:

- شهروندان مقیم انگلستان،
- شرکت‌های خصوصی ثبت شده در انگلستان،
- سازمان‌های دولتی انگلستان،
- سایر سازمان‌هایی که یک دفتر، شعبه یا فعالیت منظم در انگلستان دارند.

در این قانون سایر شرکت‌های خارجی که قصد فعالیت در انگلستان را دارند، ازجمله شرکت‌های اینترنتی به رعایت مفاد آن ملزم شده‌اند. کنترل‌گرها باید پیش از اقدام به هرگونه پردازش داده‌های شخصی برخی اطلاعات خاص را به آگاهی دفتر کمیسیونر اطلاعات (ICO)[1] برسانند. این اطلاعات

1. Information Commissioner’s Office (ICO)

شامل موارد زیر می‌شوند:

- نام و آدرس کنترل‌گر داده‌های شخصی،
- توصیفاتی درخصوص داده‌های شخصی پردازش شده،
- اهداف پردازش داده‌های شخصی (بوردمن،[1] ۲۰۱۵).

دفتر کمیسیونر اطلاعات (ICO) نیز که وظیفه نظارت بر حسن اجرای قوانین حمایت از حریم خصوصی کاربران در فضای مجازی در انگلستان را برعهده دارد، موظف است اطلاعات دریافتی از طرف کنترل‌گرها را در یک رجیستری که توسط عموم شهروندان قابل دستیابی آنلاین و جستجو است نگهداری کند. این دفتر مستقیماً به پارلمان انگلستان گزارش می‌دهد. ریاست این دفتر برعهده کمیسیونر اطلاعات است که فردی مستقل است و توسط پادشاهی انگلستان منصوب می‌شود. مأموریت اصلی این دفتر «حمایت از حقوق حریم خصوصی کاربران در فضای مجازی در جهت منافع عمومی، ترویج آزادی از طریق مؤسسات دولتی و حفظ حریم خصوصی کاربران در فضای مجازی» است. مهمترین وظایف دفتر کمیسیونر اطلاعات به‌شرح زیر هستند:

- ثبت اطلاعات مربوط به کنترل‌گرهای داده‌های شخصی،
- رسیدگی به شکایات دریافت شده ازسوی شهروندان درباره مسائل مرتبط به حریم خصوصی کاربران در فضای مجازی،
- اعمال قانون سازمان‌های دولتی و خصوصی که مشغول گردآوری، استفاده یا نگهداری داده‌های شخصی شهروندان هستند. این اعمال قانون می‌تواند شامل تعقیب قضایی مجرمان، اجرای قانون عاری از جرم و ممیزی عملکرد چنین سازمان‌هایی باشد. بدین منظور فعالیت‌های زیر توسط این دفتر صورت می‌گیرد:

ـ ارسال اخطاریه‌هایی به کنترل‌گرها تا اطلاعات خاصی در مورد عملکردشان درخصوص پردازش داده‌های شخصی شهروندان را ظرف مدت معلومی به اطلاع این دفتر برسانند،

ـ اعلام وظایفی که یک سازمان خاص باید در قبال شکایت دریافت شده از شهروندان در مورد حریم خصوصی کاربران در فضای مجازی به انجام رساند،

ـ ارسال اخطاریه «اکنون عملیات پردازش را متوقف کنید» هنگام آگاهی از وقوع رخنه‌های امنیتی در یک سازمان به‌منظور الزام سازمان به انجام اقدامات امنیتی ضروری برای حفاظت از حریم خصوصی کاربران در فضای مجازی،

ـ انجام ممیزی‌هایی برای سنجش نحوه عملکرد سازمان‌های مختلف در مورد حفاظت از حریم خصوصی کاربران در فضای مجازی،

1. Boardman

ـ ارسال نتایج ممیزی عملکرد سازمان‌ها به خود سازمان‌ها برای اطمینان‌دهی به آنها درخصوص عملکرد مناسبشان در قبال حفاظت از حریم خصوصی کاربران در فضای مجازی،

ـ اعمال جریمه‌های پولی برای سازمان‌هایی که به‌نوعی موجب نقض حریم خصوصی شهروندان شده‌اند،

ـ تعقیب قضایی افرادی که مرتکب جرائمی در زمینه حریم خصوصی کاربران در فضای مجازی شده‌اند،

ـ ارسال گزارش به پارلمان انگلستان در مورد مسائل مرتبط با حریم خصوصی کاربران در فضای مجازی (سایت رسمی دفتر کمیسیونر اطلاعات انگلستان).[1]

۴. کانادا

در اواخر دهه ۱۹۶۰ و اوایل ۱۹۷۰ میلادی، دولت کانادا اولین قانون حفاظت از حریم خصوصی را در بخش چهارم از قانون حقوق انسانی کانادا[2] در سال ۱۹۷۷ مصوب کرد. در این قانون اولیه، کمیسیونر حریم خصوصی کانادا[3] که عضوی از کمیسیون حقوق انسانی کانادا بود، موظف شد تا شکایات عمومی را دریافت، بازرسی‌های لازم را انجام و پیشنهادهایی برای تغییر قانون حریم خصوصی به مجلس قانونگذاری کانادا ارائه دهد. بعدها به‌دلیل تطابق با اصول بین‌المللی حمایت از حریم خصوصی، به‌خصوص اصول مطرح شده در سازمان همکاری و توسعه اقتصادی (OECD)[4]، قانون حفاظت از حریم خصوصی که خیلی هم کامل نبود، ارتقا پیدا کرد. قانون کنونی حمایت از حریم خصوصی کاربران در فضای مجازی در کانادا در اول جولای سال ۱۹۸۳ در مجلس قانونگذاری کانادا تصویب شد و آخرین نسخه آن تا سال ۲۰۱۶ با تغییرات جزئی به‌طور جدی مورد اجرا قرارگرفت. در سال ۱۹۹۸، قوه قضائیه کانادا مقاله‌ای را با عنوان «حفاظت از اطلاعات شخصی: ایجاد اقتصاد و جامعه اطلاعاتی کانادا» منتشر کرد که در آن بر جلب اعتماد مشتریان جهت رشد اقتصاد اطلاعاتی تمرکز شده بود. همچنین در آن این‌گونه نتیجه‌گیری شده بود که امکان سوءاستفاده از اطلاعات مشتریان در نتیجه نبود قانونی جامع برای حفاظت از اطلاعات شخصی آنان، وجود دارد و قوانین موجود در کانادا در حوزه تجارت الکترونیک دچار نقصان هستند. نتیجه انتشار این مقاله تلاش مجلس قانونگذاری کانادا برای تصویب قانونی جداگانه برای بخش خصوصی در همان سال بود: قانون حفاظت از اطلاعات شخصی و اسناد الکترونیکی.[5] در اول ژانویه سال ۲۰۰۱ اصلاحیه این قانون در مجلس قانونگذاری کانادا تصویب شد. این قانون نارسایی‌های موجود در حفاظت از حریم خصوصی مشتریان در تجارت الکترونیک را تا حد زیادی برطرف کرد (هولمز،[6] ۲۰۰۸).

1. https://ico. org. uk/
2. Canadian Human Rights Act
3. the Privacy Commissioner of Canada
4. Organization for Economic Cooperation and Development
5. the Personal Information Protection and Electronic Documents Act
6. Holmes

هدف قانون حمایت از حریم خصوصی در کانادا «حفاظت از حریم خصوصی افراد در قبال اطلاعات شخصی درباره آنها که توسط نهادهای دولتی نگهداری می‌شوند و نیز فراهم کردن حق دسترسی به اطلاعات برای افراد است». در این قانون اطلاعات شخصی[1] به معنای «اطلاعات درباره یک فرد قابل شناسایی[2] که به هر شکل ممکن ضبط شده باشد شامل موارد زیر، تعریف شده است:

الف) اطلاعات مربوط به نژاد، ملیت، قومیت، رنگ، مذهب، سن یا وضعیت تأهل فرد،

ب) اطلاعات مربوط به سوابق آموزشی، پزشکی، کیفری یا استخدامی فرد یا اطلاعات در مورد تراکنش‌های مالی که فرد داشته است،

ج) هر شماره، نماد یا دیگر سمبل‌های خاص مربوط به فرد که وی را قابل شناسایی کند،

د) آدرس، اثر انگشت یا گروه خونی فرد،

هـ) نظرات یا دیدگاه‌های فرد بجز هنگامی‌که دیدگاه‌ها در مورد فرد حقیقی یا حقوقی یا فرد وابسته به دولت یا جوایز و نشان‌های اخذ شده در گذشته یا آینده توسط آن فرد باشد،

و) مکاتبات انجام شده میان فرد و نهاد دولتی که به‌صورت ضمنی یا آشکار ماهیتی محرمانه[3] داشته و پاسخ‌های داده شده به این مکاتبات که افشاکننده مبدأ آن می‌باشد،

ز) نظرات و دیدگاه‌های یک فرد دیگر در مورد وی،

ح) نظرات فردی دیگر در مورد پیشنهاد جایزه، هدیه یا پاداشی که به یک فرد توسط یک نهاد یا بخشی از نهاد باید داده شود،

ط) نام فرد هنگامی‌که با اطلاعات شخصی مربوط به وی همراه می‌شود یا هنگامی‌که افشای نام به‌تنهایی باعث افشای اطلاعات در مورد فرد شود». (قانون حریم خصوصی کانادا،[4] ۲۰۱۶: ۳).

هولمز[5](۲۰۰۸) معتقد است قانون حریم خصوصی کانادا سه مؤلفه اصلی دارد: ۱. به شهروندان حق قانونی دسترسی به اطلاعات شخصی آنها که توسط نهادهای دولتی نگهداری می‌شود را می‌دهد؛ ۲. در آن الزامات منصفانه‌ای برای روش‌های گردآوری، استفاده، نگهداری و افشای اطلاعات شخصی شهروندان که در کنترل نهادهای دولتی است، تعیین شده است؛ ۳. در آن یک بازرس مستقل[6] با عنوان «کمیسیونر حریم خصوصی»[7] برای برطرف کردن مشکلات و نظارت بر تطابق عملکرد سازمان‌های دولتی با قانون معین شده است. وی معتقد است مهمترین اصل زیربنایی در این قانون این است که اطلاعات شخصی تحت کنترل دولت نباید بدون رضایت شهروند مورد استفاده قرار گیرند، مگر اینکه این نوع استفاده از

1. Personal Information
2. Identifiable
3. Confidential
4. Canada Privacy Act
5. Holmes
6. Independent Ombudsman
7. The Privacy Commissioner

اطلاعات در تطابق با اهداف گردآوری توسط نهاد دولتی باشد یا برای استفاده با هدفی سازگار با اهداف اعلام شده به شهروند صورت گیرد. تمامی شهروندان در کانادا حق دسترسی به اطلاعاتی را دارند که در مورد آنها توسط نهادهای دولتی نگهداری می‌شود. همچنین اگر شهروند از دقت اطلاعات راضی نباشد، می‌تواند تقاضای اصلاح اطلاعات را به آن سازمان بدهد. همچنین وی می‌تواند مشکلات به‌وجود آمده در مسیر دستیابی یا اصلاح اطلاعات شخصی‌اش را به کمیسیونر حریم خصوصی گزارش دهد. درصورتی‌که شهروند از روند پیگیری شکایت خود توسط کمیسیونر حریم خصوصی رضایت نداشته باشد، می‌تواند شکایت خود را به دادگاه فدرال کانادا تسلیم کند (هولمز، ۲۰۰۸).

در پاسخ به اصول سازمان همکاری و توسعه اقتصادی (OECD)، کانادا نیز اصول مشابه و ۱۰ گانه‌ای را به‌عنوان اصول زیربنایی در قانون حریم خصوصی در نظر گرفته است. مهمترین اصول حمایت از اطلاعات شخصی در قانون حمایت از حریم خصوصی کانادا عبارتند از:

اصل یکم. پاسخگویی: یک سازمان مسئول اطلاعات شخصی است که تحت اختیار داشته و باید افراد مسئول برای تطابق سازمان با اصول حمایت از اطلاعات شخصی را مشخص کند.

اصل دوم. مشخص کردن اهداف: اهدافی که اطلاعات شخصی برای آنها گردآوری می‌شوند باید توسط سازمان پیش از زمان گردآوری اطلاعات تعیین شوند.

اصل سوم. رضایت: دانش و رضایت افراد برای گردآوری، استفاده یا افشای اطلاعات شخصی بجز در زمانی که غیرمناسب است، مورد نیاز است.

اصل چهارم. محدودیت گردآوری: گردآوری اطلاعات شخصی باید به اهداف گردآوری تعیین شده توسط سازمان محدود شود. اطلاعات باید از طریق روش‌های منصفانه و قانونمند گردآوری شود.

اصل پنجم. محدودیت استفاده، افشا و نگهداری: اطلاعات شخصی نباید برای اهدافی به‌جز اهداف از پیش تعیین شده در هنگام گردآوری استفاده، افشا یا نگهداری شوند مگر درصورتی‌که رضایت فرد اخذ شده باشد یا ضرورت قانونی وجود داشته باشد. اطلاعات شخصی باید تا زمانی که برای رسیدن به آن اهداف ضروری است، نگهداری شود.

اصل ششم. دقت: اطلاعات شخصی باید برای اهداف استفاده دقیق و کامل بوده و در هنگام ضرورت به‌روزرسانی شود.

اصل هفتم. تدابیر حفاظتی: اطلاعات شخصی باید با توجه به سطح حساسیت آنها، توسط تدابیر حفاظتی امنیتی مورد حفاظت قرار گیرند.

اصل هشتم. شفافیت: یک سازمان باید اطلاعات خاص در مورد روش‌ها و سیاست‌های مربوط به مدیریت اطلاعات خود را در دسترس قرار دهد.

اصل نهم. دسترسی فردی: هر فرد، در صورت درخواست باید در مورد وجود، استفاده و افشای اطلاعات شخصی مربوط به خود آگاه شده و به وی امکان دسترسی به آنها داده شود. هر فرد باید قادر

باشد تا صحت و کامل بودن اطلاعات را به چالش بکشد و بتواند آنها را اصلاح کند.

اصل دهم. هر فرد باید بتواند تطابق سازمان یا فرد و افراد مسئول حفاظت از اطلاعات شخصی خود در سازمان را با اصول فوق به چالش بکشد (هولمز، ۲۰۰۸).

یکی از مهمترین ارکان قانون حمایت از حریم خصوصی، دفتر کمیسیونر حریم خصوصی کانادا (OPC)[1] است که نهادی مستقل از دولت بوده و وظیفه نظارت بر حسن اجرای قانون حریم خصوصی را دارد. کمیسیونر حریم خصوصی توسط ریاست مجلس کانادا و با اخذ مشورت رؤسای احزاب مطرح در سنا و مجلس عوام[2] و برای مدت هفت سال تعیین می‌شود. وی همچنین چند دستیار برای کمیسیونر تعیین می‌کند. برای انجام وظایف سنگین نظارت بر حسن اجرای قوانین حفظ حریم خصوصی، کارمندانی نیز در دفتر کمیسیونر حریم خصوصی تحت قانون استخدام کارگزاران عمومی[3] استخدام می‌شوند. در صورت نیاز به متخصصان حوزه فناوری اطلاعات، کمیسیونر مجاز به عقد قرارداد موقت با افراد خبره در این حوزه در جهت انجام وظایف خود می‌باشد (قانون حریم خصوصی کانادا، ۲۰۱۶، بخش ۲، بندهای «۵۸-۵۳»). مهمترین وظایف کمیسیونر حریم خصوصی در کانادا به‌شرح زیر هستند:

الف) بازرسی داده: کمیسیونر حریم خصوصی می‌تواند در هر زمان، به بازرسی از نهادهای دولتی نگهداری کننده اطلاعات شخصی شهروندان اقدام نموده و از تطابق عملیات آنها با قانون حریم خصوصی اطمینان حاصل کند و در صورت عدم تطابق با قانون، گزارش نتیجه بازرسی را به همراه پیشنهادهای اصلاحی مورد نیاز به بالاترین مقام در آن سازمان ارائه کند (**همان**، بند «۳۷»).

ب) گزارش‌دهی به پارلمان کانادا: کمیسیونر موظف است ظرف مدت سه‌ماه پس از پایان هر سال مالی، گزارشی را به پارلمان کانادا در مورد فعالیت‌های انجام شده در طول سال توسط خود را ارائه دهد. همچنین، گزارش‌های موردی را در هر زمان دلخواه به پارلمان تسلیم نماید (**همان**، بند «۳۸»). علاوه‌بر دو مورد فوق، گزارش نتایج بازرسی‌های انجام شده از سازمان‌های مختلف دولتی به پارلمان کانادا از دیگر وظایف کمیسیونر است (**همان**، بند «۳۹»).

ج) دریافت و رسیدگی به شکایات شهروندان: یکی از وظایف مهم کمیسیونر حریم خصوصی، دریافت و رسیدگی به شکایات شهروندان است:

- شهروندانی که ادعا می‌کنند اطلاعات شخصی در مورد آنها توسط یک نهاد دولتی نگهداری شده یا مورد استفاده قرار گرفته یا افشا شده است؛
- شهروندانی که درخواست دسترسی آنها به اطلاعات شخصی‌شان توسط نهاد دولتی رد شده است؛
- شهروندانی که ادعا می‌کنند یکی از حقوق آنها در مورد حریم خصوصی کاربران در فضای مجازی

1. Office of the Privacy Commissioner of Canada (OPC)
2. House of Commons
3. Public Service Employment Act

از آنها سلب شده است؛

- شهروندانی که ادعا می‌کنند درخواست اصلاح اطلاعاتی شخصی آنها توسط نهاد دولتی رد شده است؛
- شهروندانی که ادعا می‌کنند دسترسی به اطلاعات شخصی‌شان توسط نهاد دولتی در بازه زمانی نامعقولی صورت گرفته است؛
- شهروندانی که ادعا می‌کنند دسترسی آنها به اطلاعات شخصی خود در زبانی غیررسمی یا فرمت رایانه‌ای غیرمعمول فراهم شده است؛
- شهروندانی که ادعا می‌کنند برای دسترسی به اطلاعات شخصی از آنها پولی طلب شده است؛
- شهروندانی که شکایتی در مورد مسائل مربوط به گردآوری، نگهداری، افشا یا استفاده اطلاعات شخصی دارند (**همان**، بندهای «۳۰-۲۹»).

د) انجام مطالعات خاص و گزارش به وزارت دادگستری کانادا[1]

- گزارش مربوط به حفاظت از حریم خصوصی افراد،
- گزارش مربوط به امکان گسترش حقوق شهروندان در مورد حریم خصوصی کاربران در فضای مجازی،
- گزارش مربوط به گردآوری، نگهداری یا نابودسازی، افشا یا استفاده از اطلاعات شخصی افراد توسط اشخاص حقیقی یا بخش‌ها و سازمان‌های دولتی یا غیردولتی (**همان**، بند «۶۰»).

۵. اسپانیا

«قانون حفاظت از داده اسپانیا»[2] در سال ۱۹۹۹ به تصویب مجلس قانونگذاری این کشور رسید و بعدها، نسخه اصلاح شده آن در ۲۱ دسامبر ۲۰۰۷ با حکم پادشاه این کشور تأیید شد و در سال ۲۰۰۸ اجرایی شد. در اسپانیا هم همچون کشورهای منتخب مورد بررسی، رویکرد اروپایی حمایت از حریم خصوصی کاربران در فضای مجازی در پیش گرفته شده است؛ به‌طوری‌که در این کشور قوانین بخشی خاصی وجود ندارد (مثلاً برای بخش بهداشت و درمان، آموزش، امور مالی و...) بلکه قانون جامع حمایت از داده با رویکردی کل‌نگر، الزامات حفاظت از حریم خصوصی کاربران در فضای مجازی را برای تمامی بخش‌های دولتی و خصوصی این کشور مطرح کرده است (کاترکازاس،[3] ۲۰۱۵). در اسپانیا، داده‌های شخصی اشاره به تمامی اطلاعات مربوط به یک شخص حقیقی شناخته شده یا قابل شناسایی ـ که با عنوان سوژه شناخته می‌شود ـ دارد و برای عملیات مختلف پردازش همچون گردآوری، استفاده و به‌کارگیری،

---

۱. وزارت دادگستری نیز موظف است حداکثر ظرف مدت ۵۰ روز گزارش‌هاي دريافت شده را به پارلمان کانادا تسلیم کند (Canada Privacy Act, 2016: Sch. II "60").

2. The Data Protection Act (Law 15/1999 on the protection of personal data)

3. Cuatrecasas

ذخیره‌سازی و حذف و همچنین افشای داده‌های شخصی در این قانون قوانینی مطرح شده است. حوزه قانون فوق شامل سازمان‌های دولتی و خصوصی می‌شود که شرایط زیر را داشته باشند:

- پردازش داده توسط یک کنترل‌گر در خاک اسپانیا به انجام رسیده باشد یا کنترل‌گر از یک پردازشگر (پیمانکار) استفاده کند که زیرساخت‌های فیزیکی آن در خاک اسپانیا قرار گرفته باشد.
- پردازش داده توسط یک کنترل‌گر داده که در خارج از خاک اسپانیا قرار گرفته است انجام گیرد که آن کشور مشمول قوانین اسپانیا باشد یا طبق قوانین بین‌المللی به رعایت قوانین اسپانیا ملزم باشد.
- پردازش داده‌ها توسط یک کنترل‌گر داده که در خارج از حوزه اتحادیه اروپا باشد صورت گیرد که از ابزارهای سخت‌افزاری که در خاک اسپانیا مستقر شده‌اند استفاده کند.

برای این قانون استثناهایی نیز در نظر گرفته شده است. این استثناها عبارتند از:

- داده‌های شخصی که برای استفاده‌های صرفاً شخصی توسط یک فرد حقیقی مورد استفاده قرار می‌گیرند.
- فایل‌های داده که بنا به مسائل محرمانه باید مورد حفاظت قرار گیرند.
- فایل‌های داده که برای تحقیقات پیرامون مسائل تروریسم و جرایم جدی سازمان‌یافته طبقه‌بندی شده‌اند (گویلین و سالا،[1] ۲۰۱۵).

در اسپانیا سازمان دیده‌بان حریم خصوصی کاربران در فضای مجازی، با عنوان «آژانس حفاظت از داده[2]» یا به‌اختصار AGPD[3] شناخته می‌شود که وظیفه اطمینان از انطباق سازمان‌های دولتی و خصوصی اسپانیایی با قانون حمایت از داده و حسن اجرای آن، خصوصاً در مورد حقوق شهروندان در مورد دسترسی به داده‌های شخصی و شکایت‌های آنها نسبت به پردازش غیرمجاز داده‌های شخصی‌شان را دارد. مهمترین وظایف این سازمان به‌شرح زیر هستند:

- پاسخگویی به شهروندان (سوژه‌ها)،
  - ـ رسیدگی به شکایات و درخواست‌های آنان،
  - ـ آگاه‌سازی آنان از حقوق خود که در قانون برایشان در نظر گرفته شده است،
  - ـ ارتقای کمپین‌های رسانه‌ای از طریق رسانه‌ها،
  - ـ اطمینان از دسترس‌پذیر بودن فایل‌های داده عمومی.
- رسیدگی به سازمان‌هایی که به‌دنبال پردازش داده‌ها هستند،
  - ـ درخواست از سازمان‌ها برای کسب مجوزهای قانونی (برای پردازش داده‌ها)،
  - ـ درخواست از آنها برای انجام اقدامات اصلاحی،

1. Guilayn and Sala
2. Data Protection Agency
3. Agencia Española de Protección de Datos (AGPD)

ـ اعمال قانون در صورت غیرمجاز بودن پردازش داده‌ها توسط آنها و خاتمه به پردازش داده‌های شخصی توسط آنها،

ـ تعیین جریمه برای سازمان‌های متخلف براساس مجازات‌های تعیین شده در قانون حمایت از داده،

ـ راهنمایی سازمان‌ها درخصوص اقدامات لازم برای انجام وظایفشان در زمینه حفاظت از داده‌های شخصی،

ـ مجوزدهی انتقال بین‌المللی داده‌ها.

- توسعه استانداردها،

ـ کمک به توسعه استانداردهایی برای حمایت از داده،

ـ آگاه‌سازی سازمان‌ها درخصوص تغییرات به‌وجود آمده در قوانین حمایت از داده،

ـ ارائه پیشنهادها و دستورالعمل‌هایی برای تطبیق‌پذیری سازمان‌ها با قانون حمایت از داده،

ـ ارائه پیشنهادهایی برای پیاده‌سازی استانداردهای امنیتی حفاظت از داده مشخص شده در قانون حمایت از داده.

- وظایف مربوط به مسائل مخابراتی،

ـ حفاظت از حقوق شهروندان و تضمین حقوق کاربران اینترنتی در زمینه حریم خصوصی ارتباطاتی شامل جلوگیری از ارسال پیام‌های تبلیغاتی و هرزنامه‌ها[1] از طریق ایمیل یا سایر رسانه‌های الکترونیکی،

ـ ارسال هشدارهایی درخصوص وقوع رخنه‌های امنیتی در سامانه‌های خدمات‌دهندگان الکترونیکی که ممکن است بر داده‌های شخصی اثرگذار باشد،

- سایر وظایف،

ـ همکاری با سازمان‌های بین‌المللی و دولتی در اتحادیه اروپا در حوزه حریم خصوصی کاربران در فضای مجازی،

ـ عمل به‌عنوان نماینده اسپانیا در گردهمایی‌های بین‌المللی،

ـ کنترل بر اجرایی کردن قوانین حمایت از داده در اسپانیا،

ـ انتشار گزارش سالیانه در زمینه حمایت از حریم خصوصی کاربران در فضای مجازی در اسپانیا که توسط ریاست آژانس در محضر دادگاه عالی این کشور قرائت خواهد شد (سایت رسمی آژانس حفاظت از داده اسپانیا).[2]

در اسپانیا سازمان‌های دولتی و خصوصی ملزم شده‌اند پیش از اقدام به انجام پردازش داده‌های شخصی، روندی اداری را طی کنند که در طی این فرایند ابتدا باید به ثبت موارد زیر در «رجیستری

1. Spam
2. http://www. agpd. es

حفاظت از داده عمومی»[1] ـ که در سایت «آژانس حفاظت از داده» به‌صورت آنلاین نگهداری می‌شود ـ اقدام نمایند:

- اهداف فایل داده‌ای که سازمان قصد ایجاد آن را دارد،
- بخش‌های داده‌ای که در فایل داده قرار خواهد گرفت،
- هرگونه افشای داده‌های شخصی،
- سطوح امنیتی که برای حفاظت از داده‌های شخصی مورد نیاز است،
- هر نوع انتقال بین‌المللی داده‌های شخصی.

در هر زمانی که سازمان کنترل‌گر تغییری در موارد فوق ایجاد کند، باید بلافاصله به اصلاح اطلاعات ثبت شده در رجیستری حفاظت از داده عمومی اقدام کند. همچنین درصورتی‌که سازمان کنترل‌گر به حذف داده‌های شخصی اقدام کند، باید این موضوع را در رجیستری ثبت نماید (گویلین و سالا،[2] ۲۰۱۵).

۶. نروژ

«قانون حمایت از داده نروژ»[3] در ۱۴ آوریل سال ۲۰۰۰ به تصویب مجلس قانونگذاری این کشور رسید. این قانون مشتمل بر ۹ فصل و ۵۲ بخش است. مهمترین هدف این قانون «حفاظت از افراد حقیقی برای نقض حق حریم خصوصی آنها از طریق پردازش داده‌های شخصی آنان است» (قانون حمایت از داده نروژ،[4] ۲۰۰۰: ۱). در این قانون، کنترل‌گر هر فرد یا سازمان دولتی یا خصوصی است که تعیین‌کننده روش‌های مورد استفاده در پردازش داده‌های شخصی است. همچنین فرد یا سازمانی که توسط کنترل‌گر به‌عنوان پیمانکار برای پردازش داده‌های شخصی شهروندان انتخاب می‌شود، پردازشگر (پیمانکار) تعریف شده است. در قانون نروژ، داده‌های شخصی عبارت است از «هر نوع اطلاعات و ارزیابی‌هایی که ممکن است با یک فرد حقیقی ارتباط پیدا کند» (**همان**، بخش ۲، شماره ۱). با این تعریف وسیع هر نوع اطلاعاتی که به نحوی مشخص‌کننده هویت یک فرد حقیقی باشد، داده شخصی شناخته می‌شود. گردآوری، استفاده، نگهداری و ذخیره‌سازی و افشای داده‌های شخصی افراد در این قانون تحت پوشش قرار گرفته‌اند و برای آنها الزاماتی تعیین شده است (**همان**، بخش ۲، شماره ۲). برخی موارد دیگر که علاوه‌بر مصادیق پردازش داده‌های شخصی در قانون نروژ بحث شده‌اند عبارتند از:

- نظارت ویدئویی،
- انتقال داده‌های شخصی به کشورهای ثالث،

1. General Data Protection Registry
2. Guilayn and Sala
3. The Norwegian Data Protection Act
4. The Norwegian Data Protection Act

- کنترل داخلی،
- اصلاح داده‌های شخصی یا داده‌های شخصی ناقص،
- امنیت اطلاعات،
- الزاماتی در مورد شهروندان (همچون فراهم کردن دسترسی به داده‌های شخصی)،
- الزامات در مورد اطلاع‌رسانی و اخذ مجوزهای قانونی از بازرس داده،[1]
- حق کارکنان و مستخدمان برای دسترسی به ایمیل‌های شخص خود.

قانون حمایت از داده نروژ به کلیه کنترل‌گرهای داده‌ای که در نروژ مستقر شده‌اند و همچنین تمامی کنترل‌گرهایی که در کشورهای خارج از حوزه اتحادیه اروپا مستقر هستند، اما از تجهیزات سخت‌افزاری و سرورهای داخل نروژ استفاده می‌کنند قابل اعمال است. البته اگر کنترل‌گر از سرورها و تجهیزات سخت‌افزاری داخل نروژ تنها برای انتقال داده‌های شخصی استفاده کند، مشمول این قانون نمی‌شود. تمامی کنترل‌گرهای داده‌های شخصی ملزم شده‌اند در صورت تصمیم به پردازش هر نوع داده شخصی شهروندان، ابتدا مراتب را به نهادی به‌عنوان «بازرس داده» اطلاع دهند. اطلاع‌رسانی به بازرس داده باید حداقل تا ۳۰ روز قبل از شروع به پردازش داده‌های شخصی توسط کنترل‌گر به اطلاع بازرس داده برسد.

همچون اغلب کشورهای منتخب، هرگونه پردازش داده‌های شخصی حساس باید توسط نهاد ناظر بر حریم خصوصی (که در نروژ بازرس داده نام دارد) مجوزدهی شود. به‌عبارت دیگر، اگر در داده‌های شخصی، برخی از اقسام داده‌های شخصی حساس وجود داشته باشند، سازمان کنترل‌گر نیازمند اخذ مجوز خاص برای این مورد است. مواردی که سازمان کنترل‌گر باید پیش از اقدام به پردازش داده‌های شخصی به اطلاع بازرس داده برساند عبارتند از:

- نام و آدرس کنترل‌گر و نماینده قانونی او به همراه نام و آدرس پردازشگر (پیمانکار) (در صورت برون‌سپاری عملیات پردازش به یک پردازشگر (پیمانکار) خارجی)،
- زمان شروع عملیات پردازش داده‌های شخصی،
- مسئول مستقیم عملیات روزمره پردازش داده‌های شخصی در سازمان جهت نظارت بر انطباق عملیات پردازش کنترل‌گر با قانون حفاظت از داده،
- اهداف پردازش داده‌های شخصی،
- توصیفاتی درخصوص نوع داده‌های شخصی که باید پردازش شوند،
- مبانی قانونی گردآوری داده‌های شخصی،
- افراد (یا سازمان‌هایی) که داده‌های شخصی به آنها افشا خواهد شد، شامل کشورهای دریافت‌کننده داده،

1. Data Inspectorate

- اقدامات امنیتی تدارک دیده شده برای پردازش داده‌های شخصی،

همچنین مواردی که پادشاه نروژ تشخیص دهد نیز قابل افزوده شدن به موارد فوق است (**همان**، بخش ۳۲). البته در موارد زیر سازمان نیازمند اخذ مجوز نیست:

- پردازش داده‌های شخصی مربوط به مشتریان و کاربران یا تأمین‌کنندگان به‌عنوان بخشی از الزامات تعیین شده در قرارداد عقد شده با آنان،
- پردازش روتین داده‌های شخصی کارکنان برای مسائل پرسنلی و مدیریت نیروی انسانی،

مهمترین اصول حفاظت از داده در قانون نروژ عبارتند از:

- پردازش داده‌های شخصی باید با الزامات تعیین شده در قانون حمایت از داده تطابق داشته باشند؛
- استفاده از داده‌های شخصی باید با اهداف اولیه گردآوری آنها و سایر فعالیت‌های کنترل‌گر تطابق داشته باشد مگر آنکه رضایت شهروند قبلاً کسب شده باشد؛
- کنترل‌گر باید اطمینان حاصل کند که داده‌های شخصی با اهداف پردازش سازگار بوده و تا حد کفایت گردآوری شده باشند؛
- کنترل‌گر باید اطمینان یابد داده‌های شخصی دقیق و به‌روز بوده و برای مدتی بیش از مدت مورد نیاز برای اهداف اولیه نگهداری نشوند (**همان**، بخش ۱۱).

نهاد بازرس داده در نروژ حداقل ۴۰ عضو دارد که شامل حقوقدانان، متخصصان فناوری اطلاعات و دانشمندان علوم اجتماعی هستند. این نهاد زیر نظر قوه قضائیه و پادشاه نروژ فعالیت می‌کند. ریاست این نهاد را پادشاه نروژ تعیین می‌کند. برخی از مهمترین وظایف نهاد بازرس داده در نروژ به‌شرح زیر است:

- نگهداری و انتشار یک رکورد اطلاعاتی از تمامی پردازش‌های صورت گرفته توسط کنترل‌گرها به همراه اطلاعاتی همچون موارد زیر: نام کنترل‌گر و آدرس وی یا نماینده قانونی او، نام مسئول عملیات پردازش، اهداف پردازش داده‌های شخصی و...
- رسیدگی به فرآیند دریافت اطلاع‌رسانی از کنترل‌گرها،
- رسیدگی به فرآیند صدور مجوز پردازش داده‌های شخصی،
- اطمینان از جامعیت قوانین و مقررات موجود درخصوص پردازش داده‌های شخصی،
- اصلاح کمبودهای موجود در قوانین حمایت از داده‌های شخصی،
- به‌روزرسانی دانش نهاد با توسعه‌های بین‌المللی پردازش داده و شناسایی مشکلات مربوط به پردازش داده‌های شخصی،
- تشخیص ریسک‌های حفاظت از حریم خصوصی اطلاعات و توصیه پیشنهادهایی برای اجتناب از یا محدود کردن چنین ریسک‌هایی،

- ارائه توصیه و راهنمایی‌هایی درخصوص حفاظت از حریم خصوصی افراد و حفاظت از داده‌های شخصی آنان برای سازمان‌ها یا افرادی که قصد پردازش داده‌های شخصی افراد را دارند یا توسعه سامانه‌هایی برای چنین پردازش‌هایی،
- ارائه نظرات کارشناسی به کنترل‌گرهای داده شخصی در مورد مسائل مربوط به پردازش داده‌های شخصی با تقاضای این سازمان‌ها یا طبق تشخیص خود نهاد،
- تدوین و ارائه گزارش فعالیت‌های انجام شده به پادشاه نروژ،
- صدور احکامی برای جریمه سازمان‌های متخلف در مواردی همچون:

ـ سرپیچی از دستورات نهاد بازرسی داده یا عدم اطلاع‌رسانی در موارد پردازش داده،

ـ پردازش داده‌های شخصی که نیاز به دریافت مجوز داشته‌اند، بدون کسب مجوزهای لازم،

ـ نقض قانون حمایت از داده،

ـ پردازش داده‌های شخصی برخلاف الزامات تعیین شده در قانون حمایت از داده،

ـ سرپیچی از ارائه اطلاعات درخواستی نهاد بازرسی داده (**همان**، بخش‌های ۴۴-۴۲).

نهاد بازرسی داده همچنین موظف شده است تا در صورت صلاحدید از تجهیزات سخت‌افزاری و نرم‌افزاری پردازش داده‌های شخصی، مکان قرارگیری تجهیزات، تمهیدات امنیتی تدارک دیده شده برای حفاظت از امنیت داده‌های شخصی و سایر مسائل فنی بازرسی به‌عمل آورد (همان، بخش ۴۴). در نروژ «هیئت استیناف حریم خصوصی»[1] وظیفه دارد تا بر فعالیت‌های نهاد بازرس داده نظارت کند و در مسائلی که مورد اختلاف این نهاد با سایر سازمان‌ها، ازجمله کنترل‌گرهاست، داوری کند. این هیئت متشکل از هفت عضو است ک برای یک یا دو دوره چهارساله منصوب می‌شوند. رئیس و نایب رئیس این هیئت را پارلمان نروژ[2] تعیین می‌کند و سایر اعضا توسط پادشاه تعیین می‌شوند. مهمترین وظیفه این هیئت تجدیدنظر در احکام صادر شده یا تصمیمات اتخاذ شده توسط نهاد بازرسی داده است. این هیئت، همچون نهاد بازرس داده به‌صورت قانونی مجاز شده است تا به هر نوع اطلاعاتی که برای انجام وظایفشان ضروری است دست پیدا کنند و سازمان‌ها موظف شده‌اند تا با آنها همکاری کنند (**همان**، بخش ۴۴).

۷. سوئد

مهمترین قانون مصوب در کشور سوئد در زمینه حمایت از حریم خصوصی کاربران در فضای مجازی، قانون «حمایت از داده‌های شخصی»[3] است که در تاریخ ۲۴ اکتبر ۱۹۹۸ توسط مجلس قانونگذاری سوئد با هدف حمایت از حریم خصوصی کاربران در فضای مجازی و آزادی‌های اساسی آنان تصویب شد. این

1. The Privacy Appeals Board
2. The Storting
3. Personal Data Act or Personuppgiftslag (in Swedish)

قانون نسخه اصلاح شده قانون داده[1] مصوب سال ۱۹۷۳ است که در آن اصلاحات اساسی برای حفاظت هرچه بهتر داده‌های شخصی شهروندان توسط نهادهای دولتی و غیردولتی به‌وجود آمده است. آخرین نسخه اصلاح شده این قانون در اکتبر سال ۲۰۰۶ به‌وجود آمده و در دسترس عموم قرار گرفته است (قانون حمایت از داده سوئد،[2] ۲۰۰۶). این قانون به کنترل‌گرهای داده‌های شخصی که به‌تنهایی یا با کمک سایرین در مورد اهداف پردازش داده‌های شخصی تصمیم‌گیری می‌کنند قابل کاربرد است. در این قانون کنترل‌گر داده‌های شخصی عموماً یک سازمان دولتی یا خصوصی در نظر گرفته شده است که البته می‌تواند یک فرد حقیقی نیز باشد.

در قانون حمایت از داده سوئد، داده‌های شخصی به هر نوع اطلاعاتی اطلاق می‌شود که بتواند به‌صورت مستقیم یا غیرمستقیم (در ترکیب با سایر داده‌ها) به یک فرد حقیقی زنده قابل ارجاع باشد. به‌عنوان مثال در این قانون آدرس آی پی[3] اینترنتی به‌عنوان داده شخصی شناسایی شده است، زیرا می‌توان با ترکیب آدرس آی پی با فیش پرداخت خدمات‌دهنده اینترنتی[4] یک فرد حقیقی را شناسایی کرد. این قانون وابسته به فناوری خاصی نبوده و هر نوع پردازش داده‌های شخصی که تماماً یا بخشی از آن توسط هر نوع فناوری الکترونیکی انجام گرفته باشد یا حتی پردازش‌های انجام شده به‌صورت غیرخودکار را که در آن اطلاعات شخصی افراد به‌صورت طبقه‌بندی و منظم به شکل ساختارمندی نگهداری می‌شوند، نیز دربر می‌گیرد. هرچند داده‌های شخصی که فقط برای مصارف شخصی افراد حقیقی پردازش می‌شوند و جنبه‌ای کاملاً خصوصی دارند از شمول این قانون مستثنا شده‌اند. به‌عنوان مثال، برخی شهروندان ممکن است به تهیه فایلی شامل خاطرات روزانه الکترونیکی یا ثبت اطلاعات تماس و آدرس دوستان و خویشاوندان خود اقدام کنند (هاگر،[5] ۲۰۱۵).

در قانون حمایت از داده سوئد، داده‌های شخصی افراد تنها هنگامی قابل گردآوری است که از قبل اهدافی مشخص و مشروع برای آنها تعریف شده باشد. نکته مهم این است که در صورت نیاز سازمان گردآوری‌کننده به بازپردازش داده‌های شخصی، دیگر نمی‌تواند با استناد به اهداف اولیه اقدام به بازپردازش آنها کند، مگر اینکه در اهداف اولیه، این نوع بازپردازش پیش‌بینی شده باشد و به اطلاع شهروندان رسیده باشد یا زمینه‌های حقوقی خاصی به‌وجود آمده باشد. در قانون سوئد، سازمان‌های دولتی موظف شده‌اند اسناد دولتی را در دسترس عموم قرار دهند، مگر آنکه بنا به طبقه‌بندی محرمانه این اسناد قابل انتشار عمومی نباشند. همچنین کنترل‌گرهای داده‌های شخصی باید موارد زیر را به اطلاع شهروندان برسانند:

1. The Data Act
2. Swedish Personal Data Act
3. IP Address
4. Internet Service Provider
5. Häger

- نام، آدرس، شماره تلفن، آدرس ایمیل و شماره ثبت شرکت (در صورت خصوصی بودن) کنترل‌گر،
- اطلاعاتی در مورد اهداف پردازش داده‌های شخصی،
- هر نوع اطلاعات ضروری که شهروندان را به برخورداری از حقوق خود در زمینه حریم خصوصی خود قادر می‌کند (**همان**).

همچنین کنترل‌گرها موظفند تا در صورت افشای داده‌های شخصی شهروندان، اطلاعاتی را در مورد دریافت‌کنندگان داده‌های شخصی آنان به اطلاع آنها برسانند؛ علاوه‌بر این، شهروندان باید بتوانند از کنترل‌گر هر نوع اطلاعاتی که در مورد عملیات پردازش آن است را دریافت کنند و در صورت نیاز بتوانند درخواست اصلاح داده‌های شخصی خود را به کنترل‌گر داده‌های شخصی بدهند. در صورت درخواست اصلاح، کنترل‌گر نیز موظف به اصلاح داده‌های شخصی مطابق خواسته شهروند یا شهروند است

در سوئد، «انجمن بازرسی داده»[1] وظیفه نظارت بر نحوه اجرای قانون حمایت از داده را دارد که نهادی دولتی بوده و تحت حمایت وزارت دادگستری سوئد فعالیت می‌کند. این انجمن بر فعالیت تمامی سازمان‌های دولتی و خصوصی در زمینه پردازش داده‌های شخصی شهروندان نظارت می‌کند. مهمترین مأموریت این انجمن طبق آنچه در وب‌سایتش مطرح شده است، «حفاظت از حریم خصوصی شهروندان در جامعه اطلاعاتی» است.[2] این انجمن دارای متخصصان امنیت فناوری اطلاعات و مشاوران حقوقی خاص خود است. مهمترین وظایف انجمن بازرسی داده سوئد به‌شرح زیر است:

- نظارت بر فعالیت سازمان‌های خصوصی و دولتی در زمینه پردازش داده‌های شخصی شهروندان و اطمینان از قانونی بودن این نوع فعالیت‌ها در جهت حفاظت از حریم خصوصی شهروندان،
- اعمال جریمه برای کنترل‌گرهای داده‌های شخصی که از دادن اطلاعات در مورد فعالیت‌های پردازش داده‌های شخصی شهروندان در سازمان خود امتناع ورزند و دستور به توقف عملیات پردازش آنان،
- دستور به اصلاح عملیات پردازش کنترل‌گرهای داده‌های شخصی درصورتی‌که عملیات آنان غیرقانونی اما قابل اصلاح باشد،
- دستور به توقف عملیات پردازش داده‌های شخصی در صورت پی بردن به غیرقانونی بودن آنها و عدم قابلیت اصلاح آنها،
- حکم به حذف داده‌های شخصی که از نظر انجمن به‌صورت غیرقانونی گردآوری شده باشند،
- همکاری با دادگاه‌های ویژه در جهت صدور احکام مرتبط با حریم خصوصی شهروندان (قانون حمایت از داده سوئد، ۲۰۰۶: ۲۷).

در سوئد، هر سازمان دولتی یا خصوصی که قصد گردآوری داده‌های شخصی را داشته باشد باید پیش از اقدام به عملیات، فرم اطلاع‌رسانی مکتوبی را به انجمن بازرسی داده تحویل دهد. با وجود این،

1. Data Inspection Board or Datainspektionen(in Swedish)
2. http://www. datainspektionen. se/in-english/

اگر قبلاً سازمان کنترل‌کننده یک «مأمور حفاظت از داده»[1] را منصوب کرده باشد و این موضوع را به اطلاع انجمن رسانده باشد، الزامی ندارد. همچنین هر نوع تغییر در نصب یا عزل مأمور حفاظت از داده باید به اطلاع انجمن حفاظت از داده برسد. وظیفه مأمور حفاظت از داده در سوئد این است که از قانونی بودن فعالیت‌های مرتبط با پردازش داده توسط کنترل‌گر داده‌های شخصی اطمینان حاصل کند. برخی دیگر از وظایف مأمور حفاظت از داده به‌شرح زیر هستند:

- شناسایی هر نوع کاستی در مورد حفاظت از داده‌های شخصی شهروندان در سازمان کنترل‌گر،
- ثبت و نگهداری یک فایل رجیستری از تمامی عملیات پردازش داده‌های شخصی انجام شده توسط کنترل‌گر داده‌های شخصی،
- اطلاع‌رسانی به انجمن بازرسی داده در موارد لازم (هاگر، ۲۰۱۵).

۸. آلمان

قانون حمایت از داده دولتی آلمان[2] توسط پارلمان آلمان[3] در ۲۷ اُم ژانویه سال ۱۹۷۷ به تصویب رسید و در اول ژانویه سال ۱۹۷۸ اجرایی شد. این قانون با اختصار BDSG[4] شناخته می‌شود. سال‌ها بعد قانون حمایت از داده در آلمان به این دلیل که تمامی جنبه‌های حریم خصوصی کاربران در فضای مجازی را دربرنمی‌گرفت، مورد اصلاح قرار گرفت. مهمترین مشکل قانون اولیه این بود که پردازش داده را تنها شامل استفاده از داده در نظر گرفته بود و هیچ قانونی برای گردآوری داده‌های شخصی در آن وجود نداشت. همچنین اصل مشخص بودن هدف نیز در این قانون مشخص نشده بود. قانون حمایت از داده‌های شخصی آلمان در سال ۱۹۹۱ مورد بازبینی قرار گرفت و در ۱۴ ژوئن سال ۲۰۰۰ توسط دولت اجرایی شد (فیشر ـ هانبر،[5] ۲۰۰۱: ۱۴). مهمترین اصلاحات صورت گرفته در قانون حمایت از داده آلمان به‌شرح زیر است:

- برخی قوانین جدید برای پردازش داده‌های شخصی در بخش خصوصی،
- برخی قوانین جدید برای پردازش داده‌های شخصی حساس،
- برخی قوانین جدید برای محدودیت انتقال داده‌های شخصی به کشورهای ثالث که خارج از حوزه اتحادیه اروپا هستند در صورت سؤال‌برانگیز بودن سطوح حمایت از داده در آنها،
- برخی قوانین جدید برای الزام سازمان‌های دولتی به انتصاب مأمور حفاظت از داده جهت رصد نحوه تبعیت از قانون حمایت از داده در آن سازمان‌ها،

1. Data Protection Officer
2. The German Federal Data Protection Act (Bundesdatenschutzgesetz)
3. Bundestag
4. Bundesdatenschutzgesetz
5. Fischer-Hübner

- برخی قوانین جدید برای بررسی ریسک‌های مربوط به پردازش داده‌های شخصی،
- برخی قوانین جدید برای نحوه پردازش تمام‌خودکار داده‌های شخصی و اجازه به شهروندان برای درخواست پردازش دستی داده‌های شخصی خود،
- افزایش حقوق شهروند (مثل حق اعتراض، حق آگاهی از پردازش داده‌های شخصی در دستگاه‌های دولتی و...)،
- اعطای حقوق بشری به سازمان‌های ناظر بر حسن اجرای قوانین حمایت از داده (کمیسیونرها)،
- بازبینی پیوست‌ها (پیوست‌ها مربوط به تدابیر فنی و سازمانی حمایت از داده هستند) (فیشر ـ هانبر، ۲۰۰۱: ۱۶).

براساس بخش ۱ این قانون، هدف این قانون «حفاظت از افراد در برابر نقض حقوق شخصی آنها از طریق مدیریت داده‌های شخصی آنها می‌باشد». این قانون به تمامی سازمان‌های دولتی و همچنین سازمان‌های خصوصی و تجاری کاربرد پیدا می‌کند. تمامی سازمان‌های دولتی آلمان به تبعیت از مفاد این قانون و پیروی از الزامات تعیین شده در آن ملزم هستند. قانون حمایت از داده آلمان پنج بخش و چند پیوست دارد. در بخش اول قانون مذکور، الزاماتی برای پردازش داده‌های شخصی افراد توسط نهادهای دولتی و خصوصی در نظر گرفته شده است. این قوانین شامل نحوه گردآوری، نگهداری و ذخیره، استفاده و افشای داده‌های شخصی هستند که در زیربخش ۴ در بخش اول این قانون مطرح شده‌اند. همچنین حقوق سوژه[1] در زیربخش ۶، نحوه جبران ضررهای وارد به شهروند در زیربخش‌های ۷ و ۸ و نیز تمهیدات فنی و سازمانی لازم جهت حفاظت از داده‌های شخصی در زیربخش ۹ و پیوست ۱ این قانون مطرح شده‌اند. در بخش دوم این قانون مبانی خاص حقوقی پردازش داده‌های شخصی توسط هریک از نهادهای خصوصی و دولتی به‌صورت جداگانه مطرح شده است که در این بخش استثناها هریک از بخش‌ها مطرح شده است. باید توجه داشت که برخی از قوانین مطرح شده در این دو بخش باهم تفاوت دارند؛ مواردی همچون نحوه پردازش، حقوق شهروند و نحوه نظارت بر قانون حمایت از داده. در بخش سوم این قانون، الزاماتی برای پردازش داده‌های شخصی با اهداف تجاری و بازاریابی به‌عنوان مثال توسط نهادهای تحقیقات بازاریابی مطرح شده است. در بخش چهارم این قانون نیز نحوه پردازش داده‌های شخصی توسط بخش‌های خاصی همچون رسانه‌ها و سازمان‌های تحقیقاتی مطرح شده است. بخش پنجم این قانون به حمایت‌های کیفری از حریم خصوصی کاربران در فضای مجازی پرداخته است و نحوه مجازات مجرمان در محاکم و دادگاه‌های آلمان را مشخص کرده است. در این بخش برای ارتکاب جرم در رابطه با نقض حریم خصوصی کاربران در فضای مجازی، به فراخور میزان خسارات وارده به شهروندان جزای نقدی و حبس پیش‌بینی شده است (قانون حمایت از داده فدرال آلمان، ۲۰۱۴، بخش ۲).

1. Subject

در قانون حمایت از داده آلمان، گردآوری داده‌های شخصی توسط سازمان‌های دولتی تنها هنگامی مجاز است که شهروند از هدف گردآوری آن آگاه باشد. همچنین گردآوری داده‌های شخصی باید با اهداف سازمان گردآوری‌کننده سنخیت داشته باشد. در این قانون همچنین استفاده و نگهداری داده‌های شخصی زمانی مجاز شمرده می‌شود که گردآوری آنها توسط سازمان کنترل‌کننده (متولی داده‌های شخصی) به‌صورت قانونی انجام گرفته باشد؛ بنابراین هرگونه استفاده یا نگهداری داده‌های شخصی هنگامی‌که بدون آگاهی شهروند صورت گرفته باشد یا اهداف گردآوری به اطلاع شهروند نرسیده باشد غیرمجاز تلقی می‌شود. در قانون حمایت از داده آلمان، افشا با عنوان «انتقال داده‌های شخصی»[1] شناخته می‌شود؛ در این قانون افشای داده‌های شخصی زمانی مجاز است که این افشا ضروری بوده و سازمان دریافت‌کننده داده‌های شخصی تنها برای اهداف از پیش تعیین شده از آنها استفاده کند.

در قانون حمایت از داده آلمان سازمانی به نام «کمیسیونر حمایت از داده دولتی»[2] وظیفه نظارت بر حسن اجرای قانون حمایت از داده توسط سازمان‌های دولتی را برعهده دارد که وظایف آن در زیربخش‌های ۲۲ تا ۲۶ مطرح شده است. با توجه به اینکه بخش‌های فدرال در آلمان به تبعیت از قانون حمایت از داده ملزم هستند، برای نظارت بر حسن اجرای این قانون در بخش‌های فدرال دولتی، سازمان‌های مجزایی به نام «کمیسیونرهای حمایت از داده»[3] در نواحی فدرال مختلف حضور داشته و تحت نظر کمیسیونر حمایت از داده مرکزی بر نحوه اجرای قانون حمایت از داده نظارت می‌کنند. برای نظارت بر بخش خصوصی، در هریک از ایالت‌های فدرال بخشی به نام «مرجع نظارتی»[4] شکل گرفته است که بر تبعیت سازمان‌های بخش خصوصی از قوانین حمایت از داده نظارت می‌کند. علاوه‌بر این، سازمان‌های بخش خصوصی و دولتی به تعیین چند کارمند تمام‌وقت به‌عنوان «مأمور حفاظت از داده[5]» ملزم هستند که وظیفه دارند نحوه تبعیت سازمان خود از قوانین حمایت از داده را رصد کنند (قانون حمایت از داده فدرال آلمان، ۲۰۱۴، بندهای «۲۶-۲۲»).

۹. ایرلند

«قانون حمایت از داده ایرلند»[6] که در سال ۱۹۸۸ برای اولین بار مصوب شد و در سال ۲۰۰۳ نسخه اصلاح شده و نهایی آن در اختیار سازمان‌های دولتی و خصوصی و شهروندان قرار گرفت، به‌عنوان «قانونی برای حمایت از حریم خصوصی الکترونیکی افراد» توسط مجلس قانونگذاری ایرلند مورد تصویب قرار گرفته است. این قانون به تمامی افراد و سازمان‌هایی که در ایرلند اقدام به گردآوری، نگهداری یا پردازش

1. Communication of Personal Data
2. The Federal Data Protection Commissioner or Bundesbeauftragter für den Datenschutz (in German)
3. Data Protection Commissioners or Landesdatanschutzbeauftragte (in German)
4. Supervisory Authority
5. Data Protection Officer or Betrieblicher Datenschutzbeauftragter (in German)
6. Ireland Data Protection Act (DPA)

داده‌های افراد زنده بر روی هر نوع سیستم رایانه‌ای یا سیستم فایلینگ ساختاریافته مشغولند، کاربرد پیدا می‌کند. در این قانون میان پردازشگر (پیمانکار) داده‌های شخصی و کنترل‌گر داده‌های شخصی تمایز ایجاد شده است. کنترل‌گر داده‌های شخصی در این قانون هر فرد یا سازمانی است که به‌تنهایی یا با کمک سایرین به کنترل محتوا و استفاده از داده‌های شخصی اقدام می‌کند. در مقابل پردازشگر (پیمانکار) داده‌های شخصی عبارت است از هر فرد یا سازمانی که به‌جای کنترل‌گر اقدام به پردازش داده‌های شخصی می‌کند. البته منظور برون‌سپاری عملیات پردازش توسط کنترل‌گر است و در این قانون کارمندان کنترل‌گر که بنا به وظایف شغلی خود اقدام به پردازش داده‌های شخصی می‌کنند، پردازشگر (پیمانکار) شناخته نمی‌شوند (کوکس و همکاران،[1] ۲۰۱۵).

در قانون ایرلند، سوژه به‌عنوان هر شخص حقیقی که داده‌های شخصی به وی ارتباط پیدا می‌کند معرفی شده است. همچنین، داده‌ها عبارتند از هر دو نوع داده‌های دستی و خودکار. داده‌های دستی،[2] عبارتند از اطلاعاتی که یکی از دو شرط زیر را داشته باشند:

- به‌عنوان بخشی از سیستم فایلینگ نگهداری شده باشند،
- با این قصد نگهداری می‌شوند که بعداً به‌عنوان بخشی از یک سیستم فایلینگ مرتبط درآیند.

همچنین، داده‌های خودکار[3] اطلاعاتی هستند که دارای یکی از شرایط زیر باشند:

- توسط ابزارهای خودکار عملیاتی در پاسخ به دستورالعمل‌های داده شده برای اهداف مشخص پردازش شده باشند؛
- با هدف پردازش از طریق ابزارهای خودکار عملیاتی، در آینده نگهداری شده باشند.

در قانون ایرلند، کنترل‌گرهایی که حائز شرایط زیر باشند مشمول قانون حمایت از داده ایرلند می‌شوند:

- سازمان کنترل‌گر داده‌های شخصی در ایرلند مستقر شده باشد؛
- افرادی که خود اقدام به پردازش داده‌های شخصی می‌کنند ساکن ایرلند باشند؛
- سازمان کنترل‌گر داده‌های شخصی مشمول سایر قوانین ایرلند شود؛
- سازمان کنترل‌گر داده‌های شخصی با همکاری سایر سازمان‌های مشمول قوانین ایرلند اقدام به پردازش داده‌های شخصی نماید؛
- افراد حقوقی که یک دفتر، شعبه یا نهاد در ایرلند را به‌صورت خصوصی اداره می‌کنند، به صورتی که پردازش داده‌های شخصی برایشان به‌صورت یک فعالیت یا فعالیت‌های منظمی باشد که به پردازش داده ارتباط پیدا می‌کند.

1. Cox et al.
2. Manual
3. Automated

قانون فوق برای برخی موارد که در ادامه شرح آنها آمده است، کاربرد پیدا نمی‌کند:

- داده‌ای که برای مقاصد امنیت ملی ایرلند نگهداری یا طبقه‌بندی شده باشد؛
- داده‌ای که شامل اطلاعاتی است که فرد نگهدارنده داده‌ها توسط قانون ملزم به عمومی‌سازی آنها شده باشد؛
- داده‌ای که برای مقاصد شخصی، خانوادگی یا خصوصی نگهداری شده باشد (کوکس و همکاران، ۲۰۱۵).

مهمترین اصول حفاظت از داده در قانون حفاظت از داده ایرلند به‌شرح زیر است:

- کسب و پردازش داده‌های شخصی به‌صورت منصفانه صورت گیرد؛
- نگهداری داده‌های شخصی تنها برای یک یا چند هدف مشخص و قانونی باشد؛
- پردازش داده‌های شخصی با اهداف اولیه تعیین شده توسط کنترل‌گر سازگاری داشته باشد؛
- داده‌های شخصی به‌صورت امن و ایمن نگهداری شوند؛
- داده‌های شخصی به‌صورت دقیق و به‌روز نگهداری شوند؛
- اطمینان از اینکه داده‌های شخصی (برای اهداف اولیه) کفایت داشته باشند و با آن تناسب داشته باشند؛
- نگهداری داده‌های شخصی بیش از زمان ضروری برای اهداف مشخص صورت نگیرد؛
- یک کپی از داده‌های شخصی هر فرد، در صورت تقاضای آن فرد در اختیارش قرار گیرد.
- اطمینان از وجود تمهیدات امنیتی کافی توسط کنترل‌گر به‌منظور:

ـ پیشگیری از دسترسی غیرمجاز به داده‌های شخصی، تغییر غیرمجاز آنها، افشا یا نابودی غیرمجاز داده‌های شخصی (خصوصاً زمانی که پردازش، انتقال داده‌های شخصی از طریق شبکه را دربر می‌گیرد)،

ـ اطمینان از حفاظت از داده‌ها در برابر تمامی اشکال غیرقانونی پردازش (همان).

در ایرلند «کمیسیونر حفاظت از داده»[1] مسئولیت حفاظت از حقوق حریم خصوصی شهروندان را برعهده دارد. این نهاد که در سال ۱۹۸۸ تأسیس شد زیر نظر دولت بوده، اما در انجام وظایفش دارای استقلال کامل می‌باشد و می‌تواند سازمان‌های دولتی و خصوصی را برای امهال درخصوص حفاظت از حریم خصوصی کاربران در فضای مجازی با جریمه‌هایی مجازات کند.[2] انتخاب اعضای کمیسیونر حفاظت از داده با پیشنهاد افرادی توسط نخست‌وزیر ایرلند و با موافقت وزیر مالی[3] تعیین می‌شود. این افراد همگی باید از کارکنان بخش عمومی باشند. نخست‌وزیر ایرلند می‌تواند برخی از اختیارات خود را به کمیسیونر تفویض کند تا این کمیسونر بتواند به انجام وظایفش بپردازد. مهمترین وظیفه‌های کمیسیونر حفاظت از داده ایرلند به‌شرح زیر هستند:

1. Data Protection Commissioner
2. https://www. dataprotection. ie/docs/About-the-office-of-the-DPC/b/1032. htm
3. Minister of Finance

- نظارت بر قانونی بودن عملیات پردازش داده‌های شخصی توسط کنترل‌گرها و انطباق آن با قانون حمایت از داده،
- انجام هرگونه وظیفه‌ای در ارتباط با حفاظت از داده‌های شخصی که توسط دولت ایرلند برای انطباق با قوانین بین‌المللی تعیین می‌شود،
- انجام تحقیقات پیرامون نقض قانون حفاظت از داده و نقض حقوق حریم خصوصی یک شهروند در صورت ارسال شکایت توسط شهروند و رسیدگی به شکایات شهروندان،
- مسدودسازی، اصلاح یا حذف و نابودسازی هر نوع داده شخصی در اختیار کنترل‌گرها در صورت صلاحدید،
- پاسخگویی به سؤالات و مشکلات کنترل‌گرهای داده و دادن نظرات کارشناسی در مورد مسائل مرتبط با حفاظت از داده،
- حل‌وفصل مسائل مربوط به حفاظت از داده میان کنترل‌گر و شهروند،
- اعمال جریمه برای کنترل‌گرهایی که به هر نحو نتوانند با قانون حمایت از داده انطباق پیدا کنند (طبق نظر این نهاد مجرم شناخته شوند (قانون حمایت از داده ایرلند، ۲۰۰۳: بخش‌های ۱۰-۹).

۱۰. ایتالیا

قانون حفاظت از حریم خصوصی کاربران در فضای مجازی در ایتالیا با عنوان «کد حفاظت از داده‌های شخصی»[1] شناخته می‌شود که به اختصار به «کد»[2] نیز شهرت دارد. در این قانون برای حفاظت از حریم خصوصی کاربران در فضای مجازی توسط پردازشگر (پیمانکار)ها و کنترل‌گرهای داده‌های شخصی در بخش‌های دولتی و غیردولتی الزاماتی مطرح شده است. در قانون ایتالیا میان کنترل‌گرهای داده‌های شخصی و پردازشگر (پیمانکار)های داده‌های شخصی تمایز ایجاد شده است. کنترل‌گرهای داده‌های شخصی دارای استقلال کامل برای تعیین اهداف و مکانیسم‌های عملیات پردازش داده و سایر مسائل امنیتی مرتبط هستند. در مقابل، پردازشگر (پیمانکار)های داده‌های شخصی توسط کنترل‌گرهایی انتخاب می‌شوند و به‌جای آنها به انجام عملیات پردازش داده‌های شخصی می‌پردازند (پانتا و دی ـ اوتاویو،[3] ۲۰۱۵).

در قانون ایتالیا داده‌های شخصی، هر نوع اطلاعاتی که به یک شخص حقیقی شناخته شده یا قابل شناسایی تعریف شده است. شناسایی فرد می‌تواند هم به‌صورت مستقیم (مثلاً از طریق کد ملی) و هم به‌صورت غیرمستقیم (اشاره به سایر اطلاعات مربوط به وی همچون آدرس آی پی)[4] انجام گیرد. اما

1. Personal Data Protection Code
2. Code
3. Panetta & D'Ottavio
4. IP Address

درصورتی‌که داده‌های شخصی مربوط به شهروند به طریقی غیرقابل شناسایی شوند (به‌اصطلاح Anonymize)، به‌طوری‌که نتوان داده‌ها را به‌هیچ‌عنوان به یک شخص نسبت داد، آنگاه از دامنه شمول قانون کد حفاظت از داده ایتالیا خارج می‌شوند. در قانون ایتالیا تمامی داده‌های شخصی افراد، حتی اگر در خارج از کشور نگهداری شوند، درصورتی‌که پردازش آنها در خاک ایتالیا انجام شده باشد یا سازمان متولی امور پردازش مشمول سایر قوانین ایتالیا گردد، تحت حمایت این قانون قرار می‌گیرند. همچنین درصورتی‌که نهادی که در خارج از کشور ایتالیا مشغول پردازش داده‌های شخصی افراد باشد اما از تجهیزات و ابزارهای پردازش داخل کشور ایتالیا بهره برده باشد نیز مشمول این قانون خواهد بود. در این صورت، کنترل‌گر داده‌های شخصی خارجی باید یک نماینده را در خاک ایتالیا منصوب و معرفی کند که الزامات تعیین شده در این قانون را اجرا کند.

قانون ایتالیا تمامی بخش‌های دولتی و غیردولتی را تحت پوشش خود قرار می‌دهد و یک قانون جامع برای حفاظت از داده‌های شخصی شهروندان ایتالیایی محسوب می‌شود. مهمترین اصول حفاظت از داده در این قانون به‌شرح زیر است:

- پردازش داده‌های شخصی شهروندان، به‌خصوص در مسائل محرمانه، هویت فردی و حقوق دسترسی به داده‌های شخصی، باید با توجه به حقوق سوژه، آزادی‌های اساسی و کرامت انسانی وی، صورت گیرد.
- سامانه‌ها و نرم‌افزارهای اطلاعاتی باید به طریقی پیکربندی شوند که حداقل استفاده از داده‌های شخصی را داشته باشند. این امر باید به‌گونه‌ای صورت پذیرد که پردازش داده‌های شخصی توسط این سامانه‌ها را هنگامی‌که پردازش به‌صورت ناشناخته (گمنام)[1] ممکن باشد، ممانعت به‌عمل آورد یا تمهیدات مناسبی را برای امکانپذیر شدن شناسایی هویت شهروندان تنها در مواقع لزوم فراهم آورد.
- پردازش داده‌های شخصی باید:

ـ قانونی و منصفانه صورت گیرد؛

ـ برای اهداف مشروع و مشخصی گردآوری و نگهداری شوند و استفاده از آنها نیز با اهداف اولیه گردآوری آنها ناسازگار نباشد؛

ـ داده‌های شخصی باید دقیق بوده و در مواقع لزوم به‌روزرسانی شوند؛

ـ داده‌های شخصی باید مربوط، کامل و در حد کفایت برای اهداف اولیه گردآوری یا پردازش‌های بعدی باشند؛

ـ داده‌های شخصی باید به طریقی نگهداری شوند که اجازه شناسایی هویت شهروندان را برای مدت‌زمانی بیش از زمان مورد نیاز برای اهداف اولیه گردآوری فراهم نیاورد؛

1. Anonymous

ـ زمانی آغاز شود که به شهروند در مورد پردازش داده‌های شخصی اطلاع داده شده باشد؛

ـ زمانی آغاز گردد که شهروند رضایت خود را در این خصوص اعلام کرده باشد (پانتا و دی ـ اوتاویو، ۲۰۱۵).

در قانون ایتالیا برای اینکه پردازش داده‌های شخصی مشروع باید، کنترل‌گر داده‌های شخصی نیاز دارد تا رضایت شهروندان را برای پردازش داده‌های شخصی آنان جلب کند. رضایت شهروندان باید دارای برخی شرایط باشد تا بتوان آن را یک رضایت آشکار[1] تلقی کرد. این شرایط عبارتند از:

- رضایت شهروند باید آزادانه و برای عملیات پردازش به‌وضوح مشخص ابراز شده باشد؛
- اخذ رضایت می‌تواند به‌صورت کتبی (برای پردازش داده‌های حساس) و آنلاین (برای پردازش داده‌های شخص عام) صورت گیرد. برای افرادی که دارای صغر سنی هستند یا به‌دلایلی نمی‌توانند رضایت خود را اعلام کنند، اخذ رضایت از اولیا یا نماینده قانونی آنها الزامی است؛
- برای جلب رضایت شهروند باید به وی اطلاعات مناسبی درخصوص عملیات پردازش داده‌های شخصی مربوط به وی اعلام شده باشد (**همان**).

۱۱. بلژیک

قانون حفظ حریم خصوصی کاربران در فضای مجازی در بلژیک، که با عنوان «قانون حفاظت از داده[2](DPL)» در ۸ دسامبر ۱۹۹۲ به‌منظور حفاظت از حریم خصوصی شهروندان بلژیکی در برابر پردازش داده‌های شخصی‌شان به تصویب رسید. نسخه اصلاح شده و نهایی این قانون در ۱ سپتامبر سال ۲۰۰۱ اجرایی شد. همچون سایر کشورهای منتخب، در بلژیک نیز رویکرد قانونگذاری یکپارچه برای حفظ حریم خصوصی کاربران در فضای مجازی در پیش گرفته شده است و در بلژیک قانون بخشی برای حفظ حریم خصوصی کاربران در فضای مجازی وجود ندارد (دی‌هالست،[3] ۲۰۱۶). قانون حفاظت از داده (DPL) در بلژیک به‌تمامی کنترل‌گرها ـ که هر شخص حقیقی، حقوقی، نهاد یا هر سازمان دولتی، که به‌تنهایی یا به همراه سایر نهادها اقدام به تعیین اهداف یا روش‌های پردازش داده‌های شخصی می‌کنند- کاربرد پیدا می‌کند (قانون حمایت از داده بلژیک، بند «۱-۴»). در قانون بلژیک داده‌های شخصی به هر نوع اطلاعاتی که به یک فرد شناخته شده یا قابل شناسایی حقیقی ارتباط پیدا می‌کند، اطلاق می‌شود. قابلیت شناسایی در این قانون به معنای قابلیت شناخته شدن به‌صورت مستقیم یا غیرمستقیم، از طریق یک کد شناسایی یا یک یا چند عامل خاص مرتبط با وضعیت فیزیکی، روان‌شناختی، روحی، اقتصادی، فرهنگی یا اجتماعی تعبیر شده است (همان، بند «۱-۱»). در این قانون شهروندی که داده‌های شخصی

1. Express Consent
2. Data Protection Law
3. D'hulst

به وی ارتباط پیدا می‌کند، «سوژه» (یا سوژه اطلاعاتی)[1] نامیده می‌شود. در قانون بلژیک، حوزه قانون به موارد زیر محدود شده است:

- کنترل‌گرها یا پردازشگرهایی که دارای مستقلات یا تجهیزات دائمی درون خاک بلژیک هستند؛
- کنترل‌گرها یا پردازشگرهایی که عملیات پردازش را در جایی که قانون بلژیک قابل اعمال است به انجام می‌رسانند؛
- کنترل‌گرها یا پردازشگرهایی که فاقد مستقلات یا تجهیزات پردازش درون حوزه اتحادیه اروپا هستند، اما عملیات پردازش را تجهیزات مستقر در خاک بلژیک انجام می‌دهند (همان، بند ۳).

در بلژیک نهادی با عنوان «کمیسیون حریم خصوصی»[2] وظیفه نظارت بر حسن اجرای قوانین حفاظت از حریم خصوصی کاربران را در فضای مجازی دارد. این کمیسیون می‌تواند جهت انجام وظایف نظارت و بازرسی خود، سازمان‌های دولتی بلژیک را به تکمیل فرم مربوط به اطلاع‌رسانی عملیات پردازش ملزم کند. این فرم می‌تواند به‌صورت آنلاین در وب‌سایت این نهاد[3] یا ارسال فایل به‌صورت پستی به آدرس آن، توسط کنترل‌گرها ارسال شود. در فرم اطلاع‌رسانی عملیات پردازش موارد زیر باید لحاظ شود:

- نام و آدرس دفتر کنترل‌گر داده‌های شخصی شهروندان،
- اهداف پردازش خودکار،
- اقلام اطلاعاتی مورد پردازش،
- اقلام اطلاعاتی که به دریافت‌کنندگان داده‌های شخصی افشا خواهد شد،
- روش‌های اطلاع‌رسانی به شهروندان در مورد حقوق آنها توسط کنترل‌گر،
- دوره‌های حفظ داده‌های شخصی،
- اطلاعاتی در مورد داده‌های شخصی حساس،
- توصیف عمومی تمهیدات امنیتی اندیشیده شده،
- بخش‌هایی از اطلاعات شخصی شهروندان که به سایر کشورها افشا خواهد شد،
- درصورتی‌که داده‌های شخصی به کشورهای فاقد سطوح امنیتی کافی ارسال می‌شود، مبنای قانونی این نوع افشا باید ذکر شود.

همچنین اطلاعات زیر می‌تواند توسط نهاد دیده‌بان حریم خصوصی (کمیسیون حریم خصوصی) از سازمان‌های دولتی درخواست شود:

- اطلاعاتی در مورد منبع داده‌های شخصی،
- فناوری پردازش خودکار داده‌های شخصی،

1. Data Subject
2. Privacy Commission
3. www.privacycommission.be

- تمهیدات امنیتی ـ کاربردی،
- سایر اطلاعات اضافی در مورد تمهیدات امنیتی و حفاظتی به‌منظور انتقال بین‌المللی داده‌های شخصی (**همان**، بند «۱۷»).

مهمترین اصول حفظ حریم خصوصی کاربران در فضای مجازی در قانون بلژیک به‌شرح زیر است:

- کنترل‌گر داده‌های شخصی باید داده‌های شخصی شهروندان را تنها با رضایت آنها پردازش کند یا در مواردی که قانون اجازه این کار را می‌دهد، بدون رضایت مجاز به پردازش آنهاست؛
- پردازش داده‌های شخصی باید مشروع بوده و با اصول کیفیت داده تطابق داشته باشد؛
- کنترل‌گرها باید اطلاعات کافی را در مورد مواردی که شهروند باید از آنها آگاهی داشته باشد، همچون حق دسترسی، اعتراض، اصلاح، مسدودسازی یا حذف داده‌های شخصی مربوط به وی به شهروند بدهد؛
- کنترل‌گرهای داده‌های شخصی باید تمهیدات فنی سازمانی مناسب را برای حفاظت از داده‌های شخصی در برابر رخدادهای زیر تدارک ببینند:
  - تخریب تصادفی یا غیرقانونی داده‌های شخصی،
  - تغییر یا دستیابی غیرمجاز به داده‌های شخصی،
  - سایر اشکال پردازش غیرقانونی داده‌های شخصی.
- درصورتی‌که کنترل‌گر اقدام به برون‌سپاری عملیات پردازش می‌کند، باید پردازشگر (پیمانکار) داده اصلح را انتخاب کند (همان، بند «۱۶»).

جمع‌بندی

با توجه به ضعف مبانی نظری مورد توافق در عرصه قانونگذاری حفاظت از داده‌های کاربران به‌نظر می‌رسد مطالعات کشورهای منتخب به‌ویژه کشورهای پیشرو در این عرصه یکی از منابع اصلی قانونگذاری ملی است. براساس آمار ارائه شده توسط نهاد دی.ال.ای[1] از ۱۹۶ کشور جهان، تنها ۱۱ کشور در وضعیت خیلی خوب قرار دارند: کره جنوبی، کانادا، انگلستان، آلمان، فرانسه، ایتالیا، اسپانیا، بلژیک، سوئد، نروژ، ایرلند. بر این اساس، در این تحقیق این ۱۱ کشور به‌عنوان کشورهای منتخب و پیشرو در حوزه صیانت از حریم خصوصی کاربران در فضای مجازی انتخاب شدند با مروری بر مطالعات و جمع‌بندی آنها درمی‌یابیم که در این کشورها در هفت حوزه برای حفاظت از داده‌های کاربران تلاش کرده‌اند که عبارتند از: ۱. الزامات گردآوری داده‌های شخصی کاربران در فضای مجازی، ۲. الزامات استفاده از داده‌های شخصی کاربران در فضای مجازی، ۳. الزامات نگهداری داده‌های شخصی شهروندان، ۴. الزامات افشای

1. DLA

داده‌های شخصی کاربران در فضای مجازی، ۵. حقوق کاربران در زمینه حریم خصوصی در فضای مجازی، ۶. مسئولیت‌های متولیان داده‌های شخصی در فضای مجازی، ۷. الزامات دسترسی کاربر به داده‌های شخصی. با توجه به این الزامات و در نظر گرفتن اسناد و سیاست‌های کلی کشور می‌توان به شاخص‌ها و سیاست‌های مشخصی برای قانونگذاری در این عرصه دست یافت.

منابع و مآخذ

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

۲. محسنی، فرید. گفتمان سیاست جنایی قانونگذار در قانون احترام به آزادی‌های مشروع و حفظ حقوق شهروندی، ۱۳۸۶.

3. Belgium Data Protection Law. (2001). Data Protection Law (DPL). [Online], Retreived from: https://www. privacycommission. be [2/5/2016]

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

5. Canada Privacy Act. (2016). Privacy Act of 198. [Online], Retrieved from: http://laws-lois. justice. gc. ca/PDF/P-21. pdf [3/14/2016]

6. Cox, C. , Mullooly, O. , Bollard, C. , O'Brien, C. & Neary, J. (2015). Data protection in Ireland: overview, [Online], Retreived from: uk. practicallaw. com/6-505-8262#a745226 [2/5/2016]

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

8. Finn, P. & Horwitz, S. (June 21, 2013). U. S. charges Snowden with espionage, The Washington Post, [Online], Retrieved from: http://www. washingtonpost. com/world/national-security/us-charges-snowden-with-espionage/2013/06/21/507497d8-dab1-11e2-a016-92547bf094cc_story. html [4/26/2016]

9. Fischer-Hübner, S. (2001). IT-security and privacy: design and use of privacy-enhancing security mechanisms. Springer-Verlag.

10. Germany Federal Data Protection Act. (2014). Federal Data Protection Act of 2014(FDPA). [Online], Retreived from: www. bfdi. bund. de. [2/13/2016]

11. Greenleaf, G. (2009). Five years of the APEC Privacy Framework: Failure or promise?. Computer Law & Security Review, 25(1), 28-43.

12. Greenleaf, G. , & Park, W. I. (2012). Korea’s new Act: Asia’s toughest data privacy law. Privacy Laws & Business International Report, (117), 1-6.

13. Häger, E. W. (2015). Data protection in Sweden: overview. [Online], Retrieved from: uk. practicallaw. com/8-502-0348 [4/17/2016]

14. Holmes, N. (2008). Canada's Federal Privacy Laws. [Online], Retrieved from: www. lop. parl. gc. ca/content/lop/researchpublications/prb0744-e. htm#proposals [4/17/2016]

15. Ireland Data Protection Act. (2003). Data Protection Act of 2003(DPA). Retreived from https://www. dataprotection. ie.

16. Japan-Personal-Information-Protection-Act. (2003). Personal Information

Protection Act. Japan Government, [Online], Retreived from: http://www5. cao. go. jp/seikatsu/kojin/foreign/act. pdf.
17. Italian Personal Data Protection Code. (2003). Personal Data Protection Code of 2003(PDPC). Retreived from www. privacy. it/privacycode-en. htm.
18. 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/oecdguidelinesontheprotectionofprivacyandtransborderflowsofp ersonaldata. htm#part2 [4/26/2016]
19. Panetta, R. & D'Ottavio, A. (2015). Data protection in Italy: overview. [Online], Retreived from:uk. practicallaw. com/9-502-4794?service=crossborder [3/12/2016]
20. Parent, W. A. (1983). Privacy, morality, and the law. Philosophy & Public Affairs, 269-288.
21. Philippe, J. (2015). Data protection in France: overview, [Online], Retreived from: uk. practicallaw. com/6-502-1481?service=crossborder [3/12/2016]
22. Spanish Data Protection Act. (2008). Data Protection Act. [Online], Retreived from: www. agpd. es [4/9/2016]
23. UK Data Protection Act. (2015). Data Protection Act of 1998(DPA). [Online] Retreived from: https://ico. org. uk [1/12/2016]

مرکز پژوهش‌های مجلس شورای اسلامی

شناسنامه گزارش	شماره مسلسل: ۱۵۸۷۷

عنوان گزارش: بررسی قوانین حفاظت از داده‌های کاربران در کشورهای منتخب

نام دفتر: مطالعات ارتباطات و فناوری‌های نوین (گروه فناوری اطلاعات و ارتباطات)

تهیه و تدوین‌کنندگان: مهدی فقیهی، محمدجواد جمشیدی

ناظر علمی: حسین افشین

متقاضی: معاونت پژوهش‌های زیربنایی و امور تولیدی

ویراستار تخصصی: ـــــــ

ویراستار ادبی: ـــــــ

واژه‌های کلیدی:

۱. حمایت از داده‌ها

۲. حفاظت از داده‌ها

تاریخ انتشار: ۱۳۹۷/۳/۹