



اعمال فراسرزمینی قانون اروپایی حفاظت از داده‌های شخصی در آمریکا

محمدعلی شریفی کیا؛ فریده شعبانی جهرمی^۲

چکیده

در عصر حاضر، لزوم حمایت از داده‌های شخصی کاربران در فضای مجازی، امری گریزناپذیر است؛ بنابراین، حکومت‌ها و سازوکارهای منطقه‌ای و بین‌المللی مانند اتحادیه اروپا نیز دست به فعالیت‌های تقنینی در این عرصه زده‌اند. از یک سو، برداشت غالب درباره قوانین مصوب درون اتحادیه اروپا این است که اجرای این قوانین، محدود به سرزمین دولت‌های تشکیل‌دهنده این نهاد منطقه‌ای است و از سوی دیگر، از مفاد آخرین سند حفاظت از داده اروپا (GDPR, 2016) چنین برداشت می‌شود که ویژگی فرامرزی داشته و در خارج از مرزهای اتحادیه نیز قابل اعمال است. پژوهش حاضر نیز با استفاده از روش تحلیلی-توصیفی در تلاش است با بررسی متن این سند و نسخه پیشین آن (DPD, 1995) و مهم‌ترین پرونده‌های مطرح‌شده در دیوان دادگستری اتحادیه اروپا درباره انتقال داده‌های شخصی کاربران اروپایی به ایالات متحده آمریکا، امکان اعمال فرامرزی این سند را در کشورهای غیرعضو اتحادیه، مانند آمریکا، واکاوی کند. سرانجام، یافته‌های پژوهش حاضر حاکی از این است که با توجه به قدرت سیاسی و اقتصادی قابل توجه اتحادیه، تعداد زیاد کاربران اروپایی در فضای نت، تفاسیر و آرای ارائه‌شده توسط دیوان اروپا، پیشینه سازوکارهای انتقال داده بین اروپا و آمریکا، و همچنین، ضمانت اجراهای پیش‌بینی‌شده در این سند، می‌توان گفت، در عمل، این مقررات، ویژگی فرامرزی دارند و در خارج از اتحادیه نیز اعمال می‌شوند.

کلیدواژه‌ها: اعمال فرامرزی قوانین اروپا، حفاظت از داده‌های شخصی، راهنمای حفاظت از داده (۱۹۹۵)، مقررات عمومی حفاظت از داده‌های شخصی (۲۰۱۶)، ایالات متحده آمریکا



۱. کارشناس ارشد رشته حقوق بین الملل، دانشکده حقوق، دانشگاه تهران، ایران، نویسنده مسئول:

(mo.ali.kia@gmail.com / ali.ghadamgahi@ut.ac.ir)

۲. استادیار، دانشکده حقوق، دانشکده گان فارابی، دانشگاه تهران، ایران. (faridehshabani@ut.ac.ir)

The Ability to Apply EU law's Extraterritorially in the United States

Mohammad Ali Sharifi Kia¹, Farideh Shabani Jahromi²

Abstract

The need to protect users' personal data in cyberspace is inevitable nowadays, thus governments and regional and international mechanisms such as the European Union have also taken legislative actions in this regard. On the other hand, the interpretation of the framework of laws adopted within the European Union is that the implementation of these laws is also limited to the territory of the constituent states of this regional body, while the provisions of the latest European Data Protection Document (GDPR: 2016) shows that it has extraterritorial character and can be applied outside the borders of the union. Therefore, this study uses a descriptive analytical method to examine the text of this document and its previous version (DPD: 1995), and the most important cases before the European Union Court of Justice regarding the transfer of European users' personal data to the United States of America to clarify the possibility of cross-border application of this document in non-EU countries. Finally, the findings of the present study indicate that due to the significant political and economic power of the Union, the large number of European users in the Internet space, interpretations and opinions provided by the European Court, history of data transfer mechanisms between Europe and the United States, as well as the administrative mandates provided in this document, it can be said that in practice this regulation has extraterritorial character and is applied outside the union.

Key words: Extraterritorial enforcement of European laws, Personal data protection, Data protection directive (1995), General data protection regulations (2016), United States of America



۳۳۳

اعمال فراسرزمینی قانون
اروپایی حفاظت از
داده‌های شخصی در
آمریکا

¹ Master of International Law, Faculty of Law, University of Tehran, Iran

(Corresponding Author, Email: mo.ali.kia@gmail.com / ali.ghadamgahi@ut.ac.ir)

² Assistant Professor, Faculty of law, College of Farabi, University of Tehran, Iran

مقدمه

راهنمای حفاظت از داده‌های شخصی^۱ و همچنین، مقررات عمومی حفاظت از داده‌های شخصی^۲ از مجموعه قوانین حفظ حریم خصوصی و داده‌های شخصی در اتحادیه اروپا به شمار می‌آیند که سازمان‌ها را ملزم می‌کنند، داده‌های اشخاص را ایمن نگه دارند؛ درحالی‌که به افراد، کنترل بیشتری بر نحوه استفاده از داده‌ها می‌دهند. بندهای سه‌گانه ماده ۳ مقررات عمومی، هرگونه پردازش داده‌های شهروندان اروپا را در هر کجا که باشند، مشمول قواعد آن می‌داند؛ بنابراین، شرکت‌های بزرگ پردازش‌کننده داده که در کشورهای غیر عضو اتحادیه نیز مستقر هستند (برای مثال، شرکت‌های بزرگ پردازنده داده که مقر اصلی فعالیت آن‌ها در ایالات متحده آمریکا است، مانند فیس‌بوک^۳، گوگل^۴، آمازون^۵ و...) اگر خواهان دسترسی به داده‌های کاربران و اتباع اتحادیه اروپا باشند، باید از مفاد این مقررات عمومی پیروی کنند که این خود، به دلیل ویژگی فرامرزی^۶ این سند قانونی است.

مقررات عمومی، در عمل، نخستین قانونی است که همه کشورهای عضو اتحادیه و همچنین، خدمات‌دهندگان بین‌المللی که با داده‌های شخصی شهروندان اتحادیه سروکار دارند، ملزم به رعایت مفاد آن هستند؛ درحالی‌که تا سال ۲۰۱۸ که این سند لازم‌الاجرا شد، برخی اسناد مورد توافق کشورهای اروپایی، تنها جنبه توصیه‌ای در زمینه قانون‌گذاری داخلی کشورها داشتند (اصول سازمان همکاری و توسعه اقتصادی^۸ و راهنما)، و تعدادی از مقررات دیگر، تنها درباره برخی زمینه‌های خاص ابلاغ شده و



۳۳۴

پژوهش‌نامه ایرانی

سیاست بین‌الملل،

سال ۱۲، شماره ۱، شماره

پیاپی ۲۳، پاییز و زمستان

۱۴۰۲

۱ Data Protection Directive (1995)

- (DPD) از این پس در متن با عنوان «راهنما» خواهد آمد.

۲ General Data Protection Regulation (2016)

- (GDPR) از این پس در متن با عنوان «مقررات عمومی» خواهد آمد.

۳ Facebook

۴ Google

۵ Amazon

۶ Extra-Territorial in Scope

۷ <https://gdpr.eu/>

۸ در اواخر دهه ۱۹۸۰، کشورهای عضو سازمان همکاری و توسعه اقتصادی، تدوین مقررات عمومی‌ای را ضروری دانستند که به هماهنگ کردن قوانین ملی حفظ حریم خصوصی کمک کند و درعین حال که از حقوق بشر حمایت می‌کند، از بروز وقفه در انتقال جریان‌های بین‌المللی داده نیز جلوگیری کند. این مقررات در قالب یک توصیه‌نامه از سوی شورای OECD، توسط گروهی از کارشناسان و متخصصان دولتی در ۲۲ ماده، تهیه و در ۲۳ سپتامبر ۱۹۸۰ به تصویب رسید و قابل اجرا شد و پس از آن، بسیاری از کشورهای عضو این سازمان یا قواعد

دست به قاعده‌سازی زده‌اند (Directive, 2002; Directive, 2006).

نکته قابل توجه و شاید جدید دربارهٔ مقررات عمومی، ویژگی فرامرزی^۳ و قابلیت اعمال آن بر شرکت‌های خدمات‌دهنده و نهادهای ارائه‌دهندهٔ خدمات مجازی و الکترونیکی، در ورای مرزهای سرزمینی اتحادیه اروپا و خارج از آن است. همان‌گونه که در بخش قلمرو سرزمینی این مقررات عمومی نیز اشاره شده است:

«اعمال این قانون تنها برای سازمان‌های درون اتحادیه اروپا لازم‌الاجرا نیست، بلکه سازمان‌هایی که داده‌های شخصی مرتبط با افراد درون اتحادیه اروپا را برای پیشنهاد کالا یا خدمات پردازش می‌کنند، صرف‌نظر از اینکه پرداخت به چه شکلی باشد، یا رفتار اشخاص موضوع داده را درون اتحادیه اروپا، بررسی و نظارت می‌کنند نیز مشمول اجرای این قانون هستند؛ حتی اگر در خارج از اتحادیه اروپا باشند یا تابعیت اروپایی نداشته باشند (GDPR, chapter 1, article, 3)».

ضمانت اجرای این مقررات عمومی در اصل این است که نقض مقررات مندرج در مقررات عمومی می‌تواند جریمه‌های بسیار سنگینی برای شرکت‌ها یا نهادهای سرپیچی‌کننده داشته باشد؛ تا آنجا که در برخی موارد به دادگاه‌های ملی و منطقه‌ای مجوز داده شده است تا جریمه‌های مالی تا سقف ۲۰ میلیون یورو یا ۴ درصد کل تراکنش سالیانهٔ آخرین سال مالی شرکت خاطی را برای جبران خسارت زیان‌دیدگان در نظر بگیرد (GDPR, chapter 8, article 83).

شاید در نگاه نخست، مبلغ ۲۰ میلیون یورو در مقایسه با درآمد سالانهٔ برخی پیشگامان عرصهٔ خدمات سایر

پیشین خود را با آن هماهنگ کردند یا دست به تدوین قواعد جدید در راستای محتویات این راهنما زدند؛ البته گفتنی است، این رهنمودها همراه با یک یادداشت توضیحی به‌منظور فراهم کردن اطلاعات موردنیاز دربارهٔ بحث‌ها، استدلال‌ها، و منطقی که بر ساختار آن‌ها تأکید دارد، ارائه و در سال ۲۰۱۳ توسط همان سازمان به‌روزرسانی شده است:

- Organization for Economic Co-operation and Development (OECD)

۱. مقررات عمومی نگهداری داده‌های شخصی تولید و پردازش شده در چارچوب تأمین خدمات ارتباطی الکترونیکی (۲۰۰۶):

DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 March 2006.

۲. مقررات عمومی حفظ حریم خصوصی و ارتباطات الکترونیکی:

DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 July 2002/ concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

۳ Extra-Territoriality in Scope

۴ Monitor





در جهان امروزی، مبلغ بسیار ناچیزی به‌نظر برسد، ولی بخش دوم جریمه‌های پیش‌بینی‌شده توسط این مقررات عمومی به مبالغ بسیار بالاتری خواهد رسید؛ برای مثال، براساس گزارش یکی از سایت‌های معتبر تجزیه‌وتحلیل داده‌های مالی، سود سالیانه شرکت مایکروسافت در سال ۲۰۲۰، ۴۴/۲۸ میلیارد دلار آمریکا^۱ برآورد شده است (<https://www.statista.com/statistics/267808/net-income-of-microsoft-since-2002>) که در این صورت، اگر این شرکت در سال ۲۰۲۱ توسط دادگاه‌های اتحادیه یا محاکم ملی دیگر در کشورهای غیر اتحادیه اروپا، با جریمه‌ای برابر ۴ درصد سود سال ۲۰۲۰ خود روبه‌رو شود، باید حدود ۱/۷۶ میلیارد دلار بپردازد که به‌مراتب، بالاتر از مبلغ ۲۰ میلیون یورو خواهد بود.

بنابراین، با توجه به اینکه از یک سو، بزرگ‌ترین خدمات‌دهندگان فضای سایبر فعلی جهان، شرکت‌هایی با تابعیت ایالات متحده هستند و این شرکت‌ها برای ارائه خدمات به گردآوری و پردازش داده‌های شخصی افراد نیاز دارند و از سوی دیگر، اتحادیه اروپا با تصویب راهنما و مقررات عمومی، قصد حفاظت از داده‌های شخصی اتباع خویش را در فرایندهای پردازش و انتقال داده‌ها دارد و قوانین اتحادیه اروپا نیز بر کشورهای غیر عضو، بدون توافقات رسمی و رضایت کشور ثالث قابل اعمال نیستند، در پژوهش حاضر، ابتدا اشاره‌ای کلی به برخی ویژگی‌ها و همسانی‌های مهم راهنمای حفاظت از داده اروپا و مقررات عمومی حفاظت از داده‌های شخصی، که به‌نوعی نسخه به‌روزشده راهنما است (Ghadamgahi, 2021, 53)، خواهد شد و پس از آن، سازوکارهای انتقال داده بین اروپا و ایالات متحده و همچنین، برخی از مهم‌ترین آرای قضایی دیوان دادگستری اروپا درباره مشروعیت انتقال داده‌های شهروندان اروپا به این کشور بررسی خواهد شد. سرانجام نیز با در نظر گرفتن موارد بیان‌شده و بحث‌های یادشده، به این پرسش پاسخ خواهد داد که «اتحادیه اروپا با تصویب مقررات عمومی اروپایی تاچه‌حد در اعمال قوانین خود در ورای مرزهایش و سرزمین یک کشور ثالث (یا غیر عضو) مانند ایالات متحده، موفق بوده است؟»

۱. پیشینه پژوهش

در بررسی پیشینه پژوهش‌های انجام‌شده، مقاله یا نوشته‌ای یافت نشد که به‌طور مشخص، اعمال فرامرزی مقررات حفاظت از داده‌های شخصی اروپا در ایالات متحده آمریکا را بررسی کرده باشد، اما موضوعات مشابهی در زمینه‌های مرتبط وجود داشت که به‌عنوان نمونه به برخی از آن‌ها اشاره شده است.

^۱ Microsoft

۲ 44.28 Million Dollars (U.S)

محمد تقی کروی در کتابی با عنوان «اتحادیه اروپا و بحث حمایت از داده‌های شخصی و حریم خصوصی در ارتباطات الکترونیکی» در پی بررسی کنوانسیون حمایت از افراد در پردازش خودکار داده‌های شخصی ۱۹۸۱ و دستورالعمل‌های پارلمان و شورای اروپا از سال ۱۹۹۵ تا ۲۰۰۲ بوده و به‌طور مشخص بر روند قانون‌گذاری و سیر تکامل قواعد بین‌المللی امروزی در این زمینه تمرکز داشته است؛ اما همان‌گونه که اشاره شد، پایان بازه زمانی این پژوهش، سال ۲۰۰۲ بوده و به موضوع مقررات عمومی حفاظت از داده اتحادیه را که در سال ۲۰۱۶ تصویب شد، توجه نداشته است.

بیتا نجفی شوشتری در پایان‌نامه کارشناسی ارشد خود با عنوان «نقش مراجع حمایت از داده‌های شخصی با نگاهی به آیین‌نامه حمایت از داده‌های ۲۰۱۶ اتحادیه اروپا» نحوه عملکرد مراجع عمومی و مستقلاً را که توسط پارلمان اروپا برای نظارت بر حسن اجرای این مقررات عمومی در سرتاسر اتحادیه و به‌صورت موردی در کشورهای عضو پیش‌بینی شده است (مقام ناظر)، بررسی کرده و اشاره‌ای نیز به عملکرد کمیته حمایت از داده اتحادیه اروپا داشته است. البته همان‌گونه که از عنوان پژوهش یادشده پیداست، موضوع اصلی آن، مراجع به‌وجودآمده توسط اتحادیه برای نظارت بر اجرای مقررات یادشده بوده و اشاره چندانی به مفاد حمایتی بیان‌شده درباره اعمال فرامرزی این مقررات در کشورهای غیرعضو مانند ایالات متحده آمریکا ندارد.

فلور قاسم‌زاده و لیلا رئیسی دزکی در مقاله‌ای با عنوان «چالش‌های نظام حقوقی ایران در نقض داده‌های شخصی و حریم خصوصی در فضای سایبر» مشکلات نظام حقوقی ایران را در بازدارندگی از نقض حریم خصوصی و داده‌های شخصی در فضای سایبر بررسی کرده و با اشاره به دستاوردهای مثبت و برخی معضلات این نظام حقوقی، پیشنهادهایی را برای شناسایی چارچوب‌های مناسب‌تر در راستای تدوین قوانین به‌روز و کاربردی و همچنین، رفع معضلات این نظام، ارائه داده است؛ اما مورد مطالعه این پژوهش، تنها بررسی حقوق ایران بوده و فقط اشاره‌هایی جزئی به مقررات عمومی اروپایی موردنظر پژوهش حاضر کرده‌اند.

آمنه صرامی در مقاله‌ای با عنوان «بررسی موافقت‌نامه انتقال فرامرزی داده‌های شخصی بین ایالات متحده آمریکا و اتحادیه اروپا؛ با نگاهی به قوانین جمهوری اسلامی ایران» اصول حریم خصوصی بندرگاه ایمن و سپر حریم خصوصی اروپا را بررسی، و با دیدگاهی کلی، برخی مفاد این سازوکارهای انتقال داده را تشریح کرده است. همچنین، نویسنده اشاره کوتاهی به الزامات حقوقی انتقال فرامرزی داده در جمهوری اسلامی ایران داشته است؛ اما در پژوهش حاضر، مفاد مندرج در متن این سازوکارها، چندان حائز اهمیت

نموده و تمرکز اصلی بحث بر اهمیت مقررات عمومی اتحادیه اروپا است که ایالات متحده را به طراحی و اجرای چنین سازوکارهایی وادار می‌کند.

۲. راهنمای حفاظت از داده اتحادیه اروپا و سند مقررات عمومی

در اکتبر سال ۱۹۹۵، پارلمان و شورای اروپا یک سازوکار قانونی را با عنوان «راهنمای حفاظت از داده‌های شخصی» تصویب کردند که هدف اصلی آن «حفاظت از افراد در رابطه با پردازش داده‌های شخصی و آزادی گردش این نوع داده‌ها» اعلام شد (DPD, Cf. Directive n. 95/46/ce). مصوبه یادشده در عمل، در مقام راهنمای کشورهای عضو اتحادیه ظاهر شد که چارچوب‌های قانون‌گذاری در حیطه پردازش داده‌های شخصی شهروندان اتحادیه را مشخص می‌کرد.

نویسندگان این راهنما درباره علت لزوم پیروی کشورهای عضو اتحادیه از آن، در مقدمه چنین شرح داده‌اند که از آنجا که اهداف جامعه اروپایی، همان‌گونه که در عهدنامه تشکیل اتحادیه اروپا بیان شده است، شامل ایجاد اتحادی نزدیک‌تر بین مردم اروپا، پرورش دادن روابط نزدیک‌تر بین کشورهای اتحادیه، تضمین پیشرفت‌های اقتصادی و اجتماعی با از بین بردن موانعی که اروپا را از هم جدا می‌کند، بهبود شرایط زندگی مردم اروپا، حفظ و تقویت صلح و آزادی و ترویج دموکراسی برپایه حقوق اساسی به رسمیت شناخته شده در قانون اساسی کشورهای اروپایی و همچنین، حقوق مندرج در کنوانسیون اروپایی برای حمایت از حقوق بشر و آزادی‌های اساسی، است (DPD, introduction, para: 1) و همچنین، به این سبب که نظام‌های پردازش داده برای خدمت به نوع بشر طراحی شده‌اند، بنابراین، لازم است که فارغ از ملیت یا اقامتگاه شخص حقیقی، به حقوق و آزادی‌های اساسی وی، به‌ویژه حق بر حریم خصوصی او، احترام گذاشته و همچنین، به پیشرفت اقتصادی و اجتماعی و گسترش تجارت و رفاه افراد کمک کنیم (DPD, Introduction, para, 2)؛ به این ترتیب، نویسندگان این راهنما، به هماهنگی آن با بند ۸ کنوانسیون اروپایی حقوق بشر و حمایت از آزادی‌های اساسی (برای داشتن زندگی خصوصی و خانوادگی) اشاره کرده‌اند (Users data protection, 2018, 9).

این راهنما، سه اصل کلی شفافیت، هدف مشروع، و تناسب را برای قانونگذاری به کشورهای عضو

۱. همچنین:

Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols: No. 11 and 14, article: 8.

۲ Transparency



۳۲۸

پژوهش‌نامه ایرانی
سیاست بین‌الملل،
سال ۱۲، شماره ۱، شماره
پیاپی ۲۳، پاییز و زمستان
۱۴۰۲

پیشنهاد می‌دهد که به‌نظر می‌رسد، از یک سو، ارتباط مفهومی آشکاری با اصول معرفی شده توسط سازمان همکاری و توسعه اقتصادی در این زمینه دارند (Ghadamgahi, 2021, 47)، و از سوی دیگر، به‌طور مشخص از کشورهای عضو می‌خواهد که از شهروندانشان در برابر نقض حقوق بنیادین شهروندی و آزادی‌های فردی، به‌ویژه در زمینه حفاظت از داده‌های شخصی آن‌ها حمایت کنند، و در عین حال، از گردش جریان آزاد داده‌ها حمایت کرده و هرگونه محدودسازی این جریان در بین کشورهای عضو اتحادیه، ممنوع است (<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046>, articles: 1-2).

راهنمای یادشده نیز مانند اصول سازمان توسعه و همکاری اقتصادی، جنبه پیشنهادی داشته و هنوز الزام قطعی‌ای برای رعایت جزئی مفاد و موارد مربوط به حفاظت از داده‌های شخصی توسط ارکان رسمی اتحادیه اروپا به کشورهای عضو ابلاغ نشده است و تا این زمان معمولاً هر کشوری، خود در این باره قاعده‌سازی کرده است (البته این راهنما که خود دربرگیرنده همه اصول یادشده است، نقش بسزایی در شکل‌گیری قواعد جدید تدوین شده در این زمینه توسط کشورهای عضو داشته است؛ همان‌گونه که در ادامه اشاره خواهد شد، پس از لازم‌الاجرا شدن مقررات عمومی، برخی کشورهای عضو در مقدمه متون قوانینی که تصویب می‌کنند، بر ایجاد هماهنگی‌های جدید با متن این سند تأکید کرده و قوانین پیشین را که در راستای این راهنما بودند، نسخ می‌کنند).

این راهنما از اصول اولیه حفاظت از داده‌ها که در کنوانسیون ۱۰۸ آمده است، پیروی می‌کند، اما شامل شش معیار برای مشروعیت پردازش داده‌ها است که در کنوانسیون، مشخص نشده است. به این معنا که

۱ Legitimate purpose

۲ Proportionality

۳. در اوایل دهه ۱۹۷۰، شورای اروپا به این نتیجه رسید که ماده ۸ کنوانسیون اروپایی حقوق بشر در پرتو پیشرفت‌های جدید، به‌ویژه با توجه به استفاده روزافزون از فناوری اطلاعات، دارای کاستی‌هایی است که عبارتند از: عدم اطمینان درباره آنچه تحت پوشش «زندگی خصوصی» قرار می‌گیرد، تأکید بر محافظت در برابر مداخله مقامات دولتی و فقدان رویکرد فعال‌تر، همچنین، مقابله با سوءاستفاده احتمالی از اطلاعات شخصی توسط شرکت‌ها یا سایر سازمان‌های مرتبط در بخش خصوصی. این مسئله موجب ارائه دو توصیه توسط کمیته وزیران به کشورهای عضو شد، تا تمام اقدامات لازم را برای اجرای برخی اصول مربوط به حفاظت از حریم خصوصی افراد در بخش خصوصی و عمومی انجام دهند، که سرانجام، منجر به تصویب کنوانسیون حفاظت از داده‌ها در سال ۱۹۸۱ و در استراسبورگ شد که به‌عنوان کنوانسیون ۱۰۸ نیز شناخته شده و نخستین ابزار الزام‌آور قانونی در سطح بین‌المللی برای حفاظت از داده‌ها است. هدف کنوانسیون این بود که در قلمرو هر یک از طرفین و برای هر شخصی، صرف‌نظر از ملیت یا محل اقامت، احترام به حقوق و آزادی‌های اساسی و به‌ویژه حق او بر حفظ حریم خصوصی، با توجه به پردازش خودکار داده‌های شخصی مربوط به مفهوم (داده‌های شخصی) را تضمین کند. در دسترس در نشانی زیر:

<https://www.coe.int/en/web/data-protection/convention108-and-protocol>.





براساس آن، داده‌های شخصی، تنها در صورتی قابل پردازش هستند که شخص موضوع داده، به گونه‌ای واضح رضایت داده باشد (Hustinx, 2017, 10-12)، یا پردازش داده به منظور اجرای قراردادی که شخص موضوع داده یک طرف آن است انجام شود، یا برای رعایت یک تعهد قانونی، برای اجرای یک عملیات دولتی، به منظور حفاظت از منافع حیاتی شخص موضوع داده، یا حفاظت از منافع مشروع کنترل‌کننده باشد؛ به استثنای مواردی که این منافع تحت تأثیر منافع شخص موضوع داده قرار گرفته باشد، که به نظر می‌رسد، استثنای یادشده در راهنما، بر اولویت منافع شخص موضوع داده بر منافع کنترل‌کننده‌ها از نظر تدوین‌کنندگان آن، تأکید خاصی دارد.

با گذشت چند سال از تصویب راهنمای حفاظت از داده، «اتحادیه اروپا پس از مدت‌ها مذاکره بر سر پیشنهاد اولیه‌ای که توسط شورای اروپا در سال ۲۰۱۲ مطرح شده بود، به منظور حمایت از حریم خصوصی افراد و حفاظت از داده‌های شخصی آنان در فضای سایبر، مجموعه قوانینی را در قالب مقررات عمومی حفاظت از داده اتحادیه اروپا، تصویب و اجرا کرد که پس از لازم‌الاجرا شدن آن در سال ۲۰۱۸، جایگزین راهنمای حفاظت از داده اتحادیه اروپا (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995) شد و همه کشورهای عضو اتحادیه ملزم به هماهنگ‌سازی نظام حمایت از داده خود با آن شدند» (Ghadamgahi, 2021, 4). گفتنی است، در حال حاضر سند مقررات عمومی حفاظت از داده، مهم‌ترین سند حقوقی بین‌المللی برای حفاظت از داده‌های شخصی کاربران فضای سایبر است و همه نهادهایی که قصد پردازش و انتقال داده‌های کاربران اروپایی را دارند، ملزم به رعایت مفاد آن هستند.

۳. اصول حریم خصوصی بندرگاه ایمن و سپر حفاظتی حریم خصوصی اروپا

مهم‌ترین مقررات حفاظت از داده در اتحادیه اروپا تا سال ۲۰۰۰، همان راهنمای حفاظت از داده مصوب سال ۱۹۹۵ بوده است که براساس آن، انتقال داده‌های شخصی شهروندان اروپایی به کشورهای ثالث، ممنوع و غیرمجاز است. اما بند ۶ ماده ۲۵ این راهنما به کمیسیون حفاظت از داده اروپا اجازه می‌دهد که

۱ General Data Protection Regulations (2018)

۲ April, 14, 2016

۳ May, 25, 2018

۴ Safe Harbor principles (2000)

۵ U.S – EU Privacy Shield (2016)

کشور ثالثی را که سطح مناسبی از حمایت از داده‌های شخصی را اعمال می‌کند، برای عملیات انتقال مجاز بشمارد تا انتقال داده‌ها به آن انجام شود (El khoury, 2015, 659).

اصول حریم خصوصی بندرگاه ایمن نیز پس از آنکه مقامات اتحادیه اروپا و ایالات متحده دریافتند که تفاوت‌های اساسی بین رژیم‌های حفاظت از داده‌ایالات متحده و اتحادیه اروپا سبب ایجاد اختلال یا جلوگیری از انتقال داده‌های شخصی بین اتحادیه اروپا و ایالات متحده خواهد شد، و همچنین، به این سبب که نگران بودند که این تفاوت در رویکردها بر روابط تجاری و سرمایه‌گذاری میان اتحادیه اروپا و ایالات متحده و همچنین، بسیاری از مشاغل و صنایع در هر دو سوی اقیانوس اطلس تأثیر منفی بگذارد (Weiss, 2016, 5)، به منظور قانونی کردن گردش جریان داده بین اتحادیه اروپا و آمریکا، توسط وزارت بازرگانی ایالات متحده در ۲۱ ژوئیه ۲۰۰۰ صادر شد (U.S. Department of Commerce, Safe Harbor Privacy Principles and Related Frequently Asked Questions, July 21, 2000) و اندکی پس از آن از طریق تصمیم کمیسیون اروپا (Commission Decision 2000/520/EC, of July 26, 2000) نیز به رسمیت شناخته شد و به کشورهای عضو ابلاغ گردید.

اصول بندر امن اروپا-آمریکا که با عنوان اصول هشت‌گانه حفظ حریم خصوصی در تجارت الکترونیک نیز شناخته می‌شوند، عبارتند از: اطلاع، انتخاب، محدودیت در انتقالات بعدی، امنیت، یکپارچگی داده‌ها، دسترسی، و اجرا؛ که هر شرکت مستقر در آمریکا می‌توانست به صورت داوطلبانه و با ارائه گواهی تعهد به اجرای اصول یادشده به وزارت بازرگانی ایالات متحده، به این طرح بپیوندد (El khoury, 2015, 659). اگرچه برخی پژوهشگران این سازوکار را یک چارچوب خودتنظیمی مفید به‌شمار می‌آوردند که به ابزار مؤثر و نوآورانه‌ای برای حفاظت از داده‌های شخصی در حال انتقال به ایالات متحده تبدیل شده است (Greer, 2011, 143)، ولی در ۶ اکتبر ۲۰۱۵، دیوان دادگستری اتحادیه اروپا تصمیمی صادر کرد که نظام اجرایی بندر امن را از همان روز، لغو و متوقف کرد. کما اینکه در حال حاضر نیز چنین است؛ تصمیم دیوان ناشی از شکایت یک تبعه اتریشی به نام ماکسیمیلیان شرمس از مقام نظارتی حفاظت از داده‌ایرلند

۱. برای مطالعه بیشتر به گزارش مرکز پژوهش‌های مجلس شورای اسلامی، صفحات ۲۴ و ۲۵، مراجعه شود؛ همچنین می‌توان به متن اصلی در آدرس زیر مراجعه کرد:

<http://www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm>

۲ The Court of Justice of the European Union (CJEU)

۳ Maximillian Schrems

بود، که در ادامه به آن اشاره خواهد شد.

سرانجام با توجه به دستور دیوان و بروز انتقادات و شکایت‌های روزافزون از سازوکار بندر امن، این نظام توسط اتحادیه اروپا کنار گذاشته شد و در ۱۲ ژوئیه ۲۰۱۶، کمیسیون اروپا سپر حفاظتی حریم خصوصی اروپا-آمریکا را برای فعال‌سازی دوباره طرح انتقال داده‌ها براساس قوانین اتحادیه اروپا، سازوکاری مناسب و چارچوب سپر حریم خصوصی را برای حفاظت از داده‌های شخصی کاربران اروپایی، کافی دانست (<https://www.privacyshield.gov/Program-Overview>)؛ اما سرانجام در تاریخ ۱۶ ژوئیه ۲۰۲۰، دیوان دادگستری اتحادیه اروپا، طی حکمی، تصمیم کمیسیون اروپا (Commission Implementing Decision (EU) 2016/1250 of 12 July 2016)، مبنی بر کفایت حمایت ارائه‌شده توسط سپر حفاظتی اتحادیه اروپا و ایالات متحده را، «بی‌اعتبار» اعلام کرد (CJEU, 16 July 2020) و به این ترتیب، این نظام حمایتی نیز متوقف شد، ولی بنا به دلایلی، که برای نویسندگان پژوهش حاضر مبهم و نامعلوم است، سایت رسمی سپر حفاظتی حریم خصوصی، برخلاف نظر دیوان، همکاری‌کنندگان و اعضای سپر امنیتی را از مسئولیت‌های خویش در این چارچوب، معاف نمی‌داند (<https://www.privacyshield.gov/Program-Overview>, para, 2).

۴. مهم‌ترین پرونده‌های قضایی مطرح‌شده درباره انتقال داده‌ها به ایالات متحده

با توجه به مطالب ارائه‌شده و اهمیت سازوکارهای انتقال داده‌های شخصی از اروپا به ایالات متحده آمریکا، در این بخش، برخی از مهم‌ترین پرونده‌های مطرح‌شده در دیوان دادگستری اروپا بررسی شده‌اند. همان‌گونه که مشاهده خواهد شد، دیوان در این پرونده‌ها با ارائه نظرات تفسیری و قضایی، انتقال داده‌های شخصی را به آمریکا به دلایل گوناگونی از جمله عدم رعایت مفاد راهنما و مقررات عمومی حفاظت از داده، متوقف و گاهی تصمیمات کمیسیون را نیز بی‌اعتبار کرده است.

۴-۱. پارلمان اروپا در مقابل شورا و کمیسیون اروپا

پس از حمله‌های (به‌ظاهر) تروریستی ۱۱ سپتامبر ۲۰۰۱، ایالات متحده در نوامبر ۲۰۰۱ قانونی را تصویب کرد که براساس آن، شرکت‌های هواپیمایی که به مقصد یا از مبدأ آمریکا پرواز می‌کنند، می‌بایست اجازه

۱ Data Protection Authority (DPA)

۲. ناظر حفاظت از داده، مقامی است که در کشورهای عضو اتحادیه اروپا، وظیفه نظارت بر حسن اجرای GDPR و همچنین، بررسی شکایت‌های اشخاص حقیقی، از پردازشگران تخطی‌کننده از مفاد این سند را به‌عهده دارد.

۳ Invalid



دسترسی الکترونیک به داده‌های سامانه‌های رزرواسیون و کنترل خروج خود را به مقامات گمرکی و امنیت ملی این کشور بدهند؛ این اطلاعات به داده‌های «سوابق نام مسافران» معروف بود (CJEU, JOINED CASES C-317/04 and C-318/04, para, 33). پس از آن، کمیسیون به اطلاع مقامات آمریکا رساند که این قوانین جدید ممکن است با مقررات کشورهای عضو در زمینه حفاظت از داده‌های شخصی و همچنین، برخی از مقررات عمومی شورا درباره آیین‌نامه عملکردی سامانه‌های رزرواسیون در تضاد باشد (۲۰۰۲)؛ بنابراین، مقامات ایالات متحده، اجرایی شدن این مقررات را به‌طور موقت به تعویق انداختند، اما در نهایت، اقدام به جریمه کردن شرکت‌هایی کردند که از این مقررات پیروی نمی‌کنند.

در نتیجه، کمیسیون اروپا، پیش‌نویس تصمیمی را درباره کفایت حفاظت‌های ارائه‌شده توسط آمریکا، برای تصویب به پارلمان تقدیم کرد (CJEU, JOINED CASES C-317/04 and C-318/04, para: 36). پس از آن شورا به دلیل فوریت مسئله و ضررهای اقتصادی‌ای که گریبان شرکت‌های اروپایی را می‌گرفت، از پارلمان خواست تا در اسرع وقت، نظر خود را درباره این تصمیم اعلام کند (CJEU, JOINED CASES C-317/04 and C-318/04, para: 37).

در تاریخ ۱۳ مارس ۲۰۰۴ پارلمان نتیجه را چنین اعلام کرد که تصمیم کمیسیون درباره مفاد و ماهیت حقوقی پیش‌نویس ارائه‌شده در زمینه کفایت حفاظت مورد نیاز از داده‌های شخصی، از قدرتی که ماده ۲۵ راهنما برای این نهاد در نظر گرفته، پیشی گرفته است (CJEU, JOINED CASES C-317/04 and C-318/04, para: 38). سرانجام، پارلمان اروپا در آوریل ۲۰۰۴ بنا به درخواست رئیس وقت خود، پیشنهاد کمیته امور حقوقی و بازار داخلی اروپا، مبنی بر درخواست نظر از دیوان دادگستری اروپا، را تأیید کرد (CJEU, JOINED CASES C-317/04 and C-318/04, para: 39) و در تاریخ ۱۷ مه ۲۰۰۴ با درخواست خود از دیوان، ابطال تصمیم شورا مبنی بر انعقاد یک موافقت‌نامه بین‌المللی میان جامعه اروپا و ایالات متحده، در زمینه پردازش و انتقال داده‌های سوابق نام مسافران توسط شرکت‌های هواپیمایی اروپایی به وزارت امنیت داخلی (اداره گمرکات و حفاظت از مرزها) را خواستار شد (CJEU, JOINED CASES C-317/04 and C-318/04, paras: 1-2).

سرانجام، دیوان با در نظر گرفتن جایگاه و نقش نهادهای یادشده، تصمیم شورا مبنی بر انعقاد توافق‌نامه

۱ Passenger Name Records (PNR data)

۲ United States Department of Homeland Security, Bureau of Customs and Border Protection





بین‌المللی با ایالات متحده و همچنین، تصمیم کمیسیون مبنی بر کفایت سطح حفاظت ارائه‌شده توسط آمریکا درباره داده‌های شخصی اتباع اروپا را ابطال کرد (CJEU, JOINED CASES C-317/04 and C-318/04, para: 75). این نظر دادگاه، نخستین موردی است که یک نهاد قضایی عالی اروپا، سطح حمایت از داده‌های شخصی را در ایالات متحده در حد کفایت قلمداد نکرده و از دسترسی نهاد‌های آمریکایی (حتی نهاد‌های دولتی) به داده‌های شخصی شهروندان اروپا جلوگیری می‌کند. در ادامه به موارد دیگری از این گونه نظرات دیوان در پرونده‌های گوناگون اشاره خواهیم کرد.

۴-۲. شرمس علیه ناظر حفاظت از داده ایرلند (شرمس ۱)

ماکسیمیلیان شرمس، فعال حقوقی اتریشی تبار، پس از افشاگری‌های بی سابقه ادوارد اسنودن (در مه ۲۰۱۳ و هم‌زمان با ورودش به هنگ‌کنگ) که تا آن زمان، مدیر سامانه‌های کامپیوتری شرکت آلن همیلتون^۱ بود، به‌طور رسمی از مقام ناظر حفاظت از داده^۲ (کمیسر) ایرلند شکایت کرد. مبنای این شکایت، ادعای اسنودن مبنی بر طرف قرارداد بودن شرکت محل کارش^۳ با آژانس امنیت ملی آمریکا^۴ شنود و نظارت مستقیم این آژانس آمریکایی (در غالب شرکت‌های پوششی و طرف قرارداد) بر اینترنت و سامانه‌های مخابراتی در مقیاس گسترده و جهانی بود. به این صورت که این نهاد آمریکایی، توسط شرکت‌های زیرمجموعه و طرف قرارداد خود و با استفاده از داده‌هایی که توسط شرکت‌های بزرگ خدمات‌دهنده اینترنتی آمریکایی گردآوری شده و در اختیار آن قرار می‌گیرد، اقدام به پایش و کنترل اطلاعات کاربران می‌کند (High Court of Ireland Decisions, [2014] IEHC 310).

این افشاگری‌ها، پیش‌زمینه دادخواست شرمس به دادگاه عالی ایرلند^۵ را فراهم کرد. وی بر این نظر بود که

^۱ Edward Snowden

^۲ Booz Allen Hamilton Corp

^۳ Data Protection Commissioner

^۴ در جریان این استخدام، اسنودن به‌طور غیرقانونی، هزاران پرونده محرمانه و طبقه‌بندی‌شده NSA را تصاحب و پس از ورودش به هنگ‌کنگ، برای رسانه‌هایی مانند گاردین (در بریتانیا) و نیویورک تایمز و واشنگتن پست افشا کرد.

^۵ US National Security Agency (NSA).

^۶ همچنین در دسترس در نشانی زیر:

<https://www.bailii.org/ie/cases/IEHC/2014/H310.html>, Para: 1. (آخرین دسترسی: بهمن ۱۴۰۰)

^۷ High Court of Ireland.

از آنجا که افشاگری‌های اسنودن نشان می‌دهد که هیچ رژیم مؤثر حفاظت از داده‌ای در ایالات متحده وجود ندارد، کمیسر حفاظت از داده باید از اختیارات قانونی خود برای جلوگیری از هدایت و انتقال داده‌های شخصی کاربران اروپایی توسط فیس بوک ایرلند به شرکت مادرش در ایالات متحده استفاده کند و این روند باید در اسرع وقت متوقف شود، (High Court of Ireland Decisions, [2014] IEHC 310, para: 2).

کمیسر نیز بر این نظر بود که وی متعهد به این تصمیم کمیسیون اروپا در ژوئیه ۲۰۰۰ است که رژیم حفاظت از داده‌های شخصی در ایالات متحده را برای شرکت‌هایی که داده‌ها را به ایالات متحده منتقل یا در آنجا پردازش می‌کنند، کافی و مؤثر می‌داند. بر این اساس، شرکت‌های آمریکایی، خود گواهی می‌دهند که با اصول تعیین شده در این تصمیم کمیسیون اروپا (اصول بندر امن که به آن اشاره شد) هماهنگی لازم را دارند (High Court of Ireland Decisions, [2014] IEHC 310, para: 2).

در کل پرونده، نتیجه‌گیری کمیسر مبنی بر اینکه شکایت متقاضی به لحاظ قانونی غیرقابل استماع است، دقیقاً به این دلیل است که از دیدگاه رژیم بندر گاه ایمن، انتقال این گونه داده‌ها جنبه بدیهی دارد و همچنین، بر این اساس که کمیسیون اروپا در گذشته به این نتیجه رسیده است که ایالات متحده، از داده‌های کاربران در سطح ملی به اندازه کافی حفاظت می‌کند؛ لیکن شرمس بر این نظر است که این تصمیم کمیسر به نوعی رفع مسئولیت از خود و غیرقانونی است (High Court of Ireland Decisions, [2014] IEHC 310, para: 3).

پس از بررسی دلایل و استدلال‌های ارائه شده توسط طرفین دعوی، قاضی محکمه (به‌طور خلاصه) چنین بیان می‌کند که به دلیل وجود عنصر بین‌المللی در پرونده حاضر و نیز به این سبب که در مورد مسئله مورد بحث، قانون اتحادیه اروپا، مفاد راهنمای عمومی حفاظت از داده ۱۹۹۵ اروپا، و نیز اصول بندر گاه ایمن میان اروپا و آمریکا، نسبت به قانون ملی ایرلند، ارجحیت بیشتری دارند (High Court of Ireland Decisions, [2014] IEHC 310, para: 80)، دیدگاه شرمس مبنی بر اینکه کمیسر به الزامات قانون اتحادیه اروپا پایبند نبوده است، درست نیست و در واقع، برعکس این موضوع صادق است؛ زیرا، کمیسر از دیدگاه خود به راهنمای ۱۹۹۵ و اصول بندر امن ۲۰۰۰ عمل کرده است (High Court of Ireland Decisions, [2014] IEHC 310, para: 82)، و سرانجام اینکه اعتراض متقاضی، در واقع، به شرایط خود رژیم بندر امن است نه به روشی که کمیسر، رژیم بندر امن را اعمال کرده است، و این اصول نیز بر اساس تصمیم کمیسیون اروپا اجرایی شده‌اند (High Court of Ireland Decisions, [2014] IEHC 310, para: 82).

در این شرایط، موضوع مهمی که مطرح می‌شود این است که آیا تفسیر مناسب از راهنما و تصمیم کمیسیون در ژوئیه ۲۰۰۰ در اختیار است و آیا باید در پرتو لازم‌الاجرا شدن آن‌ها، ماده ۸ منشور اروپا دوباره ارزیابی شود؟ و در نتیجه، آیا کمیسیون می‌تواند بنا به تشخیص خود، فراتر از این مقررات عمل کرده یا آن‌ها را نادیده بگیرد؟ برای روشن شدن پاسخ پرسش‌های یادشده و سایر ابهام‌های مرتبط با دعوی حاضر، رسیدگی به پرونده به‌طور موقت معلق شد و براساس ماده ۲۶۷ معاهده عملکرد اتحادیه اروپا، از دیوان دادگستری اروپا درخواست شد که در این باره اظهار نظر کند، تا پس از آن به رسیدگی به آن ادامه دهد (High Court of Ireland Decisions, [2014] IEHC 310, para: 84).

پس از اینکه پرونده یادشده توسط دادگاه عالی ایرلند به دیوان دادگستری اتحادیه اروپا ارجاع داده شد، دیوان با در نظر گرفتن این نکته که کمیسیون از پذیرفتن و بررسی شکایت اولیه شرمس خودداری کرده (CJEU, CASE C-362/14, paras: 1-2) و همین امر سبب ارجاع پرونده به دادگاه عالی ایرلند و سپس، به دیوان شده است، در تاریخ ۶ اکتبر ۲۰۱۵ اقدام به صدور رأی در این باره کرد.

دیوان پس از اینکه در پاسخ به ادعای شرمس، تصمیم کمیسیون اروپا مبنی بر راه‌اندازی و تأیید عملکرد رژیم بندر امن را در حیطه وظایف آن نهاد و در راستای احقاق حقوق اساسی‌ای همچون آزادی گردش اطلاعات می‌داند، به این نکته نیز اشاره می‌کند که کمیسیون براساس مفاد راهنما، قادر به تشخیص اینکه کدام کشور ثالث از سطح حمایت کافی در زمینه حفاظت از داده‌های شخصی برخوردار است، نیست (CJEU, CASE C-362/14, paras: 68-71)، و افزون‌بر این، این نکته را نیز مطرح می‌کند که لفظ «کافی» به کاررفته در توضیح راهنما، لزوماً به معنای همان سطح حمایتی که اتحادیه اروپا در قبال داده‌های شخصی ارائه می‌دهد، نیست (CJEU, CASE C-362/14, para: 73)؛ حال آنکه به نظر می‌رسد، هر مقداری از حمایت که از استانداردهای تعیین شده توسط اتحادیه کمتر باشد، به لحاظ منطقی می‌بایست به قید «ناکافی» ملقب شود؛ زیرا، دیوان در اینجا به بند ۶ ماده ۲۵ راهنمای یادشده اشاره کرده و ملاک تأیید کشور ثالث را در این زمینه، وجود قوانین داخلی یا تعهدات بین‌المللی در این باره، حکومت قانون، و حمایت قانونی از آزادی‌های اساسی در آن کشور می‌داند، که از دید این نهاد، در بررسی‌های کمیسیون نیز رعایت شده

۱. همچنین در دسترس در نشانی زیر:

(آخرین دسترسی: بهمن ۱۴۰۰). <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62014CJ0362>



است.

اما این موارد نیز لزوماً تضمین کننده وجود حمایت‌های کافی از داده‌های شخصی افراد نیست؛ زیرا، ممکن است کشوری با وجود مورد تأیید بودن در همه زمینه‌های یادشده، در حوزه فناوری‌های روز دنیا و کنترل فضای سایبر، از توان لازم برای حمایت از داده‌های دریافتی برخوردار نباشد؛ حال آنکه در این مورد نیز با توجه به مطالبی که بیان شد، می‌توان دریافت که در بهترین حالت ممکن، ایالات متحده با وجود در اختیار داشتن فناوری‌های مورد نیاز، به گونه‌ای عامدانه و بدون حسن نیت کافی، اقدام به پایش اطلاعات کاربران کرده است.

سرانجام، دیوان با در نظر گرفتن همه جوانب، چنین استدلال می‌کند که درستی عملکرد کمیسیون در ایجاد سازوکار بندرگاه ایمن و مورد تأیید دانستن سطح حمایتی ارائه شده توسط ایالات متحده یا هر کشور ثالث دیگری، مانع انجام وظایف کمیسر در شنیدن شکایت اتباع اروپا و بررسی حمایت‌های ارائه شده در زمینه حفاظت از داده‌های شخصی آن‌ها توسط کشورهای ثالث نخواهد شد؛ در نتیجه، دیوان با توجه به شواهد موجود در پرونده، در همین تاریخ، تصمیم کمیسیون اروپا درباره راه‌اندازی و عملکرد سامانه بندرگاه ایمن را نامعتبر دانسته و به این ترتیب، عمل به این رژیم را لغو کرد (CJEU, CASE C-362/14, para: 107).

این استدلال دیوان، به نوبه خود بسیار منحصر به فرد است؛ زیرا، دایره اختیارات مقام ناظر را بسیار گسترده دانسته و دامنه نظارت وی را به خارج از مرزهای اتحادیه و به خروجی عملکرد شرکت‌های خارجی در حمایت از داده‌های شخصی کاربران نیز بسط داده است. شاید همین دیدگاه‌های دیوان در آینده نزدیک پس از آن، زمینه‌ساز پیدایش جنبه فرامرزی در مقررات عمومی شده باشد. آنجا که نه تنها ناظران چنین اختیاراتی دارند، بلکه مفاد متن این مقررات عمومی نیز از این ویژگی برخوردار است.

این پرونده، بعدها در متون مربوط به حوزه حقوق داده‌ها و فناوری، به شرمس (۱) معروف شد؛ زیرا، این ادعای مطرح شده در نزد دادگاه عالی ایرلند، نخستین مرحله از دعوی ایشان علیه نظام تبادل داده اروپا-آمریکا در آن زمان بود و پس از اعلام نظر دیوان دادگستری اروپا درباره پرونده یادشده، دادگاه عالی ایرلند نیز به پیروی از آن، رأی نهایی را به نفع وی صادر کرد.

نکته دیگری که در اینجا اهمیت دارد، این است که این پرونده، در عمل، نخستین شکایتی بود که به صورت رسمی، نظام تبادل داده بندرگاه ایمن را به چالش می‌کشید و سرانجام نیز (همان گونه که در بخش بعدی اشاره خواهد شد) به طور کلی سبب الغای این نظام شد. شرمس پس از این پرونده یک نهاد

خصوصی را در قالب سایتی با هدف حمایت از حقوق مرتبط با حوزه دیجیتال اتباع اتحادیه اروپا (<https://noyb.eu/en>) راه اندازی کرد و کماکان نیز به صورت غیرانتفاعی در این زمینه مشغول فعالیت است.

۴-۳. شرمس علیه ناظر حفاظت از داده ایرلند (شرمس ۲)

شرمس پس از نتیجه گرفتن در شکایت نخست خود، در شکایت دیگری در ۱ دسامبر ۲۰۱۵، مدعی شد که قانون ایالات متحده، فیس بوک را ملزم می کند که داده های شخصی منتقل شده به آمریکا را در اختیار برخی مقامات این کشور، از جمله آژانس امنیت ملی و اداره تحقیقات فدرال قرار دهد. وی اظهار داشت، از آنجا که از آن داده ها در چارچوب برنامه های نظارتی گوناگون به شیوه ای ناسازگار با مواد ۷، ۸ و ۴۷ منشور استفاده شده است، سازوکار بندهای قراردادی استاندارد نمی تواند انتقال آن داده ها به ایالات متحده را توجیه کند؛ بنابراین، از کمیسر حفاظت از داده ایرلند خواست تا انتقال داده های شهروندان اروپا به ایالات متحده بر مبنای این نظام را متوقف کند (CJEU, CASE C-311/18, paras: 54-55).

پس از آن کمیسر حفاظت از داده ایرلند، یافته های خود را در قالب پیش نویسی به اطلاع عموم رساند. وی بر این نظر بود که داده های شخصی شهروندان اتحادیه اروپا که به ایالات متحده منتقل شده اند، احتمالاً توسط مقامات ایالات متحده کنترل و پردازش می شوند که با مواد ۷ و ۸ منشور ناسازگار است و قانون ایالات متحده برای این دسته از شهروندان، جبران های حقوقی متناسب با ماده ۴۷ منشور، ارائه نمی دهد. وی همچنین، دریافت که سازوکار بندهای قراردادی استاندارد، قادر به جبران خسارت های احتمالی در این زمینه نیست؛ زیرا، این رژیم تنها به حقوق شخص موضوع داده در برابر صادر کننده و وارد کننده داده اشاره



۳۳۸

پژوهش نامه ایرانی
سیاست بین الملل،
سال ۱۲، شماره ۱، شماره
پیاپی ۲۳، پاییز و زمستان
۱۴۰۲

۱ None Of Your Business - European Centre for Digital Rights

۲ Federal Bureau of Investigation (FBI).

۳. ماده ۷ منشور حقوق و آزادی های اساسی اتحادیه اروپا درباره حق بر احترام به زندگی خصوصی و خانواده.

۴. ماده ۸ منشور حقوق و آزادی های اساسی اتحادیه اروپا درباره حق بر حفاظت از داده های شخصی.

۵. ماده ۴۷ منشور حقوق و آزادی های اساسی اتحادیه اروپا درباره حق بر جبران خسارت مؤثر و رسیدگی قضایی عادلانه.

۶ Standard Contractual Clauses (SCC) for the transfer of personal data to processors established in third countries under the Commission Implementing Decision (EU) 2016/2297 of 16 December 2016;

- سازوکار (بندهای قراردادی استاندارد) که بر اساس تصمیم کمیسیون اروپا و بنا بر مجوز مقررات عمومی GDPR، به منظور انتقال داده های شخصی از اتحادیه اروپا به کشورهای ثالث پایه ریزی شده بود؛ برای مطالعه بیشتر در این باره می توان به نشانی زیر مراجعه نمود:

https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

داشته و مسئولیتی برای مقامات ایالات متحده قائل نیست (CJEU, CASE C-311/18, para: 56). با توجه به این مقدمات، کمیسر شکایت شرمس را به دادگاه عالی ایرلند ارجاع داد و دادگاه یادشده نیز به منظور دریافت پاسخ پرسش‌های خود درباره سازوکار سپر حریم خصوصی اروپا-آمریکا و رژیم بندهای قراردادی استاندارد، با درخواستی در ۴ مه ۲۰۱۸ این شکایت را به دیوان ارجاع داد. گفتنی است، این ارجاع دربردارنده ضمیمه‌ای از یافته‌های پیشین دادگاه عالی ایرلند درباره شواهد و مدارک این پرونده بود که نماینده دولت ایالات متحده نیز در این فرایند حضور داشت (CJEU, CASE C-311/18, paras: 57-58).

دادگاه ارجاع‌دهنده در مدارک ارسالی خود این گونه تصریح کرد که بخش ۷۰۲ از مقررات نظارت بر اطلاعات خارجی ایالات متحده، به دادستان کل و مدیر اطلاعات ملی آمریکا اجازه می‌دهد که به طور مشترک، پس از تأیید دادگاه نظارت بر اطلاعات خارجی آمریکا، مجوز نظارت بر افرادی را که شهروند ایالات متحده نیستند و در خارج از قلمرو قضایی ایالات متحده حضور دارند، برای دستیابی به داده‌های اطلاعاتی خارجی، صادر کند و همچنین، مبنای برنامه‌های نظارتی پریم (ابزار برنامه‌ریزی برای یکپارچه‌سازی، همگام‌سازی، و مدیریت منابع اطلاعاتی) و آپ استریم^۵ را فراهم کنند (CJEU, CASE C-311/18, paras: 61-62). دادگاه ارجاع‌دهنده دریافت که این سازوکار به آژانس امنیت ملی آمریکا اجازه می‌دهد که با دسترسی به کابل‌های زیر آب در کف اقیانوس اطلس، به داده‌های در حال انتقال به

۱ Foreign Intelligence Surveillance Act (FISA)

۲. بخش ۷۰۲، یکی از مواد کلیدی قانون اصلاحات FISA در سال ۲۰۰۸ است که به دولت ایالات متحده اجازه می‌دهد با کمک اجباری ارائه‌دهندگان خدمات ارتباط الکترونیکی (به منظور به دست آوردن داده‌های اطلاعاتی خارجی)، بر افراد خارجی (غیر آمریکایی) خارج از ایالات متحده، نظارتی هدفمند داشته باشد؛ برای مطالعه بیشتر در این باره می‌توان به نشانی‌های زیر مراجعه کرد:

<https://www.dni.gov/files/icotr/Section702-Basics-Infographic.pdf>;

<https://cdt.org/wp-content/uploads/2017/02/Section-702.pdf>;

<https://www.govinfo.gov/content/pkg/BILLS-110hr6304pcs/html/BILLS-110hr6304pcs.htm>.

۳ The United States Foreign Intelligence Surveillance Court (FISC, also called the FISA Court)

۴. PRISM: براساس یافته‌های دادگاه عالی ایرلند، در چارچوب برنامه PRISM، ارائه‌دهندگان خدمات اینترنتی موظفند همه ارتباطات را به و از یک شخص (انتخاب‌کننده) به آژانس امنیت ملی ارائه دهند که برخی از آن‌ها به FBI و آژانس اطلاعات مرکزی (CIA) نیز مخابره می‌شوند.

۵. UPSTREAM: درباره برنامه UPSTREAM نیز دادگاه عالی ایرلند دریافت که در چارچوب آن برنامه، شرکت‌های مخابراتی که ستون فقرات اینترنت را اداره می‌کنند (یعنی شبکه کابل‌ها، سوئیچ‌ها، و مسیریاب‌ها) باید به NSA برای کپی و فیلتر کردن جریان‌های ترافیک اینترنت، به منظور به دست آوردن ارتباطات از، به یا در مورد یک تبعه غیر آمریکایی مرتبط با یک شخص (انتخاب‌کننده) اجازه دهند. براساس این برنامه، NSA هم به داده‌ها و هم به محتوای ارتباطات مربوطه دسترسی دارد.



ایالات متحده دسترسی داشته باشد و پیش از رسیدن به ایالات متحده، در قالب مجوز قانون نظارت بر اطلاعات خارجی، چنین داده‌هایی را گردآوری و نگهداری کند (CJEU, CASE C-311/18, para: 63). در نتیجه، با توجه به مقدماتی که بیان شد، دادگاه عالی ایرلند از دیوان می‌خواهد که درباره اعتبار و تفسیر تصمیم کمیسیون اروپا مبنی بر راه‌اندازی سازوکار بندهای قراردادی استاندارد و سپر حریم خصوصی اروپا-آمریکا نظر بدهد (CJEU, CASE C-311/18, para: 1).

سرانجام، دیوان در رأی نهایی خود پس از ارائه تفاسیری درباره مواد ۴۶، ۵۸ و ۶۵ مقررات عمومی، تصمیم کمیسیون مبنی بر ارائه سطح حمایتی کافی توسط سپر حفاظتی حریم خصوصی را نامعتبر اعلام کرد؛ ولی درباره سازوکار بندهای قراردادی استاندارد چنین گفت که هیچ مدرکی دال بر عدم اعتبار این قراردادها نیافته و با توجه به اینکه ساختار این رژیم همچنان جای پیشرفت و بهبود دارد، به نظر دیوان، کماکان قادر به ادامه فعالیت در زمینه انتقال داده‌ها به کشورهای ثالث است (CJEU, CASE C-311/18, para: 203).

به این ترتیب، دومین سازوکار رسمی انتقال داده‌های شخصی از اروپا به ایالات متحده نیز با شکایت آقای شرمس و به دستور دیوان، از درجه اعتبار ساقط شد. اما نکته مهم در نمونه‌هایی که تا اینجا بیان شد، اولاً نقش بی‌بدیل دیوان دادگستری اتحادیه اروپا در قاعده‌سازی و نظارت بر اجرای درست مقررات جاری اروپا، و ثانیاً قدرت بالایی است که این نهاد برای مقام‌های ناظر حفاظت از داده کشورهای عضو در نظر گرفته است؛ برای مثال، آنجا که در اظهارنظرهای خود، با اینکه براساس تصمیمات رسمی کمیسیون اروپا، سازوکارهای ویژه‌ای برای انتقال داده‌های شخصی در نظر گرفته شده یا این نهاد، کشورهای ثالثی مانند ایالات متحده را دارای سطح حمایتی کافی در زمینه حفاظت از داده‌های شخصی قلمداد کرده‌اند، به کمیسرها حفاظت از داده، این ابتکار عمل را می‌دهد که فارغ از این ملاحظات، به بررسی و نظارت جداگانه بر روند و فرایند انتقال و همچنین، سطح حفاظت موجود در کشورهای ثالث پردازد و در صورت وجود نقص در این روندها، به صورت یک‌طرفه از انتقال داده‌های شخصی شهروندان اتحادیه جلوگیری

۱. ماده ۲ مقررات عمومی حفاظت از داده GDPR، درباره قلمرو اعمال این مقررات عمومی.

۲. ماده ۴۶ مقررات عمومی حفاظت از داده GDPR، درباره انتقال داده‌ها تحت حفاظت‌های مناسب.

۳. ماده ۵۸ مقررات عمومی حفاظت از داده GDPR، درباره اختیارات (قدرت اجرایی) نهادهای نظارتی مستقل (کمیسرها) حفاظت از داده.

۴. سپر حریم خصوصی اروپا-آمریکا (Privacy Shield)

کند. به عنوان مثالی دیگر در این باره نیز می توان به نظر نهایی دیوان در ماجرای پرونده شرمس ۲ اشاره کرد (CJEU, CASE C-311/18, para: 203(3)).

۵. اعمال مقررات عمومی مربوط به انتقال داده‌ها به شرکت‌های خصوصی و دولت‌های غیر عضو
در باره انتقال داده‌های شخصی کاربران اروپایی به شرکت‌های خصوصی که در خارج از مرزهای اتحادیه فعالیت داشته و مشغول به پردازش داده‌های شخصی هستند (مانند شرکت‌های آمریکایی)، به جز روش‌های نظارتی کمیسیون و قراردادهای دوجانبه‌ای که در ادامه به آن‌ها اشاره خواهد شد، مقام ملی ناظر حفاظت از داده یا کمیته حفاظت از داده اروپا نیز اهمیت بسیار زیادی در احقاق حقوق اشخاص موضوع داده دارند که در ادامه توضیح مختصری در این باره ارائه شده است.

به لحاظ منطقی، تنها وجود دسته‌ای از قوانین در زمینه حفاظت از داده، بدون نظارت بر حسن اجرای این مقررات، کمک چندانی به انجام این امر نخواهد کرد؛ بنابراین، یکی دیگر از ستون‌های اصلی نظام جدید حفاظت از داده اروپا، همین اعمال نظارت توسط ناظران حفاظت از داده است که خود، بخشی از نظام دولت مستقر در کشورهای عضو هستند (Regulation (EU) 2016/679, Chapter VI, article: 51(1)).

همان گونه که پیشتر نیز اشاره شد، این ناظران در انجام وظایف خود از استقلال کامل برخوردارند (Ibid, article: 52) و آزادی عمل نسبتاً بالایی نیز دارند. مقررات عمومی برای تضمین جایگاه و عملکرد مقام نظارتی، از یک سو، نهادهای انتخاب‌کننده آن را مجلس، دولت، رئیس دولت یا یک دستگاه مستقل فعال در زمینه حفاظت از داده با توان استخدام زیر نظر قانون کشور عضو می‌داند (Ibid, article: 53) و از سوی دیگر، وظایفی مانند نظارت بر اجرای مفاد این سند، افزایش آگاهی‌های عمومی درباره حفاظت از داده و قواعد مربوط به پردازش، توصیه به قوه مقننه کشورها برای قاعده‌سازی‌های جدید و به روز، بررسی دعوی‌های ارائه شده توسط اشخاص حقیقی یا حقوقی، انجام تحقیقات درباره اجرای مفاد این سند توسط پردازشگران یا سازوکارهای انتقال داده و دسترسی به کل محدوده کاری پردازشگر از قبیل تجهیزات و ابزار پردازش داده را به عهده این مقام می‌گذارد (Ibid, article: 57). افزون بر این، مقام ناظر، اختیار توییح و جریمه پردازشگران (همان گونه که پیشتر نیز به مواردی در این باره اشاره شد)، و دستور به آن‌ها برای اعمال حقوق اختصاصی شخص موضوع داده را نیز دارد (Ibid, article: 58).

با توجه به وظایف، کارکردها، و اختیارات مقام ناظر، بی تردید به کارگیری چنین نهادی، تأثیرات مثبتی بر

۱. رجوع شود به پرونده شرمس ۲.



حفاظت از داده‌های شخصی کاربران خواهد داشت و از یک سو، دسترسی اشخاص به نهاد تخصصی شده در زمینه حفاظت از داده‌ها برای طرح شکایت و پیگیری‌های مربوطه تسهیل شده و از سوی دیگر، از پیگیری‌های اضافی و بی‌سرانجام قضایی در زمان نشت اطلاعات شخصی جلوگیری شده و حتی در صورت بالا بودن اهمیت مسئله، خود این نهاد قادر به انجام پیگیری‌های لازم از طریق سازوکارهای قضایی و اداری اتحادیه خواهد بود.

افزون بر این، شرح محتویات این سند، درباره انتقال داده‌های شخصی به کشورهای غیر عضو اتحادیه مانند ایالات متحده آمریکا چنین بیان می‌کند که گردش آزاد اطلاعات و جریان داده‌های شخصی به و از کشورهای خارج از اتحادیه و سازمان‌های بین‌المللی برای گسترش تجارت و همکاری‌های بین‌المللی، ضروری است؛ ولی افزایش این جریان‌ها، چالش‌ها و نگرانی‌های جدیدی را در زمینه حفاظت از داده‌های شخصی ایجاد کرده است. با این حال، هنگامی که داده‌های شخصی از اتحادیه به کنترل کنندگان پردازشگران، یا گیرندگان دیگر در کشورهای ثالث یا سازمان‌های بین‌المللی منتقل می‌شود، سطح حمایت از اشخاص حقیقی که در سند مقررات عمومی در اتحادیه تضمین شده است، نباید تضعیف شود. در مورد نقل و انتقالات بعدی داده‌های شخصی از کشور ثالث یا سازمان بین‌المللی به پردازشگران همان کشور ثالث یا سازمان بین‌المللی دیگر نیز همین رویه برقرار است (<https://gdpr-info.eu/recitals/no-101>).

با توجه به موارد یادشده می‌توان چنین برداشت کرد که به‌طور کلی، نقل و انتقالات به کشورهای ثالث و سازمان‌های بین‌المللی، تنها با رعایت کامل مفاد این سند انجام می‌شود و یک انتقال، تنها در صورتی می‌تواند انجام شود که ضمن رعایت مفاد این مقررات عمومی (درباره نحوه انتقال امن داده‌های شخصی)، سایر شرایط مندرج در این سند که مربوط به کنترل یا پردازش داده‌های شخصی است (در مورد پردازش‌های قانونی و مجاز داده‌های شخصی) نیز رعایت شود، و تنها در صورت اجرای مفاد سند مقررات عمومی در هر دو مرحله انتقال و پردازش داده‌ها در کشور ثالث، اجازه این انتقال داده شده است.

این مقررات، آسیبی به موافقت‌نامه‌های بین‌المللی منعقدشده بین اتحادیه و کشورهای ثالث در راستای تنظیم شرایط و ضوابط انتقال داده‌های شخصی (از جمله تدابیر مناسب برای اشخاص موضوع داده) نخواهد زد؛ بنابراین، کشورهای عضو می‌توانند موافقت‌نامه‌های بین‌المللی‌ای منعقد کنند که شامل انتقال داده‌های شخصی به کشورهای ثالث یا سازمان‌های بین‌المللی می‌شود. البته تاجایی که توافق‌نامه‌های یادشده بر مقررات عمومی یا سایر مفاد قانون اتحادیه تأثیری نداشته باشند و سطح مناسبی از حمایت را در زمینه حقوق اساسی اشخاص موضوع داده دربر گیرند (<https://gdpr-info.eu/recitals/no-102>).

کمیسیون اروپا ممکن است برای کل اتحادیه تصمیم بگیرد که یک کشور ثالث، یک قلمرو یا بخش مشخص در یک کشور ثالث، یا یک سازمان بین‌المللی، سطح مناسبی از حفاظت از داده‌ها را ارائه می‌دهد؛ بنابراین، در سرتاسر اتحادیه، اطمینان حقوقی یکسانی در مورد آن کشور ثالث یا سازمان بین‌المللی در نظر گرفته شده است و در چنین مواردی، انتقال داده‌های شخصی به آن کشور ثالث یا سازمان بین‌المللی می‌تواند بدون نیاز به کسب مجوز بیشتر انجام شود. همچنین، کمیسیون می‌تواند با دادن اخطار و بیانیه‌ی کاملی که دلایل قانونی را به کشور ثالث یا سازمان بین‌المللی اطلاع می‌دهد، چنین تصمیمی را لغو کند (<https://gdpr-info.eu/recitals/no-103>).

وظیفه‌ی نظارت بر حسن اجرای حفاظت‌های مورد تأیید اتحادیه اروپا نیز براساس بند ششم ماده‌ی ۲۵ سند مقررات عمومی و نیز بند چهارم ماده‌ی ۲۶ راهنمای حفاظت از داده، به عهده‌ی کمیسیون بوده و این نهاد می‌بایست برای کسب اطمینان از رعایت مقررات یادشده، بررسی‌های دوره‌ای را با در نظر گرفتن نظرات پارلمان و شورای اروپا و همچنین، نهادهای اروپایی دیگری مانند دیوان، در دستور کار خود قرار دهد (<https://gdpr-info.eu/recitals/no-106>).

به‌عنوان مثال و همان‌گونه که پیشتر نیز اشاره شد، در مورد شرکت‌های خصوصی ایالات متحده آمریکا مانند فیس‌بوک، کمیسیون، ابتدا با تصمیمی سطح حمایت از داده‌های شخصی در این کشور را کافی دانست و انتقال داده را از اروپا به این کشور در چارچوب سازوکارهای بندرگاه ایمن و سپر حریم خصوصی اروپا، مجاز اعلام کرد؛ اما پس از پیگیری‌های قضایی آقای شرمس و با توجه به شواهد و مدارک موجود در پرونده‌ها مبنی بر عدم رعایت مفاد سند مقررات عمومی، این تصمیم‌های کمیسیون با رأی دیوان اروپا از درجه‌ی اعتبار ساقط شدند. به‌عنوان نمونه‌ی دیگری در مورد نهادهای دولتی آمریکا، می‌توان به پرونده‌ی انتقال داده‌های سوابق نام مسافران اروپایی به این کشور اشاره کرد که دیوان، این روند انتقال را نیز نامناسب و غیرقانونی به‌شمار آورده و متوقف کرد.

افزون‌براین، از آنجاکه تصمیم‌های کمیسیون پس از بررسی‌های تخصصی انجام‌شده توسط نمایندگان این نهاد و همچنین، برپایه‌ی قراردادهای دوجانبه با کشور ثالث (برای مثال، ایالات متحده) اتخاذ می‌شود، در عمل، برای کشور ثالث نیز در حکم قانون بوده و لازم‌الاتباع است؛ بنابراین، پس از انعقاد موافقت‌نامه‌هایی که کمیسیون با کشورهای ثالث یا سازمان‌های بین‌المللی خارج از اتحادیه به تصویب می‌رساند، تمام نهادها یا بخش‌های گوناگون کشور ثالث که در توافق به آن اشاره شده است، ملزم به رعایت مفاد سند مقررات عمومی بوده و در نتیجه، برای مقصد واقع شدن در عملیات انتقال داده‌های



۳۴۳

اعمال فراسرزمینی قانون
اروپایی حفاظت از
داده‌های شخصی در
آمریکا

شخصی، مجاز هستند.

۶. ویژگی فراسرزمینی مقررات عمومی در حفاظت از داده‌های اتباع اروپایی

بی‌شک یکی از مهم‌ترین ویژگی‌های سند مقررات عمومی، فرامرزی (یا فراسرزمینی) بودن آن در حوزه اعمال یا قلمرو است؛ زیرا، برخلاف (درعمل) بسیاری از مقرراتی که در اتحادیه وضع می‌شود، با اتکا به قدرت اقتصادی، بازار داده، جمعیت زیاد کاربران متصل به شبکه اینترنت و زیرساخت‌های فناوری موجود در اروپا، این سازمان بین‌المللی قادر به تسری دادن قلمرو قوانین خود به کشورهای غیرعضو دیگر نیز بوده است که در حال حاضر و در نوع خود یک فعالیت تقنینی کم‌نظیر است؛ آنجا که ماده «۳» تصریح می‌کند که این سند بر همه پردازش‌های داده‌های شخصی که از طریق تأسیس یا انتصاب کنترلگر یا پردازشگری که درون اتحادیه فعالیت می‌کند، اعمال شده یا بر همه کسب و کارهایی که درون اتحادیه انجام می‌شوند یا به کشورهای عضو، کالا یا خدمات ارائه می‌دهند، ناظر خواهد بود (Montalbano, 2020, 3).

در دنیای امروز و در بحث قانون‌گذاری و ضمانت اجرای آن قوانین، صلاحیت تجویزی و صلاحیت اجرایی از یکدیگر متمایز خواهند بود؛ به گونه‌ای که در مورد میزان قدرت یک دولت به لحاظ اجرای قوانین، شفافیت خاصی ایجاد می‌کند. دولت‌ها در قالب حقوق بین‌الملل، در حوزه قضایی خود قوانینی را تجویز می‌کنند که امور خارج از حوزه قلمرو آنان را تنظیم می‌کند (با فرض اینکه به اتحادیه اروپا نیز به شکل یک مجموعه واحد تابع حقوق بین‌الملل بنگریم)؛ با این حال، قوانین بین‌المللی در مسیر اجرای چنین مقرراتی در قلمرو کشورهای دیگر، بدون رضایت کشور یادشده، محدودیت‌هایی ایجاد کرده است (Pramesti and Afriansyah, 2019, 83).

لیکن شاید همین قدرت اقتصادی عظیم اتحادیه سبب شده است که در حوزه حفاظت از داده‌های اتباع خود، حتی در ورای سرزمین‌های کشورهای عضو نیز اعمال نفوذ کرده و با قواعد و مقرراتی که به تصویب رسانده است، امور شهروندان اروپایی را در این حوزه تنظیم کرده و آن‌ها را نه تنها در داخل مرزهای اتحادیه و در حالتی که در مرحله پردازش یا انتقال داده‌های خود ارتباط مستقیمی با اتحادیه دارند، بلکه در مواردی که شخص حتی در داخل اتحادیه نیز حضور ندارد، تحت پوشش خود درآورد.

با توجه به موارد یادشده و متن اصلی ماده «۳» این سند، توجه به چند نکته، ضروری به نظر می‌رسد: نخست اینکه، اصطلاح «تأسیس یا انتصاب پردازشگر» در نگاه نخست، لفظی مبهم به نظر می‌رسد، اما با توجه به قسمت «۲۲» شرح محتویات این سند، «تأسیس، مستلزم اعمال مؤثر و واقعی فعالیت از طریق ترتیبات پایدار است» (<https://gdpr-info.eu/recitals/no-22>)؛ بنابراین، برای مشخص کردن اینکه آیا فعالیت یک



۳۴۴

پژوهش‌نامه ایرانی
سیاست بین‌الملل،
سال ۱۲، شماره ۱، شماره
پیاپی ۲۳، پاییز و زمستان
۱۴۰۲

شرکت خارجی درون اتحادیه می‌بایست در چارچوب قواعد مندرج در مقررات عمومی انجام شود یا خیر، در وهله نخست باید مشخص شود که «فعالیت مؤثر و واقعی از طریق ترتیبات پایدار» وجود دارد (Korff, 2019, 6).

بنابراین، یک شعبه یا شرکت تابعه یا شرکت دختر می‌تواند کاملاً تحت مالکیت یک «مؤسسه» باشد. دیوان دادگستری اروپا تمایل دارد که دیدگاهی گسترده از این مفهوم داشته باشد. در پرونده ماریو گونزالز علیه گوگل اسپانیا، این واقعیت که گوگل، فضای تبلیغاتی را در موتور جست‌وجوی خود از طریق زیرمجموعه اسپانیایی خود ارائه می‌دهد، کافی است که آن را «تأسیس یا انتصاب» در اسپانیا در نظر بگیریم؛ حتی اگر نتایج جست‌وجوی آن از ایالات متحده آمریکا ارائه شده باشد.

دوم اینکه، بند نخست ماده «۳» آشکارا تصریح می‌کند که در عمل، فرقی نمی‌کند که پردازش (یا قسمتی از عملیات پردازشی) در اتحادیه اروپا انجام شود یا خیر. متن مقررات عمومی تصریح می‌کند که این مقررات بر فعالیت‌های پردازشی یک مؤسسه در اتحادیه اروپا «صرف‌نظر از اینکه پردازش در داخل اتحادیه انجام می‌شود یا خیر» اعمال می‌شود. در نتیجه، وجود یک کنترل‌کننده یا پردازشگر داده در اتحادیه اروپا از طریق یک ساختار کلی‌تر و مشخص (چه در خارج اتحادیه و چه در داخل آن)، و این امر که پردازش‌های انجام‌شده در زمینه فعالیت‌های این مؤسسه انجام می‌شود، سبب اعمال مقررات عمومی برای فعالیت‌های پردازشی آن مؤسسه خواهد شد؛ بنابراین، محل انجام عملیات پردازش، بر تعیین اینکه آیا پردازش انجام‌شده در محدوده مفاد این سند قرار می‌گیرد یا خیر، چندان مؤثر نیست.

سوم اینکه، مفاد این سند همواره بر دو دسته از افراد، قابل اعمال است؛ دسته نخست، شهروندان اروپایی چه در داخل مرزهای اروپا چه در خارج از آن؛ اما دسته دوم، شهروندان غیراروپایی که در داخل اروپا حضور دارند یا اطلاعات مربوط به آن‌ها توسط مؤسسه‌های اروپایی کنترل و پردازش می‌شود. کمیته حفاظت از داده اروپا از این شیوه حمایتی با عنوان «معیار هدف‌گذاری» یاد کرده (EDPB Opinion 3/2018,

د CJEU, JUDGMENT OF THE COURT (Grand Chamber), JUDGMENT OF 13. 5. 2014 — CASE C-131/12 GOOGLE SPAIN AND GOOGLE, (Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González),

- همچنین در دسترس در نشانی زیر:

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131>

(آخرین دسترسی: بهمن ۱۴۰۰)





(footnote: 3), 12–13) و این‌گونه توضیح می‌دهد که از متن بند دوم ماده «۳» این سند و لفظ «افرادی» که درون اتحادیه حضور دارند» می‌توان نتیجه گرفت که اعمال معیارهای هدف‌گیری، به تابعیت، اقامت، یا انواع دیگر وضعیت حقوقی اشخاص موضوع داده که داده‌های شخصی آن‌ها در حال پردازش است، محدود نمی‌شود. بخش «۱۴» شرح محتویات این سند نیز، این تفسیر را تأیید و بیان می‌کند: «حفاظت ارائه‌شده توسط این مقررات باید در مورد اشخاص حقیقی، صرف‌نظر از ملیت یا محل سکونت، در مورد پردازش داده‌های شخصی آن‌ها اعمال شود (<https://gdpr-info.eu/recitals/no-14/>)».

چهارم اینکه، به‌نظر می‌رسد، از آنجا که هدف کلی این سند، همان‌گونه که پیشتر نیز اشاره شد، حمایت از حریم خصوصی افراد است و این مقوله، خود یکی از مسائل مطرح حقوق‌بشری فعلی جهان به‌شمار می‌آید و به‌عبارت دیگر، با توجه به هدف حقوق‌بشری‌ای که این سند دنبال می‌کند، اعمال فرامرزی آن در کشورهای غیرعضو اتحادیه اروپا به‌نوعی تسهیل شده و با ممانعت چندانی روبه‌رو نشده است. همان‌گونه که مشاهده کردیم، در پرونده‌های شرمس «۱» و «۲» نیز کشور ایالات متحده به لغو سازوکارهای بندرگاه ایمن و سپر حریم خصوصی رضایت داده و در پی راهکار جدیدی برای ازسرگیری روند انتقال داده‌های شخصی افراد در عین توجه به حقوق اساسی آنان است.

نتیجه‌گیری

امروزه رشد روزافزون فناوری و تسهیل استفاده کاربران سراسر جهان از خدمات اینترنتی، حجم داده‌ها و اطلاعات در گردش را در فضای سایبر افزایش داده است. ازیک‌سو، با توجه به تهدیدهای موجود در این فضا و در برابر محرمانگی و حفاظت از داده‌های شخصی کاربران، حمایت هرچه بیشتر از این داده‌ها توسط حکومت‌های مرکزی کشورها و نهادهای بین‌المللی و منطقه‌ای، امری ضروری به‌شمار می‌آید. اتحادیه اروپا نیز به‌عنوان یک ساختار سیاسی منطقه‌ای با قابلیت تدوین قوانین در حوزه قلمرو کشورهای عضو خود، ضمن در نظر گرفتن اهمیت حمایت از حریم خصوصی افراد و حفاظت از داده‌های شخصی آنان در فضای سایبر، با تصویب راهنمای حفاظت از داده (۱۹۹۵) و مقررات عمومی حفاظت از داده‌های شخصی در زمینه پردازش و انتقال داده‌های شخصی (۲۰۱۶)، برخی فعالیت‌های تقنینی را در این زمینه انجام داده است.

۱. GDPR، بند ۲، ماده ۳. «این مقررات عمومی بر پردازش داده‌های شخصی، افراد موضوع داده‌ای که در اتحادیه اروپا حضور دارند اعمال می‌شود...».

به گونه‌ای که سند نخست، در قالب یک راهنما برای قانون‌گذاری در کشورهای عضو و در زمینه حفاظت از داده‌های شخصی معرفی شد و سند دوم، با پیشرفتی که در همه زمینه‌ها، به ویژه مبحث ضمانت اجرای آن (حتی در برابر کشورهای غیرعضو اتحادیه) نشان داد، نه تنها در کل قلمرو سرزمینی اتحادیه اروپا، بلکه در همه ساختارها و نهادهای عمومی و خصوصی‌ای که قصد مبادله اطلاعات با اتحادیه اروپا را داشته یا به پردازش داده‌های اتباع اروپایی می‌پردازند، تبدیل به مقررات عمومی جامع و فراگیر شد؛ به گونه‌ای که همه کشورهای اروپایی ملزم به ایجاد هماهنگی کامل با مفاد این سند در نظام حقوقی داخلی خود در راستای حفاظت از داده‌های شخصی شدند و حتی برخی از کشورهای اتحادیه، متن همین سند را به عنوان قواعد حفاظت از داده خود به تصویب رساندند؛ بنابراین، مشخص شد که در حال حاضر، روابط دولت‌های اتحادیه اروپا با کشورهای ثالث یا غیرعضو در راستای پردازش یا انتقال داده‌های شخصی، در سند مقررات عمومی و نهادهای اجرایی مرتبط با آن تنظیم می‌شود.

ایالات متحده آمریکا نیز به عنوان یک کشور غیرعضو و همچنین، کشوری که بیشترین و بزرگ‌ترین شرکت‌های خدمات‌دهنده اینترنتی کنونی دنیا را در اختیار دارد، مورد مطالعه این پژوهش قرار گرفته است که با تحلیل و بررسی سه مورد از مهم‌ترین رأی‌های دیوان دادگستری اتحادیه اروپا درباره روندهای انتقال داده‌های شخصی از اروپا به آمریکا، مانند رأی‌هایی درباره داده‌های سوابق نام مسافران، سازوکارهای انتقال داده بندرگاه ایمن، و سپر حریم خصوصی اروپا-آمریکا، مشخص شد که براساس نظر دیوان که مبتنی بر مفاد اسناد حفاظت از داده اروپایی یادشده نیز هست، افزون بر اینکه کشورهای خارج از اتحادیه، ملزم به رعایت قواعد مصوب اتحادیه در این زمینه (در داخل قلمرو سرزمینی خود به عنوان کشور ثالث) هستند، حتی اگر به صورت جداگانه، قراردادهای دوجانبه‌ای نیز در راستای انتقال داده‌های شخصی بین نهادهای ملی یا اروپایی و کشورهای غیرعضو منعقد شود، باز هم در صورت احراز تخطی کشور ثالث از قواعد سند مقررات عمومی حفاظت از داده توسط نهادهای نظارتی و قضایی اروپا، عملیات انتقال داده به منظور حفاظت از کاربران اروپایی، به صورت یک طرفه متوقف خواهد شد.

افزون بر این، به نظر می‌رسد که با توجه به (۱) دایره گسترده‌ای که متن مقررات عمومی برای نهادهای خصوصی و دولتی که با داده‌های شخصی کاربران اروپایی سروکار دارند، در نظر گرفته است؛ (۲) تعداد قابل توجه کاربران متصل به شبکه جهانی اینترنت و استفاده کنندگان از خدمات سرویس‌دهندگان فضای سایبر در داخل قلمرو کشورهای عضو اتحادیه اروپا؛ (۳) تفاسیر موسعی که دیوان دادگستری اتحادیه اروپا از پردازشگران و خدمات‌دهندگان ارائه داده است و همچنین، جریمه‌های سنگینی که در صورت تخلف



شرکت‌ها بر دوش آن‌ها بار می‌کند (که افزون‌بر اینکه به این امر در متن سند مقررات عمومی اشاره شده است، رویه قضایی دیوان اروپا و همچنین، تمکین شرکت‌های خاطی در طول زمان نیز بر کاربرد آن تأکید دارد)؛ و ۴) قدرت اقتصادی و سیاسی قابل توجه اتحادیه اروپا در فضای بین‌المللی فعلی جهان، این سازمان بین‌المللی به گونه‌ای کاملاً آشکار و با موفقیت، قادر به تسری دادن قلمرو اعمال قوانین خود در زمینه حفاظت از داده‌های شخصی، به محدوده و سرزمین کشورهای غیرعضو اتحادیه، مانند ایالات متحده آمریکا، بوده است؛ بنابراین، می‌توان نتیجه گرفت که در مرحله عمل، مقررات عمومی، دارای ویژگی فراسرزمینی است و عمل به مفاد آن برای همه شرکت‌های خصوصی یا نهادهای دولتی که متمایل به تبادل داده با اعضای اتحادیه اروپا هستند، الزامی است و ایالات متحده نیز از این قاعده مستثنا نیست.

References

- Akbari Tabar, A & Eskandarpour, E, (2013). *Social Media and Virtual Social Networks*. Tehran: National Culture Network Publications. [in Persian].
- Analytical Report of Maher Specialized Center, on GDPR and its Role in Protecting the Privacy of Social Network Users* (2018). [in Persian].
- Ansari, B (2007). *Mass Communication Law*. Tehran: Printing and Publishing Organization of the Ministry of Culture and Islamic Guidance. first edition [in Persian].
- Article 29 Data Protection Working Party. Opinion 03/2013 on purpose limitation, Adopted on 2 April 2013.
- Article 29 Data Protection Working Party, Working Party Guidelines on consent under Regulation 2016/679, Adopted on 28 November 2017, last Revised and Adopted on 10 April 2018.
- Article 29 Data Protection Working Party. *Working Party Guidelines on consent under Regulation 2016/679*.
- Aslani, H, (2010). *Information Technology Law*. Tehran: Mizan Publications. Second Edition.
- Cjeu, Judgment of the Court (Grand Chamber). Judgment of 13. 5. 2014 — Case C-131/12 Google Spain and Google, (Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González).
- Cjeu, Judgment of The Court (Grand Chamber), Judgment of 16. 7. 2020 — Case C-311/18 Facebook Ireland And Schrems, (Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems).
- CJEU, JUDGMENT OF THE COURT (Grand Chamber), JUDGMENT OF 30. 5. 2006 — JOINED CASES C-317/04 AND C-318/04, (European Parliament, European Data Protection Supervisor (EDPS) v Council of the European Union, Commission of the European Communities).
- Cjeu, Judgment of the Court (Grand Chamber), Judgment of 6. 10. 2015 — CASE C-362/14, (Maximillian Schrems v Data Protection Commissioner).
- Commission Decision 2000/520/EC, of July 26, 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protect Provided by the Safe Harbor Privacy Principles and Related Frequently Asked Questions Issued by the U.S.



- Department of Commerce, 2000.
- Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the protection provided by the EU-US Privacy Shield.
- Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, (Convention 108).
- Council of Europe, European Convention on Human Rights (1976).
- Dalla Corte, L, (2019). Scoping Personal Data: Towards a Nuanced Interpretation of the Material Scope of EU Data Protection Law. *European Journal of Law and Technology*, 10(1).
- Data Protection (Legal Protection of Privacy of Persons in Cyberspace) (2002). *Secretariat of the Supreme Informatics Council of Islamic Republic of Iran* [in Persian].
- DeCew, J (1997), In Pursuit of Privacy: Law, Ethics, and Rise of Technology. *Cornell University Press*. London.
- Decision (EU) 2016/2297 of 16 December 2016 on Standard Contractual Clauses (SCC).
- Deibert, R, Palfrey, J, Rohozinski, R & Zittrain, J, (2010). *Access Controlled: The Shaping of Power, Rights and Rule in Cyberspace*. United States of America: The MIT Press.
- Directive 2002/58/Ec of the European Parliament and of the Council of 12 July 2002/ Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications).
- Directive 2006/24/Ec of The European Parliament and of the Council of 15 March 2006.
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.
- Douglas-Scott, S. (1993). Reviewed Work: Privacy, Intimacy and Isolation. by Julie Inness. Oxford University Press. *on behalf of the Mind Association*. 102(408).
- EDPB, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679.
- EDPB, Guidelines 4/2019 on Article 25, Data Protection by Design and by Default, Version 2.0, Adopted on 20 October 2020.
- El Khoury, A, (2015). The Safe Harbor is not a Legitimate Tool Anymore. What Lies in the Future of EU-USA Data Transfers. Review of Case C-362/14 Maximillian Schrems v Data Protection Commissioner. *EJRR*.
- European Convention on Human Rights (ECHR).
- Explanatory Report to Convention 108.
- Foreign Intelligence Surveillance Act (FISA).
- Ghadmagahi, M, A, (2021). *The Right to the Protection of Personal Information in Cyberspace, with Emphasis on EU Data Protection Guidelines (GDPR: 2018)*. Master Thesis. International Law. Faculty of Law. College of Farabi. University of Tehran. [in Persian].
- Greer, D. (2011). Safe Harbor a Framework that Works. *International Data Privacy Law*, Oxford University Press. 1(3).
- High Court of Ireland Decisions (Schrems-v-Data Protection Commissioner Judgment)/ [2014] IEHC 310.
- <http://www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm>.
- <https://cdt.org/wp-content/uploads/2017/02/Section-702.pdf>.
- <https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&>

[doclang=en&mode=lst&dir=&occ=first&part=1&cid=9791227.](https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en)
[https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.](https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en)
[https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131.](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131)
[https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046.](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046)
[https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=ecli%3AECLI%3AEU%3AC%3A2006%3A346.](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=ecli%3AECLI%3AEU%3AC%3A2006%3A346)
[https://gdpr-info.eu/recitals/no-101/.](https://gdpr-info.eu/recitals/no-101/)
[https://gdpr-info.eu/recitals/no-102/.](https://gdpr-info.eu/recitals/no-102/)
[https://gdpr-info.eu/recitals/no-103/.](https://gdpr-info.eu/recitals/no-103/)
[https://gdpr-info.eu/recitals/no-106/.](https://gdpr-info.eu/recitals/no-106/)
[https://gdpr-info.eu/recitals/no-14/.](https://gdpr-info.eu/recitals/no-14/)
[https://gdpr-info.eu/recitals/no-22/.](https://gdpr-info.eu/recitals/no-22/)
[https://noyb.eu/en.](https://noyb.eu/en)
[https://www.bailii.org/ie/cases/IEHC/2014/H310.html.](https://www.bailii.org/ie/cases/IEHC/2014/H310.html)
[https://www.coe.int/en/web/data-protection/convention108-and-protocol.](https://www.coe.int/en/web/data-protection/convention108-and-protocol)
[https://www.dni.gov/files/icotr/Section702-Basics-Infographic.pdf;](https://www.dni.gov/files/icotr/Section702-Basics-Infographic.pdf)
[https://www.govinfo.gov/content/pkg/BILLS-110hr6304pcs/html/BILLS-110hr6304pcs.htm.](https://www.govinfo.gov/content/pkg/BILLS-110hr6304pcs/html/BILLS-110hr6304pcs.htm)
[https://www.privacyshield.gov/Program-Overview.](https://www.privacyshield.gov/Program-Overview)
[https://www.statista.com/statistics/267808/net-income-of-microsoft-since-2002/.](https://www.statista.com/statistics/267808/net-income-of-microsoft-since-2002/)
 Hustinx, P, (2017). *EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*. Oxford Scholarship Online.
 Jannick, S & Kosta, S. (2019). *Before and After GDPR*. The Changes in Third Party Presence at Public and Private European Websites.
 Jia, J, Ginger Zhe, J & Wagman, L. (2019). *The Short-Run Effects of GDPR on Technology*. Venture Investment.
 Kadkhodai, Abbas (2004). *Structure and Law of the European Union*. Tehran: Mizan Publications. [in Persian].
 Khalaf Rezaei, H. (1398). The Legal System of the European Union and the National Sovereignty of the Member States (with Emphasis on the Rulings of the German Constitutional Court). *Bi-Quarterly Journal of Comparative Law*, 6(2), [in Persian].
 LG Feldkirch-57 Cg 30/19b – 15.
 Libert, T, Graves, L & Nielsen, R, K. (2018). *Changes in Third-Party Content on European*. News Websites after GDPR.
 Mahboob, A & Mehdi, N, (2020). Legal Frameworks for Security of Private Data Processing (A Comparative Study of Iranian and European Union Law). *Journal of Islamic Law*, 17(66). [in Persian].
 McLean, R. (2001). *EU Law*. Translated by Majid Shokouhi. Tehran: Al-Huda International Publications.
 Montalbano, L. (2020). Jurisdiction and Applicable Law under the GDPR: A New Landscape. *The John Marshall Journal of Information Technology & Privacy Law*, Vol: 34.
 Musazadeh, R. & Tabatabai, S. (2020). A Comparative Study of Cybercrime Regulations from the Perspective of Iranian and European Union Law. *International Research Journal*, 2(1).



- Gruschka, N., Mavroeidis, V., Vishi, K & Jensen, M. (2018). Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR. *IEEE International Conference on Big Data (Big Data)*.
- Najafi Shoushtari, B. (2017). *The Role of Personal Data Protection Authorities with a Look at the 2016 EU Data Protection Regulations*. Master Thesis. Law. Faculty of Law and Political Science. Allameh Tabatabai University. [in Persian].
- Nouri, M. A. & Nakhjavani, R. (2004). *Data Protection Law*. Tehran. Ganj-e-Danesh Library Publications.
- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, (1980).
- Phillips, M. (2018). International Data-Sharing Norms: From the OECD to the General Data Protection Regulation (GDPR). *Human Genetics*. Vol.137.
- Pramesti, I & Afriansyah, A. (2019). Extraterritoriality of Data Protection: GDPR and Its Possible Enforcement in Indonesia, *Advances in Economics. Business and Management Research*, Vol 130, 3rd International Conference on Law and Governance, (ICLAVE 2019).
- Regulation (EU) 2016/679 Of the European Parliament and of the Council of 27 April 2016. On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data.
- Rengel, A. (2013). *Privacy in the 21st Century (Studies in Intercultural Human Rights, 5)*. Boston: Martinus Nijhoff Publishers.
- Safari, B. (2017). Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection. *Seton Hall Law Review*, 47(3), Article 6.
- Sean, S, Jason, R & Webb, H. (2018). Are We There Yet? Understanding the Challenges Faced in Complying with the General Data Protection Regulation (GDPR). *In Proceedings of the 2nd International Workshop on Multimedia Privacy and Security (MPS '18)*. Association for Computing Machinery, New York: NY, USA, 88–95.
- Sotoudeh, M & Atabati, N. (2020). A Comparative Study of Legal Regulations for Electronic Communications Control in Crime Detection (Some European Countries, USA and Iran). *Quarterly Journal of International Police Studies*, 11(42), [in Persian].
- Taghizad, M, Zomordi, K & Hajian, M. (2017). The Role of the European Union in Regulating Cybercrime. *Quarterly Journal of International Police Studies*, 7(29). [in Persian].
- U.S. Department of Commerce. Safe Harbor Privacy Principles and Related Frequently Asked Questions. July 21, 2000.
- United States Dept of Defense. Technology and Privacy Advisory Committee (TAPAC) (2004). Safeguarding Privacy in the Fight against Terrorism: Report of the Technology and Privacy Advisory Committee: Washington, D.C: DOD Technological Innovations in Crime Prevention and Policing: A Review of the Research on Implementation and Impact.
- User Data Protection: Global Approaches and Typology of Regulation, (2017), Research Center of the Islamic Consultative Assembly, Deputy of Infrastructure Research and Production Affairs, Office of Communication Studies and New Technologies. [in Persian].
- Weiss, M. A & Archick, K. (2016). *U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield*. Report. May 19, Washington D.C: University of North Texas Libraries.
- Martin, Y & Kung, A, (2018). Methods and Tools for GDPR Compliance Through Privacy and Data Protection Engineering.

Zandi, M. R. (2014). *Preliminary Research in Cybercrime*. Tehran: Mizan Publications. [in Persian].

Zarkalam, S. (2007). Privacy of Internet Communications (Study in Iranian and European Union Law). *Islamic Studies and Law*, 8(1). [in Persian].

Ziber, U. (2011). *Computer Crimes*. Tehran: Ganj-e-Danesh Publications. Second Edition.

