تاریخ دریافت: ۹۸/۰۴/۲۶
تاریخ پذیرش: ۹۹/۰۱/۱۸
نوع مقاله: فنی و ترویجی

بررسی موافقتنامهٔ انتقال فرامرزی داده‌های شخصی بین ایالات متحدهٔ آمریکا و اتحادیهٔ اروپا با نگاهی به قوانین جمهوری اسلامی ایران

نوشتهٔ
آمنه صرامی *

چکیده

در عصر کنونی موضوع حمایت از داده و مباحث حقوقی مربوط به آن، اهمیت بسیاری یافته است. موضوعی که در نظام‌های حقوقی مختلف و در زمینهٔ مسائل حقوقی داده با چالش‌های بیشتری روبه‌رو شده، مبحث انتقال فرامرزی داده است. در این نوشتار تلاش شده تا به این مسئله از مسیر بررسی توافقنامهٔ حامی حریم خصوصی (Privacy Shield) که میان اتحادیهٔ اروپا و ایالات متحدهٔ آمریکا منعقد شده، پرداخته شود. در همین راستا، ابتدا رویکرد آن‌ها نسبت به مبحث حمایت از داده، بررسی شده و سپس تحولات موجود در زمینهٔ انتقال فرامرزی داده در اتحادیهٔ اروپا و ایالات متحده آمریکا از توافقنامه بندرگاه امن (Safe Harbor) تا توافقنامه حامی حریم خصوصی و اصول حمایت از داده موجود در این دو سند موشکافی شده است؛ تا از این طریق بتوان به یک دیدگاه جامع و مانع در زمینهٔ انتقال فرامرزی داده در این دو نظام حقوقی مهم در سطح جهان و خلأهای مربوط به آن در نظام حقوقی جمهوری اسلامی ایران دست یافت.

کلیدواژه: داده، حمایت از داده، انتقال فرامرزی داده، توافقنامه بندرگاه امن، توافقنامه حامی حریم خصوصی.

* کارشناس ارشد حقوق ارتباطات دانشگاه علامه طباطبایی Sarami63@ gmail.com

مقدمه

امروزه در هر کشور، همگام با پیشرفت فناوری و با توجه به اوضاع و احوال نظام حقوقی آن کشور، قوانین و مقرراتی در حوزهٔ حمایت از داده به تصویب رسیده است. در برخی از کشورها حمایت از داده و حریم خصوصی افراد، مهم‌ترین چالش پیش‌رو است، در حالی‌که در کشورهای دیگر، موضوع تجارت و استفادهٔ تجاری از داده‌ها کلیدی‌ترین موضوع است. در نظام حقوقی کشورهای دستهٔ نخست، قوانین و مقررات به‌نسبت سختگیرانه‌ای، برای حمایت از داده‌های شخصی افراد وجود دارد و در نظام حقوقی دستهٔ دوم، شرکت‌ها و مؤسسه‌های تجاری از طریق خودنظام‌دهی اداره می‌شوند و بر مبحث حمایت از داده تأکید کمتری شده است. نمونهٔ بارز کشورهای دستهٔ نخست، کشورهای عضو اتحادیهٔ اروپا هستند، که با تصویب مقررات عمومی حمایت از داده (General Data Protection Regulation (GDPR)) در سال‌های ۱۹۹۸ و ۲۰۱۶ در این زمینه اهتمام ورزیده‌اند. ایالات متحده آمریکا نیز جزء دسته دوم کشورهاست که در آن خودنظام‌دهی و آزادی کسب و کار اهمیت بیشتری دارد.

در سطح بین‌الملل، همواره نیاز شدیدی به اتفاق نظر در رابطه با اصولی جهان‌شمول که بر مبنای آن بتوان به حمایت از حریم خصوصی افراد و داده‌های شخصی آنها پرداخت، احساس شده است. یکی از راهکارهایی که کشورهای مختلف برای برطرف ساختن این نیاز به آن روی آورده‌اند، تصویب توافقنامه‌ها و پیمان‌های بین‌المللی پایدار است (نورایی بیدخت، ۱۳۷۸). توافقنامه‌های بندرگاه امن و انتقال فرامرزی داده، مهم‌ترین توافقنامه‌های بین‌المللی است و با بررسی آن‌ها می‌توان به یک چارچوب کلی در این زمینه رسید.

در سال ۲۰۱۶، در نظام حقوقی اتحادیهٔ اروپا، با تصویب مقررات عمومی حمایت از داده چالش‌های جدی در زمینهٔ توافقنامه بندرگاه امن (The Safe Harbor Agreement) و انتقال فرامرزی داده میان ایالات متحدهٔ آمریکا و اتحادیهٔ اروپا مطرح شد. در نتیجه، با تصویب توافقنامهٔ حامی حریم خصوصی، این دو نظام حقوقی تلاش کردند چالش‌ها را حل کنند. در این نوشتار، با بررسی دو توافقنامهٔ مذکور و نیم‌نگاهی بر مقررات عمومی حمایت از دادهٔ اتحادیهٔ اروپا، موضوع انتقال فرامرزی داده میان این دو نظام حقوقی موشکافی شده است. در نهایت، قوانین و مقررات موجود در جمهوری اسلامی ایران نیز بررسی خواهد شد تا از این طریق، خلأهای موجود نظام حقوقی کشورمان در این زمینه مشخص شوند.

کلیات

در حال حاضر در ایالات متحده آمریکا، یک قانون جامع برای حمایت از داده در سطح فدرال وجود ندارد (calder, 2016) از نقطه نظر نظام حقوقی اتحادیهٔ اروپا، وجود چنین قانونی موجب ایجاد سطح حمایتی کافی برای داده‌های شخصی شهروندان اروپایی می‌شود. برای مثال، قانون حمایت از اطلاعات شخصی و اسناد

الکترونیکی (The Personal Information Protection and Electronic Documents Act (PIPEDA)) کشور کانادا، سطح حمایت کافی را از دیدگاه اروپاییان جهت نقل و انتقال فرامرزی داده با این کشور فراهم آورده است.

انتقال داده‌های شخصی توسط سازمان‌ها و شرکت‌های اروپایی، به کشورهایی که از نظر کمیسیون اروپا سطح حمایتی کافی ندارند، غیرقانونی تلقی شده و مجاز نیست. این موضوع مهم‌ترین چالش در زمینهٔ ارتباطات تجاری میان اتحادیهٔ اروپا و ایالات متحدهٔ آمریکا بود، که با تصویب توافقنامه بندرگاه امن در اواخر دههٔ ۱۹۹۰، دو طرف سعی کردند این چالش را حل کنند. به موجب این سند، سازمان‌ها و شرکت‌های آمریکایی می‌توانستند فعالیت خود را نزد وزارت بازرگانی ایالات متحدهٔ آمریکا ثبت کرده و اظهارنامه‌ای در رابطه با سیاست امنیت اطلاعات و حمایت از داده‌های شخصی خود منتشر کنند و از تعقیب قضایی در امان باشند.

در سال ۲۰۱۳، افشای غیرمجاز برنامه‌های نظارتی آژانس امنیت ملی آمریکا (Infoplease, 2020) و ادعاهای متعاقب مربوط به سایر فعالیت‌های اطلاعاتی ایالات متحدهٔ آمریکا در اروپا، به نگرانی‌های اروپاییان دربارهٔ مقررات حریم خصوصی و چالش حمایت از داده در این کشور دامن زد. درگیر شدن برخی شرکت‌های اینترنتی و ارتباطی در برنامه‌های آژانس امنیت ملی آمریکا، نگرانی‌های اروپاییان را نسبت به چگونگی استفاده از داده‌های شخصی در شرکت‌های آمریکایی و همچنین میزان دسترسی دولت ایالات متحده آمریکا به چنین داده‌هایی را تشدید کرد.

در ماه اکتبر سال ۲۰۱۵، دیوان دادگستری اروپا (The European Court of Justice (ECJ)) اعلام کرد که توافقنامه بندرگاه امن نامعتبر است و این توافقنامه ساز و کار معتبری برای انطباق با قوانین فعلی حمایت از داده در اتحادیهٔ اروپا نیست. در نتیجه، تلاش‌ها به منظور ایجاد جایگزینی برای این توافقنامه آغاز شد.

در ماه جولای سال ۲۰۱۵، اتحادیهٔ اروپا سندی را تحت عنوان توافقنامه حامی حریم خصوصی به تصویب رساند و در اول ماه آگوست سال ۲۰۱۶ آن را منتشر کرد. طبق نظر کمیسیون اتحادیهٔ اروپا، در این توافقنامه سطح حمایت کافی مورد نظر این کمیسیون تأمین شده که انطباق الزام‌های مندرج در مقررات عمومی حمایت از دادهٔ اروپا، برای انتقال فرامرزی داده است (Official Journal of the European Union, 2016). این الزام‌ها به اطلاعات شخصی مشتریان و کارکنان سازمان‌ها و شرکت‌های مختلف مربوط می‌شود که به‌وسیلهٔ این سازمان‌ها و شرکت‌ها جمع‌آوری شده است. به عبارت دیگر، سازمان‌ها و شرکت‌هایی که قصد پردازش یا ذخیرهٔ داده‌های منابع انسانی کارکنان اروپایی خود را دارند، باید مقررات عمومی حمایت از دادهٔ اتحادیه اروپا را رعایت کرده و به توافقنامه حامی حریم خصوصی ملحق شوند. (Calder, 2016)

امروزه ابزارهای مختلفی برای انتقال داده‌های شخصی از اتحادیهٔ اروپا به ایالات متحدهٔ آمریکا

وجود دارد؛ از جمله این ابزارها می‌توان به شروط قراردادی، قوانین الزام‌آور مشترک و توافقنامه حامی حریم خصوصی اشاره کرد. (European Commission, 2016)

رویکرد اتحادیهٔ اروپا

در مواد ۷ و ۸ منشور حقوق اساسی اتحادیهٔ اروپا، حریم خصوصی ارتباطات و حمایت از داده‌های شخصی، حقوق اساسی بشری معرفی شده‌اند و تمام کشورهای عضو اتحادیهٔ اروپا ملزم به اجرای آن هستند.

در دستورالعمل اتحادیهٔ اروپا، در زمینهٔ حمایت از داده‌ها ((Data Protection Directive (DPD) مصوب سال ۱۹۹۵، مقرر شده که انتقال داده‌های شخصی به کشوری خارج از اتحادیهٔ اروپا تنها در صورتی امکان‌پذیر است که در کشور مقصد سطح مناسبی از حمایت از داده‌های شخصی تأمین شود. مناسب بودن سطح حمایت، با توجه به اوضاع و احوال مربوط به انتقال داده از جمله ماهیت داده، هدف و مدت عملیات پردازش مورد نظر، کشور مبدأ و مقصد نهایی داده، قوانین، مقررات و اقدام‌های آن کشور در زمینهٔ امنیت داده ارزیابی می‌شود. (European Data protection supervisor, 2020)

در سال ۲۰۱۶، با تصویب مقررات عمومی حمایت از داده‌ها در اتحادیهٔ اروپا، به موضوع انتقال داده‌های شخصی به کشورهای ثالث یا سازمان‌های بین‌المللی نیز این اتحادیه توجه ویژه‌ای نشان داد و در مواد ٤٤ تا ٥٠ این مقررات به آن پرداخته شد. (Official Journal of the European Union, 2016)

در بند ۲ مادهٔ ٤٥ این مقررات شرایط مربوط به سطح حمایتی کافی کشور ثالث یا سازمان‌های بین‌المللی ذکر شده که عبارت‌اند از:

۱. وجود قانون یا مقررات عمومی یا بخشی در رابطه با حقوق بشر و آزادی‌های اساسی، شامل امنیت عمومی، دفاع، امنیت ملی و قوانین کیفری و دسترسی مقام‌های عمومی به داده‌های شخصی، تدابیر و اقدام‌های مربوط به اجرای آن، همچنین تدابیر و اقدام‌های در رابطه با انتقال داده‌ها به کشورهای ثالث یا سازمان‌های بین‌المللی مانند قوانین مؤثر و قابل اجرای مربوط به حقوق شخص موضوع داده و جبران خسارت‌های شخص موضوع داده که داده‌های او انتقال یافته است.

۲. وجود یک یا چند مقام نظارتی مستقل، در کشور ثالث یا سازمان بین‌المللی، با مسئولیت تضمین و اجرای قوانین حمایت از داده شامل اختیارات اجرایی کافی به منظور کمک و راهنمایی اشخاص موضوع داده در زمینهٔ اجرای حقوقشان و همچنین هماهنگی با مقام‌های نظارتی کشورهای عضو اتحادیه.

۳. عضویت کشور ثالث یا سازمان بین‌المللی در تعهدات بین‌المللی، منطقه‌ای و یا چندجانبه در زمینهٔ حمایت از داده‌های شخصی.

همچنین، در بند ۸ این ماده مقرر شده که کمیسیون اتحادیهٔ اروپا باید پس از ارزیابی، فهرستی از کشورها یا سازمان‌های بین‌المللی که سطح حمایتی کافی را تأمین می‌کنند در روزنامهٔ رسمی اتحادیهٔ اروپا و وب‌گاه این اتحادیه منتشر کند.

رویکرد ایالات متحدهٔ آمریکا

در قانون اساسی ایالات متحدهٔ آمریکا، احترام به حریم خصوصی، به طور گسترده‌ای، مورد توجه قرار گرفته است. با وجود این، برخلاف اتحادیهٔ اروپا، در این کشور یک چارچوب واحد فراگیر در زمینهٔ حریم خصوصی و حمایت از داده وجود ندارد (Ieuan Jolly, Loeb & Loeb, 2020). بسیاری از پژوهشگران قوانین حریم خصوصی دادهٔ از ایالات متحدهٔ آمریکا را قوانین "تکه‌تکه " فدرال و ایالتی توصیف می‌کنند. (LCLG. Com, 2020)

نگرانی‌های موجود، در زمینهٔ چگونگی ادارهٔ اطلاعات شخصی تحت تصرف دولت فدرال، منجر به تصویب قانون حریم خصوصی ایالات متحده آمریکا، در سال ۱۹۷٤ شد. در سال ۱۹۸٦، قانون حریم خصوصی ارتباطات آنلاین، محدودیت‌های دولت را در زمینهٔ ارتباطات تلفنی باسیم افزایش داد که شامل انتقال داده‌های الکترونیکی است. در عین حال، قوانین فدرال حریم خصوصی مصرف‌کننده در ایالات متحدهٔ آمریکا عمدتاً مختص صنایع بوده و در هر بخش، قوانین مختلفی بر جمع‌آوری و افشای داده‌های مالی، سلامت، دانش‌آموزی، سوابق وسایل حمل و نقل موتوری و ... حاکم است. علاوه بر این، هر یک از ایالات مختلف کشور آمریکا، طی سالیان، قوانین حریم خصوصی دیجیتال و حمایت از دادهٔ متفاوتی را تصویب کرده‌اند.

به عقیدهٔ بسیاری از مقام‌ها و وکلای تجاری ایالات متحدهٔ آمریکا، رویکرد این کشور در زمینهٔ حریم خصوصی داده، زیرکانه‌تر از دیدگاه اروپایی، تحت عنوان رویکرد "یک اندازه برای همه" (One-size-fits-all) است. در ایالات متحدهٔ آمریکا، ترویج و تقویت فناوری این کشور اهمیت بیشتری دارد. با وجود این برخی وکلای فعال حریم خصوصی در ایالات متحدهٔ آمریکا معتقدند خلأهای مهمی در رویکرد "تکه‌تکهٔ" آمریکایی، به‌ویژه در جمع‌آوری آنلاین داده‌ها، وجود دارد و بر همین اساس، از مدت‌ها پیش در کنگرهٔ این کشور موضوع تصویب قانون جامع در زمینهٔ حمایت از داده مطرح است.

توافقنامه بندرگاه امن

اتحادیهٔ اروپا و ایالات متحدهٔ آمریکا، در ارتباط با حمایت از داده‌های شخصی رویکردهای متفاوتی دارند. پس از تصویب دستورالعمل حمایت از داده، در سال ۱۹۹۵، مقام‌های اتحادیهٔ اروپا و ایالات متحدهٔ آمریکا متوجه شدند تفاوت‌های قابل توجهی میان نظام‌های حمایت از داده‌های آن‌ها وجود دارد. همچنین تهدیدی که در رابطهٔ با انتقال داده‌های شخصی میان آن‌ها در زمینهٔ از بین بردن یا جلوگیری از آن وجود داشت، باعث ایجاد نگرانی و تأثیر منفی بر بسیاری از کسب و کارها و صنایع در هر دو طرف و نیز تأثیر بالقوه بر رابطهٔ تجاری و سرمایه‌گذاری ایالات متحدهٔ آمریکا ـ اروپا شد.

در پی مذاکرات میان ایالات متحدهٔ آمریکا و اتحادیهٔ اروپا، طرفین بر ساز و کاری که "سطح حمایتی کافی" مقرر شده در دستورالعمل حمایت از داده را تأمین می‌کرد، توافق کردند در سال

۲۰۰۰، وزارت بازرگانی ایالات متحدهٔ آمریکا، اصول حریم خصوصی توافقنامه بندرگاه امن را که متعاقباً توسط کمیسیون اروپا به رسمیت شناخته شد، مورد بررسی قرار داد. با وجود این، مطابق تصمیم کمیسیون اروپایی، اصول توافقنامه بندرگاه امن، به موضوع‌های امنیت ملی، نفع عمومی یا الزام‌های اجرایی قانون محدود بود.

به موجب توافقنامه بندرگاه امن، یک شرکت آمریکایی موظف بود سالانه به وزارت بازرگانی در مورد وضعیت مالی خود، رعایت اصول هفت‌گانه توافقنامه بندرگاه امن و الزام‌های مرتبط با استاندارد سطح حمایتی اتحادیه اروپا گزارش دهد.

اصول هفت‌گانه این توافقنامه به طور مختصر عبارت‌اند از:

- **اطلاع:** سازمان‌های مربوطه، باید اشخاص موضوع داده را در جریان اهدافی قرار دهند که اطلاعات را برای آن جمع‌آوری و استفاده می‌کنند. همچنین چگونگی تماس با سازمان برای طرح سؤال‌ها یا شکایت‌ها و نیز نام اشخاص ثالثی که اطلاعات برای آنها فاش می‌شود، بایستی در اختیار اشخاص موضوع داده قرار گیرد.
- **انتخاب:** سازمان‌های مربوطه، باید به افراد فرصت انتخاب دهند تا اطلاعات شخصی آنها (الف)، برای شخص ثالثی افشا شود؛ یا (ب). برای هدفی متناقض با هدفی (اهدافی) که او مجاز دانسته، جمع‌آوری و بعد استفاده شود. در واقع، در مورد انتخاب موارد مذکور، باید رضایت پسینی اشخاص موضوع داده وجود داشته باشد.
- **در زمینهٔ اطلاعات و داده‌های حساس**، هنگامی که داده‌های شخصی به شخص ثالث منتقل می‌شوند، یا برای هدفی غیر از آنچه داده‌ها در اصل جمع‌آوری یا متعاقباً مجاز دانسته شده، استفاده می‌شود، اشخاص موضوع داده، باید به‌صراحت رضایت دهند. به عبارت دیگر، باید اشخاص موضوع داده، رضایت پیشینی از فرایند مربوطه داشته باشند. رضایت اشخاص موضوع داده، در ارتباط با این نوع از داده‌ها اهمیت بیشتری می‌یابد. داده‌های حساس شامل داده‌های مربوط به شرایط پزشکی یا سلامت افراد، ریشه نژادی یا قومی، عقاید سیاسی، باورهای مذهبی یا فلسفی آنها، عضویت در اتحادیه‌های تجاری و اطلاعات مربوط به زندگی جنسی آنهاست.
- **انتقال داده‌ها به شخص ثالث:** (Onward transfer) سازمان‌ها باید در فرایند انتقال اطلاعات به طرف ثالث، اصول اعلان و انتخاب را رعایت کنند. اشخاص ثالثی که به عنوان نماینده فعالیت می‌کنند، باید همان سطح حمایت از حریم خصوصی را تأمین کنند که شرکت‌کنندگان در توافقنامه بندرگاه امن، هماهنگ با دستورالعمل یا یافتهٔ مناسب دیگر یا مطابق قرارداد حریم خصوصی خود دارند.
- **امنیت:** سازمان‌های ایجادکننده، نگهداری‌کننده، استفاده‌کننده یا منتشرکنندهٔ اطلاعات شخصی باید اقدام‌های احتیاطی مناسب را جهت حمایت در برابر خسارت، سوء استفاده و دسترسی غیرمجاز، افشا، اصلاح و امحای اطلاعات اتخاذ کنند.

- **صحت داده‌ها:** اطلاعات شخصی باید با اهدافی که مورد استفاده قرار می‌گیرند، مرتبط باشند. سازمان‌های مربوطه باید گام‌های متناسبی را بر دارند تا تضمین کنند که داده برای استفادهٔ مورد نظر، دقیق، کامل و جاری است.
- **دسترسی:** افراد باید به اطلاعات خود که یک سازمان در اختیار دارد، دسترسی داشته و قادر به تصحیح، اصلاح یا حذف اطلاعات نادرست باشند، مگر اینکه هزینهٔ آن متناسب با تهدیدهای مربوط به حریم خصوصی افراد یا نقض حقوق سایرین باشد. علاوه بر این، اصول توافقنامه بندرگاه امن، ممکن است محدود به حد لازم برای امنیت ملی، نفع عمومی یا الزام‌های اجرای قانون باشد.
- **اجرا:** حمایت مؤثر از حریم خصوصی، باید شامل ساز و کارهایی باشد جهت تأیید انطباق، ارائهٔ ساز و کارهای مستقل برای دسترسی آسان و مقرون به صرفه در موارد عدم انطباق و تدابیر جبران خسارت برای سازمان مربوطه در زمانی که از اصول پیروی نشده است. محرومیت‌ها و جریمه‌های مربوطه باید به اندازه کافی سختگیرانه باشد تا از این طریق انطباق قوانین و رعایت حداکثری آن‌ها تضمین شود. (Export.gov, 2016)

شرکت در توافقنامهٔ بندرگاه امن، مربوط به هر سازمان آمریکایی موضوع قوانین کمیسیون تجارت فدرال بود که قوانین مختلف حمایت از مصرف‌کننده را، شامل قوانین مرتبط با روش‌های فریبکارانه و غیرمنصفانه، اجرا می‌کند و نیز برای شرکت‌های حمل و نقل هوایی و نمایندگان صدور بلیط که موضوع قوانین وزارت حمل و نقل بودند، آزاد بود. حدود ٤٥٠٠ شرکت در فهرست توافقنامه بندرگاه امن بودند. سازمان‌ها برای اینکه واجد شرایط شوند، ملزم بودند که سالانه به وزارت بازرگانی در مورد رعایت اصول توافقنامهٔ بندرگاه امن گزارش دهند. طبق ادعای کمیسیون تجارت فدرال، این کمیسیون متعهد شده بود که کلیه موارد مربوط به نقض احتمالی مقررات توسط مقام‌های کشورهای عضو اتحادیهٔ اروپا را بررسی کند. (Federal Trade Commission, 2016)

نهادهای بخش خصوصی و فدرال، مقام‌های ایالتی اجراکنندهٔ قوانین مربوط به روش‌های فریبکارانه و غیرمنصفانه، در ایالات متحدهٔ آمریکا ملزم شدند، توافقنامه بندرگاه امن را اجرا کنند. اجرای قوانین توسط بخش خصوصی شامل ساز و کارهای مربوط به تأیید، حل و فصل اختلاف و جبران خسارت بود. بدیهی است که رعایت نکردن مستمر این توافقنامه، منجر به خروج سازمان یا نهاد مربوطه از این توافقنامه می‌شد. البته ذکر این نکته ضروری است که این موضوع مربوط به شرکت‌های مالی و حامل‌های مخابراتی آمریکایی بود و شامل تمام شرکت‌های آمریکایی نمی‌شد. پس از حکم دیوان دادگستری اتحادیهٔ اروپا، در سال ۲۰۱۵، کمیسیون تجارت فدرال اعلام کرد که از نظر این کمیسیون توافقنامه بندرگاه امن دیگر قابل اجرا نخواهد بود. (Calder, 2016)

حکم دیوان دادگستری اتحادیهٔ اروپا

در ماه اکتبر سال ۲۰۱۵، دیوان دادگستری اتحادیهٔ اروپا طی حکمی اعلام کرد که از نظر این دیوان

توافقنامهٔ بندرگاه امن نامعتبر است و طبق قوانین موجود در اتحادیهٔ اروپا این توافقنامه ساز و کار معتبری نیست. (*Ibid*)

حکم دیوان دادگستری اتحادیهٔ اروپا، ناشی از شکایت یک کاربر اتریشی در فیسبوک به نام Maximillian Schrems نزد مقام حمایت از دادهٔ ایرلند بود. موضوع شکایت از این قرار بود که داده‌های شخصی شاکی به صورت کلی و جزئی در سرورهای اتحادیه اروپایی فیسبوک مستقر در ایرلند موجود بود و در ژوئن سال ۲۰۱۳، با توجه افشای غیرمجاز فعالیت‌های نظارتی ایالات متحده آمریکا، به سرورهای فیسبوک در ایالات متحدهٔ آمریکا انتقال یافته بود. مقام حمایت از دادهٔ ایرلندی، این شکایت را رد و اعلام کرد که هیچ مبنایی برای ارزیابی شکایت وجود ندارد؛ زیرا فیسبوک توافقنامه بندرگاه امن را رعایت کرده و مقام حمایت از دادهٔ ایرلندی به حکم کمیسیون اروپا، در سال ۲۰۰۰، پای‌بند بوده است. در حکم مذکور تصریح شده بود، بر اساس توافقنامه بندرگاه امن، این مقام حمایت از داده باید "سطح حمایتی کافی" را تأمین کند. پس از اینکه مقام حمایت از داده ایرلند، شکوائیهٔ این فرد را رد کرد، شکایت به دیوان عالی کشور ایرلند برده شد. این دیوان نیز بررسی کرد که آیا مقام حمایت از دادهٔ ایرلندی می‌تواند تحقیق‌هایی در زمینهٔ روش‌های حمایت از دادهٔ فیسبوک جهت ارزیابی سطح حمایت از داده انجام دهد، یا اینکه مقام حمایت از دادهٔ ایرلندی باید تحقیق‌ها را به تأیید پیشینی مندرج در چارچوب توافقنامه بندرگاه امن از سوی کمیسیون اروپا موکول کند؟ (Weiss, Archic, 2016)

در ٦ اکتبر سال ۲۰۱۵، در محاکم حقوقی مختلف، نظرهای تفسیری متعددی در مورد این حکم صادر شد. طبق نظر دیوان دادگستری اتحادیهٔ اروپا، مقام‌های حمایت از داده در سطح ملی باید بتوانند با استقلال کامل هر نوع ادعای مربوط به حمایت از حقوق و آزادی‌های شخص در فرایند پردازش داده‌های شخصی مربوط به وی را بررسی کرده و انطباق آن با دستورالعمل حمایت از داده و منشور حقوق اساسی اروپا را ارزیابی کنند. دیوان دادگستری اتحادیهٔ اروپا، توافقنامه بندرگاه امن را غیرمعتبر دانست. طبق نظر دیوان دادگستری اتحادیهٔ اروپا، مطابق مادهٔ ۲۵ دستورالعمل حمایت از داده، کمیسیون اروپا ملزم به بررسی قوانین داخلی یا تعهدات بین‌المللی کشور ثالث پیش از تصمیم‌گیری در مورد سطح متناسب حمایت از حریم خصوصی داده آن‌هاست. از آنجایی که، به موجب حکم سال ۲۰۰۰، کمیسیون چنین نتیجه‌ای را نپذیرفته بود، نمی‌توان این حکم را معتبر دانست. توافقنامه بندرگاه امن، دیگر همانند گذشته، یک مبنای قانونی برای انتقال داده بین آمریکا و اروپا ارائه نمی‌داد. اگرچه سایر روش‌ها از قبیل شرایط استاندارد قراردادی یا قوانین مشترک الزام‌آور می‌توانست به عنوان راهکار مورد استفاده قرار بگیرد. (*Ibid*)

علاوه بر این، در حکم دیوان دادگستری اتحادیهٔ اروپا مقرر شد که امنیت ملی ایالات متحدهٔ آمریکا، نفع عمومی و الزام‌های اجرایی، نسبت به اصول توافقنامه بندرگاه امن، اولویت دارند و هنگام تعارض با چنین الزام‌هایی، شرکت‌های آمریکایی بدون هیچ محدودیتی ملزم به نادیده گرفتن

قوانین حمایتی این طرح هستند. درنهایت، دیوان دادگستری اتحادیهٔ اروپا به این نتیجه رسید که توافقنامه بندرگاه امن، امکان دخالت مقام‌های آمریکایی در حقوق اساسی افرادی را ایجاد می‌کند که دادهٔ شخصی آنها از اتحادیهٔ اروپا به ایالات متحدهٔ آمریکا انتقال یافته یا انتقال می‌یابد. به علاوه، دیوان دادگستری اروپا اشاره کرد که حکم سال ۲۰۰۰ کمیسیون در زمینهٔ توافقنامه بندرگاه امن، به هیچ وجه به وجود قوانین آمریکایی یا حمایت‌های مؤثر قانونی جهت محدود کردن چنین مداخلاتی، مانند امکان جبران خسارت قانونی، اشاره نمی‌کند. (*Ibid*)

پس از حکم دیوان دادگستری اتحادیهٔ اروپا، کارگروهی متشکل از مقام‌های حمایت از دادهٔ اتحادیه اروپا (کارگروه مادهٔ ۲۹ دستورالعمل حمایت از داده) دوباره تأیید کردند، انتقال داده‌ای که به موجب توافقنامه بندرگاه امن صورت گرفته، در حال حاضر غیرقانونی است. این کارگروه، مواضع و نگرانی‌های خود را در مورد تأثیر احکام دیوان دادگستری اتحادیهٔ اروپا بر سایر ساز و کارهای انتقال و به اشتراک‌گذاری داده، مانند شرایط قراردادی استاندارد یا قوانین مشترک الزام‌آور، اعلام کردند. کارگروه مادهٔ ۲۹ دستورالعمل حمایت از داده، به منظور یافتن راه‌حل‌های سیاسی، قانونی و فنی، از مقام‌های آمریکایی درخواست مذاکره کرد تا از این طریق، در فرایند انتقال داده به ایالات متحدهٔ آمریکا، حقوق اساسی افراد محترم شمرده شود. این کارگروه تصریح کرد که ممکن است راه حل برون‌رفت از این مسئله، مذاکرهٔ مجدد دربارهٔ توافقنامه بندرگاه امن و بازنگری آن باشد. در نتیجه، کارگروه مادهٔ ۲۹، تا ۳۱ ژانویهٔ سال ۲۰۱۶، برای مذاکره‌کنندگان آمریکایی و اروپایی مهلت تعیین کرد که در زمینهٔ بازنگری توافقنامه بندرگاه امن بحث و بررسی کرده و به توافق برسند. (Article Data Protection Working Party, 2000)

توافقنامهٔ جدید حامی حریم خصوصی اتحادیهٔ اروپا ـ آمریکا

کمیسیون اروپایی و وزارت بازرگانی ایالات متحدهٔ آمریکا، در سال ۲۰۱۶، متن کامل توافقنامهٔ جدید خود را تحت عنوان حامی حریم خصوصی منتشر و اعلام کردند این توافقنامه، جایگزین رسمی توافقنامه بندرگاه امن خواهد بود. همچنین اتحادیهٔ اروپا سندی را منتشر و به موجب آن اعلام کرد توافقنامهٔ جدید، سطح حمایتی کافی و استانداردهای موجود در مقررات عمومی حمایت از داده را، در زمینهٔ انتقال فرامرزی داده، تأمین کرده است. در این سند تأکید شده که توافقنامهٔ جدید اصولی دقیق برای افزایش الزام‌ها در رابطه با شفافیت، ساز و کارهای جدید و تعهدات دولت ایالات متحدهٔ آمریکا در مورد محدود شدن اقدام‌های نظارتی و امنیتی این کشور دارد. (The European Commission, 2016)

در عین حال، نگرانی‌هایی نیز از جانب این کمیسیون مطرح شد که عبارت‌اند از:

۱. هیچ الزام مشخصی برای سازمان‌ها وجود ندارد تا آن‌ها داده‌های شخصی جمع‌آوری شده را، پس از رسیدن به هدف، حذف کنند.

۲. حمایت‌های مربوط به انتقال داده‌ها به شخص ثالث کافی نیست.

۳. ساز و کارها برای جبران خسارت بیش از حد پیچیده است.
٤. ضمانت اجرایی ارائه‌شده از جانب مقام‌های ایالات متحدهٔ آمریکا، در رابطه با دسترسی به داده‌های انبوه، با محدودیت‌هایی روبه‌روست که طبق نظر کارگروه نظارت بر رعایت استاندارد حمایت از حریم خصوصی اتحادیهٔ اروپا، در زمینهٔ نظارت مقام‌های عمومی، ضمانت اجرایی مذکور کافی نیست.
۵. با توجه به تصویب مقررات عمومی جدید حمایت از داده ((General Data Protection Regulation (GDPR) در سال ۲۰۱٦، باید توافقنامهٔ حامی حریم خصوصی در بردارندهٔ مقرراتی باشد که بتوان آن را مطابق استانداردهای اصلی مقررات عموم حمایت از داده تنظیم و اجرا کرد. (Weiss, Archic, 2016)

اصول و مقررات توافقنامهٔ حامی حریم خصوصی اتحادیهٔ اروپا ـ آمریکا

پس از تشریح وقایع و مسائل مربوط به توافقنامه حامی حریم خصوصی، لازم است که مفاد این توافقنامه و اصول و مقررات مندرج در آن نیز مورد بررسی قرار گیرد. در ادامه به این موضوع پرداخته خواهد شد.

در بخش تعاریف توافقنامهٔ حامی حریم خصوصی، مفاهیم داده‌ها و اطلاعات شخصی، پردازش و کنترل‌کننده تعریف شده است. مطابق این توافقنامه، "داده‌ها و اطلاعات شخصی" عبارت‌اند از: «داده‌هایی دربارهٔ افراد شناسایی‌شده یا قابل شناسایی که در محدودهٔ این دستورالعمل قرار دارند و سازمانی در ایالات متحده آمریکا از اتحادیهٔ اروپا دریافت و در هر گونه فرمی ثبت کرده است». همچنین "پردازش" داده‌های شخصی به معنای «هر فعالیت یا مجموعه فعالیت‌هایی است که روی داده‌های شخصی انجام شده؛ از قبیل جمع‌آوری، ضبط، سازمان‌دهی، ذخیره‌سازی، اصلاح یا تغییر، بازیابی، مشاوره، استفاده، افشا، انتشار و پاک کردن یا امحاء، خواه از طریق ابزارهای خودکار باشد یا نباشد». "کنترل‌کننده" نیز به معنای «یک فرد یا سازمان است که به‌تنهایی یا همراه با دیگران، اهداف و ابزار پردازش داده‌های شخصی را تعیین می‌کند.»

اصول کلی مندرج در توافقنامه حامی حریم خصوصی عبارت‌اند از:

۱. اطلاع: سازمان‌های مربوطه باید افراد را از این موارد مطلع کنند:

الف. مشارکت خود فرد در توافقنامه حامی حریم خصوصی و ارائهٔ یک لینک اینترنتی، یا آدرس وب‌گاه به او برای فهرست توافقنامه حامی حریم خصوصی؛

ب. انواع داده‌های شخصی جمع‌آوری‌شده و در صورت لزوم، نهادها یا شرکت‌های تابعه سازمان که از این اصول پیروی می‌کنند؛

ج. تعهد سازمان نسبت به اصول تمام داده‌های شخصی دریافت‌شده از اتحادیهٔ، با توجه به توافقنامهٔ حامی حریم خصوصی؛

د. اهدافی که اطلاعات شخصی برای آن جمع‌آوری و استفاده می‌شود؛

ه . چگونگی ارتباط با سازمان و هر سازمان مربوطه در اتحادیهٔ اروپا که پاسخگوی سؤال‌ها و یا شکایت‌های افراد در زمینهٔ این توافقنامه است،

و. موقعیت اجتماعی یا هویت اشخاص ثالثی که اطلاعات شخصی فرد برای آنها افشا می‌شود و همچنین دلیل افشای این اطلاعات برای آنها؛

ز. حق افراد برای دسترسی به داده‌های شخصی خود؛

ح. گزینه‌ها و ساز و کارهایی که سازمان برای محدود کردن استفاده و افشای داده‌های شخصی به افراد پیشنهاد می‌دهد؛

ط. نهاد حل اختلاف مستقل برای رسیدگی به شکایت‌ها و ارائهٔ راه‌حل‌های مناسب به صورت رایگان برای فرد، که ممکن است (۱) هیئت ایجادشده توسط مقامات حمایت از داده باشد یا (۲) نهاد ارائه‌کننده راه حلی برای اختلاف در اتحادیهٔ اروپا، و یا (۳) نهاد ارائه‌کننده یک راه حل اختلاف دیگر در ایالات متحده آمریکا باشد؛

ی. تحت نظارت و اعمال اختیارات کمیسیون تجارت فدرال، وزارت حمل و نقل یا هر گونه نهاد ذیصلاح دیگر بودن؛

ک. امکان درخواست داوری الزام‌آور برای فرد تحت شرایط خاص؛

ل. الزام به افشای اطلاعات شخصی در پاسخ به درخواست‌های قانونی مقام‌های عمومی مانند رعایت الزام‌های قانونی یا امنیت ملی؛

م . مسئولیت سازمان در موارد انتقال داده‌ها به اشخاص ثالث.

۲. **انتخاب:** یک سازمان باید به افراد فرصتی برای انتخاب (رضایت پسینی) اینکه آیا اطلاعات شخصی آنها (الف) به طرف شخص ثالث افشا شده یا (ب) برای هدفی کاملاً متفاوت از اهدافی که داده‌هایش از ابتدا برای آن جمع‌آوری شده، یا متعاقباً توسط آنها مجاز دانسته شده، ارائه دهد. باید ساز و کارهای شفاف، آشکار و قابل دسترس برای انتخاب افراد فراهم شود.

۳. **پاسخگویی در زمینهٔ انتقال داده‌ها به اشخاص ثالث:** سازمان‌ها برای انتقال اطلاعات شخصی به شخص ثالث باید اصول اطلاع و انتخاب را رعایت کرده و مانند یک کنترل‌کننده عمل کنند. همچنین، سازمان‌ها باید با اشخاص ثالث کنترل‌کننده، قراردادی منعقد کنند که به موجب آن چنین داده‌هایی تنها برای اهداف مشخص و محدود و سازگار با رضایت ارائه‌شده توسط فرد پردازش شود و اینکه دریافت‌کننده، همان سطح حمایت مندرج در اصول را ارائه خواهد کرد، در صورتی‌که تصمیمی گرفته شود که مطابق آن، این الزام رعایت نشود، سازمان را مطلع سازد. در قرارداد باید درج شود، هنگامی که چنین تصمیمی اتخاذ می‌شود، شخص ثالث کنترل‌کننده، پردازش را متوقف کند یا سایر اقدام‌های قانونی و متناسب برای مقابله با آن را انجام دهد.

٤. **امنیت:** با توجه به مخاطرات مربوط به پردازش و ماهیت داده‌های شخصی، سازمان‌های ایجاد کننده، نگهداری‌کننده، استفاده‌کننده یا منتشرکنندهٔ آن برای محافظت از داده‌های شخصی در

برابر از دست رفتن، سوء استفاده و دسترسی غیرمجاز، افشا، تغییر و تخریب، باید اقدام‌های منطقی و مناسب را انجام دهند.

۵. **صحت داده‌ها و محدودیت هدف:** مطابق با اصول، اطلاعات شخصی باید به اطلاعات مربوط به اهداف پردازش، محدود شود. یک سازمان نمی‌تواند اطلاعات شخصی را به طریقی که با اهداف جمع‌آوری یا مجوز بعدی فرد سازگار نیست، پردازش کند. یک سازمان باید تا حد لزوم برای رسیدن به این اهداف، گام‌های معقول بر دارد تا مطمئن شود داده‌های شخصی برای استفادهٔ مورد نظر قابل اعتماد، دقیق، کامل و جاری مناسب است. یک سازمان باید تا زمانی که چنین اطلاعاتی را نگهداری می‌کند، به اصول پای‌بند باشد.

٦. **دسترسی:** افراد باید به اطلاعات شخصی خود، که یک سازمان نگهداری می‌کند، دسترسی داشته باشند و زمانی که این اطلاعات نادرست یا برخلاف اصول پردازش شده باشد، بتوانند آن را اصلاح، ویرایش یا حذف کند. البته این موضوع به استثناء مواردی است که مسئولیت یا هزینهٔ ارائهٔ دسترسی نامتناسب و تهدید حریم خصوصی سایر افراد باشد یا حقوق اشخاص دیگر نقض شود.

۷. **بازبینی، اجرا و مسئولیت:** حمایت مؤثر از حریم خصوصی باید شامل ساز و کارهای مؤثری جهت ضمانت رعایت اصول باشد تا چنانچه فردی از رعایت نکردن اصول حریم خصوصی شکایت کرد، پیامدهای آن متوجه سازمان شود. این ساز و کارها حداقل باید شامل موارد ذیل باشند:

الف. ساز و کارهای مستقل و در دسترس برای رسیدگی به شکایت‌ها و اختلاف‌ها، به طوری که هر فرد بتواند به‌سرعت و بدون هیچ هزینه‌ای با مراجعه به اصول آن را حل کند و خسارت‌ها در مواردی که قانون قابل اجرا وجود داشته باشد یا نهادهای بخش خصوصی اقدام کنند، جبران شود.

ب. سازوکار روش‌های پیگیری برای تأیید گواهی‌ها و اظهارات سازمان‌ها دربارهٔ رویکردهای حریم خصوصی خود و رویکردهای حریم خصوصی اجرا شده، به‌ویژه در ارتباط با موارد عدم انطباق صحیح است.

ج. تعهدات برای رفع مشکلات ناشی از پیروی نکردن از اصول توسط سازمان‌هایی که اعلام کرده‌اند از آن پیروی می‌کنند و پیامدها برای چنین سازمان‌هایی باید به اندازهٔ کافی سخت باشد تا پیروی سازمان‌ها تضمین شود.

همچنین اصول تکمیلی این توافقنامه عبارت‌اند از: داده‌های حساس، استثناهای روزنامه‌نگاری، مسئولیت فرعی و انجام بازرسی‌های معقولانه و حسابرسی، نقش مقام‌های حمایت از داده، اظهارنامه، تأیید، داده‌های منابع انسانی، قراردادهای الزام‌آور برای انتقال داده‌ها به اشخاص ثالث، حل و فصل اختلاف‌ها و اجرا، انتخاب زمان‌بندی رضایت پسینی، اطلاعات سفر، محصولات دارویی و پزشکی، اطلاعات سابقهٔ عمومی و موجود در دسترس عموم، درخواست‌های دسترسی توسط مقام‌های عمومی. در ادامه به مهم‌ترین این موارد پرداخته خواهد شد:

مسئولیت فرعی (Secondary Responsibility): هنگامی که ارائه‌دهندگان خدمات اینترنتی

((Internet Service Providers (ISPs)، حامل‌هـــای مخابراتی (Telecommunications carriers) و ســـایر سازمان‌ها از جانب ســـازمانی دیگر فقط اطلاعات را انتقال می‌دهند، ذخیره می‌کنند یا مســـیر اطلاعات را می‌یابند، به موجب اصول توافقنامهٔ حامی حریم خصوصی مســـئول نیستند. همان‌گونه که در این دستورالعمل مقرر شده، توافقنامهٔ حامی حریم خصوصی مسئولیت فرعی ایجاد نمی‌کند. ســـازمان مذکور، تنها یک مجرا برای انتقال داده‌ها توسط اشخاص ثالث است و اهداف و ابزار پردازش داده‌های شخصی مربوطه را تعیین نمی‌کند.

اظهارنامه: در اظهارنامهٔ مربوط به توافقنامهٔ حامی حریم خصوصی، سازمان مربوطه باید از طریق مأمور خود به وزارتخانهٔ مربوطه یک اظهارنامهٔ امضاشده حاوی اطلاعات ذیل ارائه کند:

الف. نام سازمان، آدرس پستی، آدرس پست الکترونیکی، شماره تلفن و فکس؛

ب. شرح فعالیت‌های سازمان در ارتباط با اطلاعات شخصی دریافت‌شده از اتحادیه اروپا؛

ج. شرح سیاست حریم خصوصی سازمان در زمینهٔ اطلاعات شخصی شامل:

۱. دسترسی عمومی به سیاست حریم خصوصی سازمان، در وب‌گاه آن یا هر شکل دیگری که این امکان را فراهم کند؛

۲. تاریخ اجرا؛

۳. یک دفتر تماس برای رسیدگی به شکایت‌ها، درخواست‌های دسترسی و سایر مسائل ناشی از توافقنامه حامی حریم خصوصی؛

٤. ساختار قانونی خاص که صلاحیت رسیدگی به ادعاها علیه سازمان در زمینهٔ روش‌های غیرمنصفانه یا فریبکارانه و نقض قوانین یا مقررات حاکم بر حریم خصوصی را داشته باشد (در فهرست اصول یا ضمیمه اصول بعدی ذکر شده است)؛

۵. نام هر طرح مربوط به حریم خصوصی که سازمان عضو آن است؛

٦. روش تأیید (مثلاً در خانه، شخص ثالث)؛

۷. ساز و کار مستقل برای مراجعه جهت بررسی شکایت‌های حل نشده؛

همچنین، در پیوست این سند یک مدل داوری برای حل و فصل اختلافات وجود دارد که در آن به الزام‌های پیش از داوری، ماهیت تصمیم‌های داوری و الزام‌آور بودن آن برای طرفین، هزینه‌های داوری و مسائلی از این قبیل پرداخته شده است. (The U.S. Department of Commerce, 2016)

لازم به ذکر است که در وب‌گاه رسمی توافقنامه حامی حریم خصوصی فهرستی از سازمان‌های مشارکت‌کننده در این توافقنامه درج شده است. (Privacy Shield Frame work, 2020)

مقایسهٔ توافقنامهٔ امن و توافقنامهٔ حامی حریم خصوصی

علیرغم اینکه توافقنامهٔ حامی حریم خصوصی، در بسیاری از موارد با توافقنامهٔ بندرگاه امن شباهت دارد، در برخی موضوع‌ها نیز از توافقنامه پیشین متفاوت است. برای درک بهتر نقاط مشترک و

افتراق این دو توافقنامه می‌توان به مقایسه‌ای رجوع کرد که یک مؤسسه حقوقی آمریکایی ارائه کرده است. (Bryan Cave, 2020)

الزام‌های قانونی	توافقنامه بندرگاه امن	توافقنامه حامی حریم خصوصی
سیاست‌نامه حریم خصوصی. هر سازمان باید یک سیاست‌نامه حریم خصوصی شامل موارد ذیل منتشر کند:		
انواع داده‌های شخصی جمع‌آوری‌شده	✓	✓
هدف جمع‌آوری داده‌ها	✓	✓
اطلاعات تماس برای طرح سؤال‌ها/ شکایت‌ها	✓	✓
فهرست اشخاص ثالث دریافت‌کنندهٔ داده‌ها	✓	✓
اختیارات شخص موضوع داده برای محدود کردن استفاده از داده‌ها	✓	✓
اعلام انطباق سازمان با اصول توافقنامه	✓	✓
دسترسی به فهرست منتشرشده از جانب وزارت بازرگانی ایالات متحدهٔ آمریکا	×	✓
حق اشخاص موضوع داده برای دسترسی به داده‌ها	×	✓
تأیید صلاحیت قانونی کمیسیون تجارت فدرال، وزارت حمل و نقل ایالات متحدهٔ آمریکا یا سایر سازمان‌های اجرایی ایالات متحدهٔ آمریکا	×	✓
الزام به دادن داده‌های شخصی در قبال ارائه درخواست قانونی سازمان‌های مربوطه	×	✓
تأیید مسئولیت در قبال انتقال داده‌ها به اشخاص ثالث	×	✓
ارائهٔ ساز و کارهای مستقل	✓	✓
قابلیت ارائهٔ رضایت پسینی دربارهٔ افشای داده‌ها برای اشخاص ثالث (به جز ارائه‌دهندگان خدمات) و همچنین استفاده از داده‌ها با اهداف متفاوت و رضایت پیشینی در مورد داده‌های حساس و استفاده از آن‌ها	✓	✓
انتقال داده‌ها به کنترل‌کننده‌ها؛ زمانی که داده‌ها به یک کنترل‌کننده انتقال می‌یابد، هر سازمان باید:		
قراردادی منعقد کند که به موجب آن داده را تنها برای اهداف مشخص و محدود با رضایت شخص موضوع داده بتواند پردازش کند.	×	✓
شخص ثالث را ملزم کند که در صورتی که نتواند اصول حریم خصوصی را رعایت کند، سازمان را مطلع سازد.	×	✓
انتقال onward داده‌ها به ارائه‌دهندگان خدمات؛ زمانی که داده‌ها به یک سازمان ثالث یا ارائه‌دهنده خدمات انتقال می‌یابد، هر سازمان باید:		
تأیید کند که ارائه‌کننده خدمات عضو دستورالعمل حمایت از داده است یا توافق کند که سطح حمایتی کافی را فراهم آورد.	✓	✓

اقدام‌هایی جهت ارزیابی ارائه‌دهنده خدمات انجام دهد.	×	✓
اقدام‌هایی جهت متوقف کردن پردازش غیرمجاز انجام دهد.	×	✓
بنا بر درخواست وزارت بازرگانی خلاصه‌ای از قرارداد در اختیار این وزارتخانه بگذارد.	×	✓
مسئولیت ارائه‌دهندهٔ خدمات را در صورت پردازش اشتباه مفروض بداند.	×	✓
شخص ثالث را ملزم کند که در صورتی‌که نتواند اصول حریم خصوصی را رعایت کند، سازمان را مطلع سازد.	×	✓
امنیت: هر سازمان باید موارد ذیل را اجرا کند:		
تعقیب‌های قضایی منصفانه برای حفاظت از داده‌ها در برابر از دست رفتن، سوء استفاده، دسترسی غیرمجاز، افشا، اصلاح یا امحا انجام دهد.	✓	✓
صحت داده‌ها: هر سازمان باید:		
اقدام‌های مقتضی را جهت تضمین اینکه داده‌های شخصی دقیق، کامل، به روز و برای استفاده مورد نظر قابل اطمینان هستند انجام دهد.	✓	✓
اقدام‌های مربوط به کاهش میزان داده‌ها انجام دهد که اطلاعات تا زمانی که برای هدف پردازش مورد نیاز است باقی بماند	×	✓
دسترسی: هر سازمان باید موارد ذیل را فراهم آورد:		
حق شخص موضوع داده برای تأیید اینکه سازمان داده‌های وی را داشته باشد یا نداشته باشد.	×	✓
حق شخص موضوع داده برای اصلاح اطلاعات خود، به غیر از مواقعی که بر اثر شرایط حقوقی، انجام چنین ممکن نباشد یا حقوق شخص ثالثی این‌گونه اقتضا کند.	✓	✓
حق شخص موضوع داده برای حذف اطلاعات نادرست خود، به غیر از مواقعی که بر اثر شرایط حقوقی انجام چنین امری ممکن نباشد یا حقوق شخص ثالثی این‌گونه اقتضا کند.	✓	✓
توانایی اجرای حقوق شخص موضوع داده: هر سازمان باید:		
ساز و کار مستقلی برای جبران خسارات ارائه کند.	✓	✓
ساز و کار مستقل را رایگان ارائه کند.	×	✓
داوری الزام‌آور را قبول کند.	×	✓
احکام صادره از دادگاه‌های کشورهای عضو را قبول کند.	×	✓
مسئولیت احتمالی شخص موضوع داده را در مورد نقض داده بپذیرد.	نامشخص	✓

نظارت: هر سازمان ملزم است تا:		
به تحقیق‌ها و درخواست‌های وزارت بازرگانی پاسخ دهد.	×	✓
در صورت انتقال داده‌های منابع انسانی مستقیم به مقام‌های حمایت از داده اتحادیهٔ اروپا پاسخ دهد.	✓	✓
مسئولیت نظارتی: هر سازمان را می‌توان در مورد ذیل مسئول دانست:		
صدور حکم	✓ (کمیسیون تجارت فدرال)	✓(کمیسیون تجارت فدرال)
اجرا: هر سازمان باید موارد ذیل را به منظور ارائه گزارش خوداظهاری به وزارت بازرگانی ارائه کند:		
اطلاعات تماس سازمان	✓	✓
شرح فعالیت‌های پردازش	✓	✓
شرح سیاست‌نامه حریم خصوصی	✓	✓
آدرس اینترنتی	✓	✓
تاریخ اجرای سیاست‌نامه حریم خصوصی	✓	✓
دفتر رسیدگی به شکایات	✓	✓
نهاد حکومتی با صلاحیت نظارتی	✓	✓
اسامی طرف ثالث طرح‌های حریم خصوصی	✓	✓
روش تأیید	✓	✓
ساز و کار مستقل	✓	✓
هزینه‌ها		
هزینه‌های ثبت	۲۰۰ دلار	نامشخص

بررسی الزام‌های حقوقی انتقال فرامرزی داده در ایران

حال که موضوع انتقال فرامرزی داده در دو نظام حقوقی مطرح در سطح جهان بررسی شد، بهتر است قوانین و مقررات این حوزه در کشور ایران نیز مورد مداقه قرار گیرد.

- در نظام حقوقی ایران، جز تعداد انگشت‌شمار، قوانین و مقررات خاصی در زمینهٔ حمایت از داده و موضوع‌های مرتبط با آن وجود ندارد. یکی از مهم‌ترین قوانین در این حوزه قانون تجارت الکترونیکی مصوب سال ۱۳۸۲ است که در آن اشاره‌ای به انتقال فرامرزی داده نشده است.
- در مادهٔ ۱ آیین‌نامهٔ اجرایی مادهٔ ۸ قانون انتشار و دسترسی آزاد به اطلاعات، مصوب سال ۱۳۹۳ در هیئت وزیران نیز حق دسترسی به داده‌ها و اطلاعات تنها به اشخاص حقیقی یا حقوقی ایرانی داده شده است (آیین‌نامه اجرایی قانون انتشار و دسترسی آزاد به اطلاعات، ۱۳۹۳). البته

در مادهٔ ١٤ تا ١٧ قانون انتشار و دسترسی آزاد به اطلاعات مصوب سال ١٣٨٨، دسترسی به اطلاعات به حمایت از حریم خصوصی افراد، حمایت از سلامتی و اطلاعات تجاری محدود شده، همچنین به موضوع‌هایی مانند امنیت و آسایش عمومی، پیشگیری از جرائم یا کشف آن‌ها، بازداشت یا تعقیب مجرمان، ممیزی مالیات یا عوارض قانونی یا وصول آن‌ها و اعمال نظارت بر مهاجرت به کشور پرداخته شده است. (قانون انتشار و دسترسی آزاد به اطلاعات، ١٣٩٣)

- یکی دیگر از قوانینی که در حوزهٔ انتقال فرامرزی داده می‌توان از آن نام برد، قانون برنامهٔ پنج‌ساله پنجم توسعه جمهوری اسلامی ایران مصوب سال ١٣٨٩ است. در تبصرهٔ ٢ مادهٔ ٤٦ این قانون و همچنین در مصوبهٔ جلسهٔ سی‌وپنجم مورخ ٢٠/٩/ ١٣٩٥ شورای عالی فضای مجازی تحت عنوان "تبیین الزامات شبکهٔ ملی اطلاعات" مقرر شده: شبکهٔ ملی اطلاعات (IP) کشور، شبکه‌ای مبتنی بر قرارداد اینترنت به همراه سوئیچ‌ها و مسیریاب‌ها و مراکز داده‌ای است به صورتی که درخواست‌های دسترسی داخلی و اخذ اطلاعاتی که در مراکز داده داخلی نگهداری می‌شوند، به هیچ وجه از طریق خارج کشور مسیریابی نشود و امکان ایجاد شبکه‌های اینترانت و خصوصی و امن داخلی در آن فراهم شود». از مفاد این ماده چنین به نظر می‌رسد، با راه‌اندازی شبکهٔ ملی اطلاعات، مسیریابی داده‌ها از طریق خارج از کشور غیرممکن خواهد بود. حال سؤالی که مطرح می‌شود این است که آیا مسیریابی داده‌ها (Routing) را می‌توان با انتقال داده‌ها یکی در نظر گرفت؟ به نظر می‌رسد که این دو، دو مفهوم کاملاً متفاوت بوده و نمی‌توان مقررات مربوط به مسیریابی داده را به انتقال داده نیز تعمیم داد.
- علاوه بر این، در پیش‌نویس لوایح پنج‌گانهٔ وزارت ارتباطات و فناوری اطلاعات که در سال ١٣٩٦ با همکاری پژوهشگاه قوه قضاییه تدوین شده، موضوع انتقال فرامرزی داده مورد توجه قرار گرفته است. لایحهٔ حکمرانی الکترونیکی یکی از این لوایح است که در مادهٔ ٧٦ آن مقرر شده: «میزبانی داده‌های موضوع این قانون در خارج از کشور ممنوع است». همان‌گونه که از مفهوم این ماده برمی‌آید، به طریق اولی انتقال داده به خارج از کشور و میزبانی آن در آن‌جا ممنوع است. یکی دیگر از لوایح مذکور که در آن به موضوع انتقال فرامرزی داده توجه شده، لایحهٔ حمایت از داده و حریم خصوصی در فضای مجازی است که سال ١٣٩٦ وزارت ارتباطات و فناوری اطلاعات تهیه کرده است. مطابق مادهٔ ١٨ پیش‌نویس این لایحه: «ایجاد یا پردازش داده‌های شخصی حساس برای انجام پژوهش‌های پزشکی، پیراپزشکی و روانشناسی توسط دانشگاه‌ها و مراکز تحقیقاتی و مؤسسات پژوهشی و پژوهشکده‌ها و پژوهشگاه‌های کشور مجاز است. ارائهٔ این داده‌ها به نهادهای علمی بین‌المللی تنها با تصویب هیئت وزیران مجاز است». همان‌طور که ملاحظه می‌شود، در این ماده تنها تکلیف داده‌های حساس مشخص شده و دربارهٔ سایر انواع داده‌ها سکوت شده است.

بنابراین، طبق آنچه گفته شد، می‌توان این‌گونه نتیجه گرفت که در نظام حقوقی کشور ایران، در حوزهٔ انتقال فرامرزی داده سکوت قانونی وجود داشته و موارد اندکی در این رابطه، مانند الزام‌های شبکهٔ ملی اطلاعات، وجود دارد که شاید با تفسیر موسع بتوان آن را با این موضوع مرتبط دانست. بقیه مواردی که ذکر شد هنوز در مرحله قانونگذاری بوده و قابل استناد نیست.

نتیجه‌گیری

موضوع انتقال فرامرزی داده یکی از کلیدی‌ترین مسائل در حوزهٔ حمایت از داده‌های شخصی افراد است. توافقنامهٔ حامی حریم خصوصی، به عنوان یکی از توافقنامه‌های مهم در این زمینه و جایگزینی برای توافقنامه بندرگاه امن، نقش مهم و تعیین‌کننده‌ای در بررسی مباحث موجود در این رابطه دارد؛ زیرا این توافقنامه همانند توافقنامهٔ پیشین میان دو نظام حقوقی مهم در جهان منعقد شده و چارچوب مناسبی در این حوزه ترسیم کرده است.

همان‌گونه که در این پژوهش تشریح شد، رویکردهای متفاوتی در زمینهٔ حمایت از داده در اتحادیهٔ اروپا و ایالات متحدهٔ آمریکا وجود دارد. در توافقنامهٔ حامی حریم خصوصی دولت‌ها به یک دیدگاه مشترک، علیرغم تفاوت‌ها، دست یافته‌اند. این توافقنامه، نسبت به توافقنامهٔ بندرگاه امن از ضمانت اجرای بیشتری برخوردار است. اصول موجود در توافقنامه حامی حریم خصوصی عبارت از: اطلاع، انتخاب، پاسخگویی در زمینهٔ انتقال به شخص ثالث، امنیت، یکپارچگی داده‌ها و محدودیت هدف، دسترسی و بازنگری، اجرا و مسئولیت است. در این پژوهش تلاش شد تا با بررسی موشکافانهٔ توافقنامهٔ حامی حریم خصوصی و وقایع و مسائل مربوط به آن، از این منظر به موضوع انتقال فرامرزی داده نگاه شود، تا بتوان بر همین اساس به ارائهٔ راهکار برای رفع چالش‌های احتمالی موجود بر سر راه انتقال فرامرزی داده در کشور پرداخت. زیرا به نظر می‌رسد، نظام حقوقی ایران در این زمینهٔ خلأ قانونی دارد و به‌تازگی حقوقدانان متوجه اهمیت این موضوع شده‌اند.

منابع

نورایی بیدخت، حسن (۱۳۷۸)، "حریم خصوصی افراد در جریان بین‌المللی داده‌ها"، فصلنامه رسانه، شماره ۳۸، ۱۳۷۸.

آیین‌نامه اجرایی قانون انتشار و دسترسی آزاد به اطلاعات، ۱۳۹۳.

قانون انتشار و دسترسی آزاد به اطلاعات، ۱۳۸۸.

قانون برنامه پنج‌ساله پنجم توسعه جمهوری اسلامی ایران، ۱۳۸۹.

تبیین الزامات شبکه ملی اطلاعات (۱۳۹۵)، مصوبه شورای عالی فضای مجازی.

لایحه حکمرانی الکترونیکی، ۱۳۹۶.

پیش‌نویس لایحه حمایت از داده و حریم خصوصی در فضای مجازی (۱۳۹۶)، وزرات ارتباطات و فناوری اطلاعات.

ارائه لوایح پنج‌گانهٔ برای پر کردن خلاءهای حقوقی حوزه فناوری اطلاعات و ارتباطات، (۱۳۹۶)، دسترسی در:

https://www.ict.gov.ir/fa/newsagency/20934/%D8%A7%D8%B1%D8%A7%DB%8C%D9%87-%D9%84%D9%88%D8%A7%DB%8C%D8%AD-%D9%BE%D9%86%D8%AC%DA%AF%D8%A7%D9%86%D9%87-%D8%A8%D8%B1%D8%A7%DB%8C-%D9%BE%D8%B1-%DA%A9%D8%B1%D8%AF%D9%86-%D8%AE%D9%84%D8%A7%D9%87%D8%A7%DB%8C-%D8%AD

Calder, Alan (2016), *EU GDPR & EU-US Privacy Shield: A Pocket Guide*, IT Governance Publishing.

European Commission, (2016), GUIDE TO THE EU-U.S. PRIVACY SHIELD, Directorate-General for Justice and Consumers.

Weiss, Martin A.& Kristin Archick (2016), "From Safe Harbor to Privacy Shield", *Congressional Research Service*, 2016.

COMMISSION IMPLEMENTING DECISION (EU) 2016/1250, Official Journal of the European Union, 2016

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, Official Journal of the European Union, 2016.

Opinion 4/2000 on the level of protection provided by the "Safe Harbor Principles", Article 29 Data Protection Working Party, May 2000.

THE U.S. DEPARTMENT OF COMMERCE, EU-U.S. PRIVACY SHIELD FRAMEWORK PRINCIPLES ISSUED BY THE U.S. DEPARTMENT OF COMMERCE, 2016.

"Infoplease، June 2013 Current Events: U.S. News", Available on: https://www.infoplease.com/world/2013-current-events/june-2013-current-events-us-news, Accessed May 4, 2020.

"EUROPEAN DATA PROTECTION SUPERVISOR, The History of the General Data Protection Regulation", Available on:

https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en, Accessed May 4, 2020.

"Ieuan Jolly, Loeb & Loeb, Data protection in the United States: overview", THOMSON REUTERS Practical Law, Available on:

https://uk.practicallaw.thomsonreuters.com/Document/I02064fbd1cb611e38578f7ccc38dcbee/VieV/FullText.html?transitionType=CategoryPageItem&contextData=(sc.Default)&navId=4D7F72779E22D71007EF5B57200D5532&comp=pluk&firstPage=true&bhcp=1, Accessed May 4, 2020.

ICLG.com, " USA: Data Protection 2019", Available on:

https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa, Accessed May 4, 2020.

Export.gov, Helpful Hints on Self-Certifying Compliance with the U.S.-EU Safe Harbor Framework, 2016, Available on:

https://2016.export.gov/safeharbor/eu/eg_main_018495.asp, Accessed May 4, 2020.

"Federal Trade Commission, U.S.-EU Safe Harbor Framework, 2016", Available on:

https://www.ftc.gov/tips-advice/business-center/privacy-and-security/u.s.-eu-safe-harbor-framework, Accessed May 4, 2020.

"The European Commission, Restoring trust in transatlantic data flows through strong safeguards: European Commission presents EU-U.S. Privacy Shield, 2016", Available on:

https://ec.europa.eu/commission/presscorner/detail/en/IP_16_433, Accessed May 4, 2020.

"Privacy Shield Framework, Privacy Shield list", Available on:
https://www.privacyshield.gov/list, Accessed May 4, 2020.
Bryan Cave, "A Side-By-Side Comparison of "Privacy Shield and the "Safe Harbor", 2019, Available on:
https://www.bclplaw.com/images/content/8/5/v2/85609/Comparison-of-Privacy-Shield-and-the-Safe-Harbor.pdf, Accessed May 4, 2020.