تنظیم‌گری حریم خصوصی در فضای مجازی
(مطالعه تطبیقی در حقوق ایالات متحده آمریکا، اتحادیه اروپا و ایران)

سعیده مزینانیان*

تاریخ دریافت: ۱۴۰۲/۰۵/۲۱ تاریخ پذیرش: ۱۴۰۲/۰۷/۰۴

چکیده

امروزه فناوری نوین اطلاعات و ارتباطات، نقشی پایه در امور اجتماعی، اقتصادی و فرهنگی جوامع ایفا کرده است و به‌عنوان نیروی محرک در رشد و توسعهٔ جوامع بشری به‌شمار می‌آید که این فناوری نوین زمینه‌ساز نوعی رسانه اجتماعی شده است. این رسانه با دارا بودن ویژگی تعاملی، فضای نوینی به نام فضای مجازی را در عرصهٔ کنشگری ایجاد کرده است. از آنجا که فضای مجازی یک رسانهٔ ارتباطی منحصربه‌فرد است، شهروندان نه صرفاً مصرف‌کنندگان محتوا، بلکه خالقان محتوا نیز هستند. بنابراین محتوای فضای مجازی به همان اندازه که تفکر انسانی متفاوت است، متنوع شده است. تأثیر دسترسی و استفاده از این رسانهٔ تعاملی جهانی، ارتقا و دفاع از حقوق مدنی– سیاسی و حقوق اقتصادی در سراسر جهان است. ازاین‌رو، ارتباط حیاتی بین فضای مجازی و حقوق بشر وجود دارد. ازآنجاکه حقوق بشر حقوقی غیرقابل نقض و ذاتی هر انسان شمرده می‌شود، این حقوق نیز باید در فضای مجازی همانند فضای فیزیکی ترویج و حمایت شوند. بدیهی است برخورد بالقوه‌ای بین قوانین حمایت از حقوق بشر و اصل جریان نامحدود اطلاعات در فضای مجازی وجود دارد. یکی از مهم‌ترین حقوق بشرِ متأثر از ارتباط اینترنتی، حریم خصوصی است؛ لذا اتخاذ مدل تنظیم‌گری مطلوب در راستای حمایت از حقوق مذکور از ضروریات موضوع مورد بحث است. در این مقاله، استدلال می‌شود که مدل مطلوب تنظیم‌گری محتوای فضای مجازی، مدل تنظیم‌گری مشارکتی است. این مدل از تنظیم‌گری بر یک چارچوب قانونی استوار است که بر پایهٔ آن نهادهای خصوصی امور خود را به‌وسیلهٔ کدهای رفتاری یا مجموعه‌ای از قوانین سامان می‌دهند که می‌توان از رابطهٔ هم‌زیستی قانون، هنجارهای اجتماعی و معماری اینترنت در این مدل از تنظیم‌گری بهره‌برداری نمود تا نتیجه‌ای هم‌افزایانه قابل‌تحقق باشد.

کلید واژگان:

فضای مجازی، تنظیم‌گری، حقوق بشر، حریم خصوصی.

* دانش‌آموخته دکتری حقوق عمومی، دانشکده حقوق، دانشگاه شهید بهشتی
saeede.mazinani@yahoo.com

مقدمه

حریم خصوصی و حفاظت از داده برای صاحبان صنایع، دولت‌ها و عموم جامعه معانی مختلفی دارد و برخلاف سایر حوزه‌های حقوقی که مفاهیم، هنجارها و اصول حقوقی کاملاً ملموس و جاافتاده‌ای را به اذهان متبادر می‌سازد، این حوزه از قوانین درحال‌حاضر اصلاً تثبیت نشده است. بیش از ۴۰ سال قبل، زلمن کوون[1] گفت که انسانِ بدون حریم خصوصیْ هیچ منزلتی ندارد. بااین‌حال، موضوعاتی نظیر حریم خصوصی و حفاظت از داده برای دولت، جامعه و صنعت به‌شدت چالش‌برانگیزند که در اقتصاد دیجیتالی نوین بیش از هر زمان دیگری مطرح می‌شوند؛ اقتصادی که در آن روزانه میلیون‌ها نفر به اینترنت دسترسی دارند و نمی‌دانند حریم خصوصی‌شان محترم شمرده یا برعکس نادیده انگاشته می‌شود.[2]

حریم خصوصی به سه روش توصیف می‌شود: نخست، حریم خصوصی در برخی از وضعیت‌ها و انتخاب‌های مهمی که خودِ فرد در آن‌ها تعیین‌کننده است؛ دوم، حریم خصوصی در اطلاعات شخصی و سوم، حریم خصوصی در ارتباط با فضای شخصی و بدن فرد.[3]

مسلماً حریم خصوصیِ فرد زمانی به خطر می‌افتد که دیگران دربارهٔ آن فرد اطلاعاتی به دست بیاورند، توجه خود را به او معطوف کنند یا به او دسترسی فیزیکی پیدا کنند و ازاین‌رو حریم خصوصی از محرمانگی، ناشناخته بودن و تنهایی فرد محافظت می‌کند.[4]

در این مقاله به زمینهٔ حریم خصوصی اطلاعات پرداخته می‌شود که عبارت است از حقوق افراد برای کنترل اطلاعات شخصی خود که توسط دیگران گردآوری شده‌اند. در ادامه به این موضوع پرداخته می‌شود که چطور نظام‌های حقوقی موضوع بحث حریم خصوصی را رعایت می‌کنند. همچنین تلاش خواهد شد رویکرد ایران، ایالات‌متحده آمریکا و اروپا در این زمینه با هم مقایسه شود. پرسش اصلی این مقاله آن است با توجه به آنکه از دست رفتن حریم خصوصی به‌عنوان یکی از مصادیق شکست بازار است، آیا مداخلهٔ دولت و قوانین جامع در این حوزه روشی

1. Zelman Cowan
2. Kang, J.," Information Privacy in Cyberspace Transactions", *Stanford Law Review*, 1998, p 1201.
3. Chesterman, S., "After Privacy: The Rise of Facebook, the Fall of WikiLeaks, and Singapore's Personal Data Protection Act 2012", *Singapore Journal of Legal Studies*, 2012, p 396.
4. Ibid, p397.

کارآمد برای مواجهه با این شکست خواهد بود یا روش‌های جایگزین آن روش مناسبی محسوب می‌شود؟

ازاین‌رو در این مقاله اصول حاکم بر حریم خصوصی در فضای مجازی از منظر سازمان همکاری و توسعهٔ اقتصادی تجزیه‌وتحلیل، و سپس روش‌های تنظیم‌گری این حوزه بررسی خواهد شد.

۱. اصول حاکم بر حریم خصوصی در فضای مجازی

دستورالعمل سازمان همکاری و توسعهٔ اقتصادی در زمینهٔ حفاظت از حریم خصوصی و جریانات فرامرزیِ دادهٔ شخصی که در ۲۳ سپتامبر ۱۹۸۰ به تصویب رسید و در سال ۲۰۱۳ اصلاح شد، بیانگر اتفاق‌نظر در سطح بین‌المللی برای راهبردهای کلی در خصوص جمع‌آوری و مدیریت اطلاعات شخصی است. این دستورالعمل، با تشریح اصول اساسی، به دولت‌ها و شرکت‌ها و نماینده‌های مصرف‌کنندگان برای حفاظت از حریم خصوصی و داده‌های شخصی کمک مهمی می‌کند و نیز در رفع محدودیت‌های غیرضروری درخصوص جریانات فرامرزی داده، به‌صورت آنلاین و آفلاین، نقش قابل‌توجهی دارد.[۱]

این اصول که اقدامات مناسبِ اطلاعاتی محسوب می‌شوند و کمیسیون تجارت فدرالْ آن را به اجرا گذاشته، بدین شرح است:

۱.۱. اصل محدودیت تحصیل داده[۲]

این اصل خود به اصول فرعی ذیل تقسیم می‌شود که در ادامه بدان اشاره می‌شود:

۱.۱.۱. اصل تحصیل قانونی و منصفانه[۳]

باید محدودیت‌هایی برای جمع‌آوری داده‌های شخصی وجود داشته باشد و چنین داده‌هایی باید از طریق قانونی و منصفانه‌ای به دست آید و هرجا که مقتضی باشد، این داده با اطلاع یا رضایت فرد تحصیل شود.[۴]

1. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, available At:
http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.8/8/2019/
2. Data Collection Limitation
3. Fair and Law Full Collection
4. Ibid, p 24.

۱.۱.۲. اصل تحصیل مضیق[1]

اهداف جمع‌آوری داده‌های شخصی نباید پس از زمان جمع‌آوری داده مشخص شود و استفاده از آنها باید محدود به اجرای همان اهداف شود یا محدود به یا سایر اهدافی باشد که با اهداف مشخص‌شده سازگاری داشته باشد. اصل محدودسازی استفاده مقرر می‌کند که داده‌های شخصی نباید افشا شود یا در دسترس دیگران گذاشته شود یا برای اهدافی غیر از اهداف مشخص‌شده به کار برود، مگر با رضایت کاربر یا توسط مقامات قانونی.[2]

۱.۱.۳. اصل انتخاب[3]

اصل انتخاب بدان معناست که شرکت ارائه‌دهندهٔ خدمات اینترنت که قصد گردآوری داده‌های کاربر را دارد، مکلف است که امکانات لازم را برای اعلام صریح رضایت کاربر مبنی بر اینکه آیا با گردآوری داده‌های خود موافقت دارد یا خیر؟ فراهم کند. این عمل از طریق یک روش انتخاب صورت می‌گیرد که ممکن است مبتنی بر روش سلبی[4] بوده یا از طریق روش ایجابی[5] صورت گیرد.

۱.۱.٤. اصل اطلاع[6]

اصل اطلاع در هر دو مرحلهٔ تحصیل و همچنین مرحلهٔ به‌کارگیری داده‌ها به کار می‌رود. به‌موجب این اصل، شرکت ارائه‌دهندهٔ خدمات اینترنت ملزم است که گردآوری پردازش داده‌ها را به شخص کاربر اطلاع دهد، مگر در مواردی که قانون بنا به پاره‌ای مصالح استثنایی، مانند مسائل امنیتی، خلاف آن را مقرر دارد. بر مبنای این اصل، شرکت ارائه‌دهندهٔ خدمات اینترنت باید هویت شرکت خود، دلیل گردآوری و پردازش داده‌ها و حقوق کاربر را به وی اطلاع دهد.[7]

۱.۲. اصول مربوط به نگهداری داده‌ها

این قسمت به نگهداری داده‌ها توسط شرکت‌های ارائه‌دهندهٔ خدمات مرتبط است.

1. Use Limitation Principle
2. OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, Op Cit, p 23.
3. Opt Principle
4. Opt-Out
5. Opt-In
6. Notice Principle
7. Ibid, p 16.

۱.۲.۱. اصل امنیت

هم‌اینک، اقلیت قاطعی از سایت‌ها به بحث امنیت در خط‌مشی‌های حریم خصوصی می‌پردازند.

۱.۲.۲. اصل شفافیت[1]

شفاف‌سازی یکی از بهترین روش‌های نظارت بر فعالیت شرکت‌های ارائه‌دهندهٔ خدمات اینترنتی است. براساس این اصل، شرکت ارائه‌دهندهٔ خدمات اینترنتی مکلف است که رویهٔ خاص حمایتی خود را از حریم خصوصی کاربران به‌نحو شفاف و قابل فهم در دسترس کاربران قرار دهد.

۱.۲.۳. اصل دسترسی[2]

اصل دسترسی مقرر می‌کند که سایت‌ها دسترسی کاربران به داده‌های شخصی‌شان را که در سایت ذخیره شده است، فراهم کنند.

۱.۳. اصول مربوط به به‌کارگیری داده‌ها

این اصول ناظر بر چگونگی به‌کارگیری داده‌ها است.

۱.۳.۱. اصل پردازش مرتبط

برمبنای این اصل شرکت ارائه‌دهندهٔ خدمات اینترنتی مکلف است که در حدود قانونی و با توجه به نیاز خود به‌منظور ارائهٔ خدمات اعلام‌شده به کاربر به پردازش داده‌های کاربران بپردازد.[3]

۱.۳.۲. اصل ممنوعیت افشا و توقف انتقال داده به شخص ثالث

باید توجه داشت که اصول منصفانه درخصوص اطلاعات، از انتقال داده به شخص ثالث توسط سایت‌ها ممانعت به عمل نمی‌آورد. این اصولْ مجموعه‌ای اساسی و مشخص از امور برای حفاظت از حریم خصوصی را تجویز نمی‌کنند، بلکه بیشتر تصریح می‌کنند برای هر فعالیتی که سایت در ارتباط با داده انجام می‌دهد، باید رضایت کاربران برای این فعالیت‌ها کسب شده باشد.

1. Transparency Principle
2. Access Principle
3. Kluger, Jeffrey, *Extortion on the Internet; A daring hacker tries to blackmail an e-tailer and sparks new worries about credit-card cybertheft*, TIME, 2000, p 56.

۱.٤. اصول مربوط به امحا و انتقال داده‌ها

پس از گردآوری، نگهداری و پردازش داده‌ها نوبت به انتقال و امحای داده‌ها می‌رسد. اصول حاکم بر این مرحله در قسمت زیر مورد بررسی قرار می‌گیرد:

۱.٤.۱. اصل عدم انتقال[1]

اصل عدم انتقال با توجه به خصیصهٔ فرامرزی و گیتی گستر بودن اینترنت و به‌طورکلی فناوری‌های اطلاعات و ارتباطات تبیین شده است. براساس این اصل، در بحث حریم خصوصی اطلاعاتی، یکی از اصول حاکم و بنیادین که در تمام مراحل باید از سوی ارائه‌دهندهٔ سرویس اینترنت رعایت شود، اصل ممنوعیت انتقال فرامرزی داده‌ها[2] است.[3]

۱.٤.۲. اصل امحا[4]

اصل امنیت که از اصول حاکم بر نگهداری داده‌ها است، اقتضا دارد به‌محض برطرف شدن نیاز شرکت ارائه‌دهندهٔ خدمات اینترنتی، نسبت به پاک کردن آنها اقدام نماید.[5]

۲. تنظیم‌گری حریم خصوصی در فضای مجازی

طی چند سال گذشته، گسترش سریع ارتباطات و تجارت الکترونیکی در سراسر دنیا نگرانی‌هایی را درمورد حریم شخصی در محیط فضای مجازی ایجاد کرده است. این نگرانی‌ها توجه مردم و سیاست‌گذاران را به خود جلب کرده است، لذا کشورهای مختلف رویکردهای متفاوتی را در تنظیم‌گری حریم خصوصی اتخاذ نموده‌اند.

در ایالات‌متحده آمریکا سیاست‌های حفظ حریم خصوصی با اتحادیه اروپا تفاوت بسیاری دارد. در این قسمت از مقاله نحوهٔ تنظیم‌گری کنترل- دستوری (دولتی) در ایران، خودتنظیمی در ایالات‌متحده آمریکا و تنظیم‌گری مشارکتی در اتحادیهٔ اروپا بررسی و تحلیل خواهد شد.

1. Onward Transfer
2. Transborder Data Flow
3. OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, Op Cit, p 16.
4. Erase Principle
5. Ibid, p15.

۲.۱. رویکرد ایران: تنظیم‌گری کنترل- دستوری حریم خصوصی در فضای مجازی

در قانون اساسی ایران لفظ حریم خصوصی به کار برده نشده؛ اما به‌صورت موردی و بدون ذکر نام حریم خصوصی، در برخی از اصول به حمایت از بخشی از آن پرداخته شده است. اگر حریم خصوصی به حوزه‌های حریم خلوت و تنهایی، حریم مکانی، حریم اطلاعاتی، حریم ارتباطات و حریم جسمانی طبقه‌بندی شوند، قانون‌گذار در اصل بیست‌ودوم قانون اساسی به آن اشاره می‌کند. مهم‌ترین اصلی که مربوط به بحث بوده و به‌صراحت تمام به ممنوعیت تجاوز به حریم خصوصی افراد اشاره می‌کند، اصل بیست و پنجم قانون اساسی است. در این اصل بدون آنکه به آزادی ارتباطات تصریح‌شده باشد، به استثنائات این آزادی اشاره شده و از حریم خصوصی ارتباطات درمورد شایع‌ترین وسایل ارتباطی حمایت شده است.[۱]

در این راستا، لازم به ذکر است که در راستای اصل ۱۳۴ قانون اساسی، منشور حقوق شهروندی در سال ۱۳۸۵ مورد تصویب رئیس‌جمهوری وقت قرار گرفت. یکی از مهم‌ترین ویژگی‌های این منشور، تمرکز صرف بر حقوق و آزادی‌های فردی و اجتماعی شهروندان، با در نظر داشتن معیارهای شرعی و عرفی جامعه است. از جمله حقوق و آزادی‌های مصرح در آن حمایت از حریم خصوصی و امنیت داده‌ها است که در مادۀ ۳۵ آن مورد تصریح قرار گرفته است. در مادۀ ۳۷ و ۳۹ آن به اصل ممنوعیت جمع‌آوری و انتشار داده‌های اشخاص و در مادۀ ۳۸ آن به اصل رضایت در جمع‌آوری اطلاعات خصوصی شهروندان اشاره شده است.[۲] ازآنجاکه موضوع حمایت از حریم خصوصی و امنیت داده‌ها در فضای مجازی باید هم از منظر فنی و هم از منظر حقوق و تعهدات بازیگران درخصوص انواع داده‌ها مورد توجه و تنظیم گری قرار بگیرد، با استناد به قوانین و مقررات موجود در این حوزه، متولی تعیین الزامات و استانداردهای فنی دربارۀ تأمین امنیت بسترهای فنی نظیر بسترهای ذخیره‌سازی، انتقال و پردازش داده‌ها، ازجمله مراکز داده بر عهدۀ وزارت ارتباطات و فناوری اطلاعات است که این وزارتخانه از طریق کمیسیون تنظیم مقررات ارتباطات با وضع استانداردهای و مصوبات متعدد امنیت داده‌ها و حریم خصوصی را از منظر ابعاد فنی آن تأمین می‌نماید. اما درخصوص قسمت دوم، یعنی حقوق و تعهدات بازیگران

۱. انصاری، باقر، «حریم خصوصی و حمایت از آن در حقوق اسلام– تطبیقی و ایران»، **مجله دانشکده حقوق و علوم سیاسی**، ش ۶۶، زمستان ۸۳، ص۳۷.

2. http://citizensrights.ir/. 6/7/2019.

دربارهٔ انواع داده‌ها، اصل پردازش و مواردی از این قبیل در ایران خلأ قانونی وجود دارد؛ این در حالی است که در نظام حقوقی سایر کشورها، قانونی تحت عنوان قانون حمایت از داده وجود دارد که در آن، حقوق و تعهدات کنترل‌کنندگان و پردازشگران، کاربران، اصول حاکم بر پردازش و ضمانت اجراهای تخطی از آن عنوان شده است. در ایران جز لایحهٔ حمایت از حریم خصوصی متن خاصی که حمایت کافی و وافی از حریم خصوصی ارائه کرده باشد، وجود ندارد. این لایحه در سال ۱۳۸۴ و در اواخر دولت هشتم تقدیم مجلس شد که حرکتی روبه‌جلو و بسیار مثبت بود. مجلس شورای اسلامی و مرکز پژوهش‌های مجلس نیز از این لایحه استقبال خوبی داشتند. اما متأسفانه قبل از رسیدگی و تصویب آن، در فروردین سال ۱۳۸۵ توسط دولت جدید (دولت نهم) استرداد شد و از آن زمان مجلس و دولت یازدهم پیگیری در این موضوع نداشتند. این لایحه در ۴ سرفصل، به «حریم خصوصی جسمانی »، «حریم خصوصی اماکن و منازل»، «حریم خصوصی در محل کار»، « حریم خصوصی اطلاعات»، « اطلاعات شخصی در فعالیت‌های رسانه‌ای»، «حریم خصوصی ارتباطات» و مسئولیت‌های ناشی از نقض حریم خصوصی پرداخته بود.

در فصل مربوط به «حریم خصوصی اطلاعات» بیان گردیده است که اولاً، اطلاعات شخصی افراد تا حد امکان باید توسط خود اشخاص جمع‌آوری شود و استفاده از روش‌های غیرمتعارف برای این موضوع، ممنوع است.

ثانیاً، مؤسسات عمومی و خصوصی که خدمات عمومی ارائه می‌دهند، برای جمع‌آوری اطلاعات شخصی افراد یابد، آزادی افراد در ارائهٔ اطلاعات یا ملزم بودن قانونی آنها به ارائهٔ آن، هویت مؤسسهٔ جمع‌آوری‌کنندهٔ اطلاعات، امکان یا عدم امکان دسترسی خود فرد به اطلاعات جمع‌آوری‌شده، اهداف این کار و نتایج عدم ارائهٔ اطلاعات از سوی فرد را به اطلاع او برساند. همچنین براساس مادهٔ ۳۱ از این لایحه، مؤسسات یادشده باید اطلاعات شخصی افراد را تنها برای هدف اولیه جمع‌آوری آنها به کار برند و نمی‌توانند برای اهداف و مقاصد دیگری از آنها استفاده کنند یا آنها را در اختیار دیگران قرار دهند.

براساس مادهٔ ۳۵ نیز «افرادی که اطلاعات شخصی آنها در مؤسسات مشمول این قانون نگهداری می‌شود، حق دسترسی به اطلاعات مذکور را به نحو موردنظر خود دارند و مؤسسه مکلف به قبول درخواست آنهاست، مگر اینکه دسترسی به اطلاعات تهدید به حیات و سلامتی

فرد ایجاد کند و یا آنکه اصولاً دسترسی به آن اطلاعات طبق قانون، ممنوع باشد.» روشن است که به لحاظ عدم تصویب این لایحه موارد ذکرشده در آن مورد حمایت قانون‌گذار نخواهد بود و دارای اعتبار نخواهد بود.[1]

البته قانون‌گذار ایران به‌طور پراکنده به حمایت از حریم خصوصی و حمایت از داده‌ها در قوانین و مقررات داخلی پرداخته است. درحال‌حاضر دو سند قانونی به نام‌های « قانون تجارت الکترونیک» و «قانون جرائم رایانه‌ای» تنها قوانینی هستند که مواردی را درباب داده‌های شخصی مورد اشاره قرار داده‌اند و ازاین‌رو ضروری است مورد بحث و تحلیل قرار گیرند. در این راستا لازم به ذکر است قانون تجارت الکترونیکی تا حد زیادی خلأ موجود در حوزهٔ حمایت از داده‌ها را برطرف کرده است؛ اما باید توجه شود که قانون تجارت الکترونیکی خاص داده‌های شخصی در فضایی تجاری است و درخصوص تأمین امنیت داده‌ها در فضای غیرتجاری مقررهٔ خاصی در نظام حقوقی کشور وجود ندارد.

۲.۱.۱. قانون تجارت الکترونیک

در ابتدا باید به این نکته اشاره کرد که قانون تجارت الکترونیک که در سال ۱۳۸۳ به تصویب مجلس شورای اسلامی رسیده است. این قانون اولین و مهم‌ترین متن قانونی در باب حمایت از داده‌های شخصی در فضای مجازی است و به دلیل اینکه برگرفته از قوانین نمونهٔ کمیسیون حقوق تجارت بین‌المللی سازمان ملل متحد (آنسیترال)[2] است، سند قانونی مناسبی تلقی می‌گردد.

در مادهٔ ۵۸ این قانون به اصل رضایت در جمع‌آوری و پردازش اطلاعات وضعیت جسمانی، روانی یا جنسی اشخاص اشاره می‌کند.[3] مادهٔ ۵۹ نیز اذعان می‌دارد: «درصورت رضایت شخص موضوع «داده‌پیام» نیز به‌شرط آنکه محتوای داده‌پیام وفق قوانین مصوب مجلس شورای اسلامی باشد، ذخیره، پردازش و توزیع داده‌پیام‌های شخصی در بستر مبادلات الکترونیکی باید با لحاظ شرایط زیر صورت پذیرد: الف) اهداف آن مشخص بوده و به‌طور واضح شرح داده شده باشند؛ ب) داده‌پیام باید تنها به‌اندازهٔ ضرورت و متناسب با اهدافی که در هنگام جمع‌آوری برای شخص

1. https://rc.majlis.ir/fa/legal_draft/show/809338. 6/6/2019.
2. The United Nations Commission on International Trade Law
۳. آقایی طوق، مسلم و مهدی ناصر، «چالش‌های حفاظت از داده‌های خصوصی در حوزه اینترنت اشیا: مطالعه تطبیقی حقوق ایران و اتحادیه اروپا»، *فصلنامه حقوق اداری*، سال هفتم، ش ۲۳، تابستان ۹۹، ص ۴۰.

موضوع داده‌پیام شرح داده شده است، جمع‌آوری گردد و تنها برای اهداف تعیین‌شده مورداستفاده قرار گیرد؛ ج) داده‌پیام باید صحیح و روزآمد باشد؛ د) شخص موضوع داده‌پیام باید به پرونده‌های رایانه‌ای حاوی داده‌پیام‌های شخصی مربوط به خود دسترسی داشته و بتواند داده‌پیام جای ناقص یا نادرست را محو یا اصلاح کند؛ ه) شخص موضوع داده‌پیام باید بتواند در هر زمان با رعایت ضوابط مربوطه درخواست محو کامل پروندهٔ رایانه‌ای داده‌پیام‌های شخصی مربوط به خود را بنماید.»

مواد ۷۱ و ۷۲ نیز به بیان مجازات نقض موارد ذکرشده پرداخته است.[۱] در این راستا درمجموع مطالب مذکور جدول زیر انطباق اصول حاکم بر حمایت از داده در سازمان همکاری و توسعه اقتصادی را با مواد قانون تجارت الکترونیک نشان می‌دهد:

اصول حاکم بر حفاظت از داده‌های شخصی		متن قانونی: «قانون تجارت الکترونیک» مصوب ۲۴ دی ۱۳۸۲ مجلس شورای اسلامی
اصول مربوط به تحصیل داده‌ها	اصل تحصیل قانونی و منصفانه	بند ب ماده ۵۹: «داده‌پیام» باید تنها به‌اندازه ضرورت و متناسب با اهدافی که در هنگام جمع‌آوری برای شخص موضوع «داده‌پیام» شرح داده‌شده است، جمع‌آوری گردد و تنها برای اهداف تعیین‌شده مورداستفاده قرار گیرد.
	اصل تحصیل مضیق و مرتبط	بند ب ماده ۵۹
	اصل انتخاب	–
	اصل رضایت	ماده ۵۸: ذخیره پردازش و یا توزیع «داده‌پیام»های شخصی مبین ریشه‌های قومی یا نژادی، دیدگاه‌های عقیدتی، مذهبی، خصوصیات اخلاقی و «داده‌پیام»های راجع به وضعیت جسمانی، روانی و یا جنسی اشخاص بدون رضایت صریح آنها به هر عنوان غیرقانونی است.
	اصل اطلاع	ماده ۵۸
اصول مربوط به	اصل امنیت	–
	اصل شفافیت	–

۱. زرکلام، ستار، «حریم خصوصی ارتباطات اینترنتی (مطالعه در حقوق ایران و اتحادیه اروپا)،» *پژوهش نامه حقوق اسلامی*، ش ۲۵، ۱۳۸۶، صص ۱۸۰-۱۸۱.

نگهداری داده‌ها	اصل دسترسی	بند د ماده ۵۹: شخص موضوع «داده‌پیام» باید به پرونده‌های رایانه‌ای حاوی «داده‌پیام»های شخصی مربوط به خود دسترسی داشته و بتواند «داده‌پیام»های ناقص یا نادرست را محو یا اصلاح کند.
	اصل صحت	بند ج ماده ۵۹: «داده‌پیام» باید صحیح و روزآمد باشد.
اصول مربوط به به‌کارگیری داده‌ها	اصل پردازش	–
	اصل ممنوعیت افشاء	–
اصول مربوط به امحا و انتقال داده‌ها	اصل عدم انتقال	–
	اصل امحاء	بند ه ماده ۵۹: شخص موضوع «داده‌پیام» باید بتواند در هر زمان با رعایت ضوابط مربوطه درخواست محو کامل پرونده رایانه‌ای «داده‌پیام»های شخصی مربوط به خود را بنماید.

گرچه بر طبق جدول بالا، قانون‌گذار به اصول مهمی از اصول حاکم بر حمایت از داده اشاره کرده، اصول دیگری چون اصل امنیت، اصل شفافیت، اصل عدم انتقال، اصل پردازش مرتبط و اصل ممنوعیت افشا مورد توجه قرار نگرفته است.

از طرف دیگر، اگرچه برخی از اصول حاکم بر داده‌های شخصی در این قانون بیان شده است، همهٔ مقتضیات آن اصل به شکل کامل مورد اشاره قرار نگرفته است. به‌عنوان مثال، اگرچه در مادهٔ ۵۸ اصل تحصیل قانونی، اصل اطلاع و اصل رضایت به‌صراحت ذکر شده، مستثنیات آن پیش‌بینی نشده و در مادهٔ ۶۱ به آیین‌نامه‌ای واگذار شده که بعد از گذشت حدود پانزده سال از تصویب این قانون، نوشته نشده است.

۲.۱.۲. قانون جرائم رایانه‌ای

مادهٔ ۱ این قانون، نقض اصل تحصیل مجاز و مشروع را جرم‌انگاری کرده است. ایـن ماده با هدف حمایت همه‌جانبه از اقدام اشخاص در اتخاذ تدابیر امنیتی برای سیستم یا داده‌های خود، دسترسی غیرمجاز را به‌صورت ساده جرم‌انگاری کرده است.

مادۀ ۲ این قانون نیز نقض اصل تحصیل منصفانه داده‌ها را جرم‌انگاری نمـوده است. در این راستا لازم به توضیح است، شنود در فضای مجازی به‌معنای دریافت داده‌های در حـال انتقـال یـا بـه هـر نحـوی دسترسی به آنهاست.[۱]

منظور از داده نیز در قانون فوق هـر نمـادی از واقعـۀ اطلاعـات یـا مفاهیم قابل‌پردازش در سیستم رایانه‌ای یا مخابراتی اسـت و گسـترۀ مصـادیق آن بسـیار وسیع است. منظور از ارتباطات غیرعمومی، ارتباطی است که در مرئی و منظر عموم نباشـد و همگان از محتوای داده‌های در حال انتقال اطلاع نیابند.

مادۀ ۱۷ این قانون نیز نقض اصول راجع به افشا و انتقال داده‌ها را جرم‌انگاری کرده است.[۲] لازم به ذکر است، در پیش‌نویس‌های لایحۀ این قانون، دامنۀ مصادیق اسرار شخصی گسترده‌تر بود، ولی در متن قانون از شمول حمایت خارج شده و فقط صوت، تصویر و فیلم مشمول مواد فوق قرار گرفته‌اند. مفهوم منطوق این ماده آن است که شـخص منتشرکننده باید رضایت شخص را قبل از انتشار صوت یا تصویر یا فیلم خصوصـی یـا خـانوادگی وی به دست آورد و این رضایت باید در زمان انتشار به‌دست‌آمده باشـد و ایـن تکلیف بر عهدۀ منتشرکنندۀ اطلاعات فوق است و نباید تصور شود که صاحب اسرار باید عدم رضایت خود را در انتشار یا در دسترس قرار دادن اسرار خصوصی بـه منتشرکننده اعلام کند. این جرم نیز جرمی مقید است و باید ایراد ضرر یا هتک حیثیـت عرفـی در آن صورت گیرد.[۳] براین اساس، می‌توان گفـت کـه ایـن مـاده، از حـریم خصوصی به‌عنوان حریم خصوصی حمایت نکرده است، بلکه درصورتی‌که اعمال مذکور منجر به ضرر یا هتک حیثیت عرفی شخص گردد، از حقوق وی حمایت می‌کند.

۱. فتحی، یونس و خیراله شاهمرادی، «گستره و قلمرو حریم خصوصی در فضای مجازی»، *مجله حقوقی دادگستری*، سال هشتاد و یکم، ش ۹۹، ۱۳۹۶، ص ۲۴۱.

۲. *همان*، صص ۲۴۱-۲۴۲.

۳. محسنی، فرید، حریم خصوصی اطلاعات: مطالعه تطبیقی در فقه امامیه، حقوق کیفری ایران و ایالات متحده آمریکا، تهران: انتشارات دانشگاه امام صادق، ۱۳۸۹، ص ۵۷۵.

اصول مربوط به تحصیل داده‌ها		قانون جرایم رایانه‌ی
اصول مربوط به تحصیل داده‌ها	اصل تحصیل قانونی و منصفانه	*
	اصل تحصیل مضیق	–
	اصل انتخاب	–
	اصل اطلاع	–
	اصل رضایت	*
اصول مربوط به نگهداری داده‌ها	اصل شفافیت	–
	اصل امنیت	–
	اصل صحت	–
	اصل دسترسی	–
اصول مربوط به به‌کارگیری داده‌ها	اصل پردازش مرتبط	–
	اصل ممنوعیت افشا	*
اصول مربوط به امحا و انتقال داده‌ها	اصل عدم انتقال	*
	اصل امحا	–

۲.۱.۳. سایر مقررات

تعدادی از آیین‌نامه‌ها که در این حوزه تصویب شده‌اند، به موضوع حریم خصوصی نیز اشاره داشته‌اند؛ ازجمله آن می‌توان به آیین‌نامهٔ فعالیت پایگاه‌های اطلاع‌رسانی (سایت‌های) اینترنتی ایرانی اشاره کرد که این آیین‌نامه در سال ۱۳۸۵ به تصویب هیئت‌وزیران رسیده است. در مادهٔ ۷ فصل سوم آن که به تخلفات موضوع این آیین‌نامه اشاره می‌نماید، در بند (د) به ممنوعیت انتشار اطلاعات و داده‌های خصوصی کاربران بدون اخذ رضایت آنها تصریح کرده است. همچنین در آیین‌نامهٔ واحدهای ارائه‌کنندهٔ خدمات اطلاع‌رسانی و اینترنت رسا که در سال ۱۳۸۰ به تصویب شورای عالی انقلاب فرهنگی رسیده است، نیز در موضوع مسئولیت قانونی رساها در بند ۱۵–۳–۵ به موضوع ممنوعیت دسترسی به اطلاعات و داده‌های شخصی کاربران و به ممنوعیت انتشار روابط خصوصی افراد در بند ۱۳–۶ مادهٔ ۶ تصریح شده است. در اصول و سیاست‌های حاکم بر

مجوز خدمات سلامت در فضای مجازی که توسط کمیسیون عالی تنظیم مقررات فضای مجازی، در جلسات مورخ ۱۳۹۲/۲/۲۸ و ۱۳۹۲/۳/۱۱ در راستای بندهای ۲، ۴ و ۶ شرح وظایف خود (ابلاغیه شماره ۰۱/۹۱۱۶۰/ش مورخ ۱۳۹۱/۷/۸) و همچنین در راستای ارتقای خدمات داخلی فضای مجازی و توسعهٔ کاربرد شبکه ملی اطلاعات به تصویب رسیده، نیز در مادهٔ ۳ آن به رعایت امنیت اطلاعات کاربران اشاره شده است.

اصول مربوط به تحصیل داده‌ها		آیین‌نامه سامان‌دهی فعالیت پایگاه‌های اطلاع‌رسانی (سایت‌های) اینترنتی ایرانی	آیین‌نامه واحدهای ارائه‌کننده خدمات اطلاع‌رسانی و اینترنت رسا ISP	اصول و سیاست‌های حاکم بر مجوز خدمات سلامت در فضای مجازی
اصول مربوط به تحصیل داده‌ها	اصل تحصیل قانونی	–	*	–
	اصل تحصیل مضیق	–	–	–
	اصل انتخاب	–	–	–
	اصل اطلاع	–	–	–
	اصل رضایت	*	*	–
اصول مربوط به نگه‌داری داده‌ها	اصل شفافیت	–	–	–
	اصل امنیت	–	–	*
	اصل صحت	–	–	–
	اصل دسترسی	–	–	–
اصول مربوط به به‌کارگیری داده‌ها	اصل پردازش مرتبط	–	–	–
	اصل ممنوعیت افشا	*	*	*
اصول مربوط به امحا و انتقال داده‌ها	اصل عدم انتقال و امحا داده‌ها	–	–	–

۲.۲. رویکرد ایالات متحده امریکا: خودتنظیمی حریم خصوصی در فضای مجازی

تقریباً در تمامی جوامع دموکراتیک، سیستم قانونی، حق حریم خصوصی افراد را به رسمیت می‌شناسد. اهمیت ویژهٔ این امر تأمین امنیت افراد در برابر فعالیت‌های مداخله‌گرانه و نفوذی دیگران است. در ایالات‌متحده، مسئلهٔ حریم خصوصی ریشه‌های قانونی مرسومی دارد.[۱] کنگرهٔ ایالات‌متحده آمریکا شروع به تصویب قوانینی برای حفاظت از حریم خصوصی کرد. این قوانین ابتدایی بر استفاده دولت از اطلاعات متمرکز بودند که در آن زمان، دغدغهٔ شدیدتری به‌حساب می‌آمد. در سال ۱۹۷۰، کنگره قانون گزارش عادلانه اعتبارات[۲] را وضع کرد که افشای اطلاعات مالی و اعتباری افراد توسط ادارات اعتباری را قانونمند و محدود ساخت. این قانون حقوق معینی را به مصرف‌کنندگان داد؛ ازجمله موارد ذیل:

۱. حق دسترسی به فایل‌های اعتباری خود،

۲. امکان درخواست بازرسی اطلاعات نادرست و حق اظهارنظر دربارهٔ اختلافات.

مدت کوتاهی پس از آن، قانون حفظ حریم خصوصی فدرال در سال ۱۹۷۴ تدوین شد که مؤسسات دولتی را در نگهداری سوابق محدود می‌ساخت و در سال ۱۹۷۸، کنگره در ایالات‌متحده آمریکا قانون حریم خصوصی مالی را تصویب کرد. این قانون بانک‌ها را ملزم می‌ساخت پیش از افشای داده‌های مالی مشتریان خود به نهادهای فدرال، از مشتریان اجازه بازرسی بگیرند. در این قوانین، مطالبات مربوط به حریم خصوصی در قالب چارچوبی قانونی ترجمه شدند و حق قانونی افراد راجع به حریم خصوصی چشمگیرتر و مهم‌تر شد.[۳]

در دههٔ ۱۹۸۰، کنگره وضع قوانین مشابه را ادامه داد؛ به این امید که حقوق حریم خصوصی شهروندان ایالات‌متحده را رسمی کند. در سال ۱۹۸۴، قانون سیاست‌های ارتباطات کابلی[۴] را تصویب کرد که شرکت‌های تلویزیون کابلی را از گردآوری یا انتشار داده‌های مربوط به عادات تماشای تلویزیون مشتریانشان منع می‌کرد. قانون مرتبط دیگر قانون حفظ حریم خصوصی ویدیویی[۵] مصوب سال ۱۹۸۸ بود که کلوپ‌های کرایهٔ ویدیو را از افشای لیست ویدیوهایی که

1. Warren, Samuel D., Brandeis, Louis D., "The Right to Privacy", *Harvard Law Review*, Vol. 4, No. 5, 1890, p 205.
2. Fair Credit Reporting Act(FCRA)
3. *Ibid*, p 1196.
4. Cable Communictions Policy Act
5. Video Privacy Act

مشتریانش تماشا کرده بودند، بازمی‌داشت. برخی معتقد بودند که قانون حریم خصوصی ویدیویی واکنشی مبالغه‌آمیز بوده است؛ اما دلایل محکمی در پس حفاظت از این نوع اطلاعات وجود دارد.

در سال ۱۹۹۸، کنگره قانون حفاظت از حریم شخصی آنلاین کودکان[1] را تصویب کرد. این قانون وب‌سایت‌ها را از گردآوری اطلاعات شخصی کودکان زیر سیزده سال بدون رضایت والدینشان منع می‌کند. رضایت والدین به روش‌های مختلف ارائه می‌گردد: یادداشتی با امضای دستی واقعی، شماره کارت اعتباری یا پیام ایمیلی حاوی گذرواژه. اغلب متخصصان حریم خصوصی و شهروندان عادی حس می‌کردند که این قانون باید مدت‌ها پیش وضع می‌شد و این قانون مشکلی جدی را حل کرده است؛ اما اعمال قانون چندان ساده نبوده است. بسیاری از وب‌سایت‌های کودک‌محور صرفاً متن قانون را رعایت می‌کنند: به این صورت که یا اعلان‌هایی را بر روی سایت پست می‌کنند، مبنی بر اینکه سایت برای کودکان نیست یا امکان دروغ گفتن کودکان دربارهٔ سنشان را بسیار ساده می‌سازند.[2] در سال ۲۰۰۰، کمیسیون تجارت فدرال آمریکا «مروری» بر روی این سایت‌های کودک‌محور انجام داد و «پی برد که تنها حدود نیمی از این سایت‌ها سیاست‌های حریم خصوصی خود را پست کرده و رضایت والدین را نیز طبق قانون کسب کرده‌اند».[3] چرا قوانین جامع‌تر و فراگیرتری برای حفاظت کلیه انواع اطلاعات وجود ندارند؟ چرا اطلاعات سادهٔ مصرف‌کنندگان، اطلاعات مربوط به تراکنش‌های اینترنتی در هیچ‌یک از این قوانین حفاظتی لحاظ نشده‌اند؟ این امر دلایل مختلفی دارد. برای مثال، دولت کلینتون از سیاست خودتنظیمی در مباحث حریم خصوصی استقبال کرد. بیانیهٔ راهگشای کلینتون درمورد عصر اطلاعات، به نام «چارچوبی برای تجارت الکترونیکی جهانی»[4] که رویکرد حداقلی را در تنظیم‌گری را دنبال می‌کرد، مسئولیت حفاظت از حریم خصوصی را در وهلهٔ اول بر عهدهٔ بخش خصوصی گذاشت، نه دولت. البته برخی موارد استثنا، همچون حریم خصوصی کودکان و حریم خصوصی پزشکی وجود داشت. لذا در دهه‌های اخیر در ایالات‌متحده آمریکا مداخلهٔ دولت به‌عنوان مناسب‌ترین روش تنظیم‌گری حریم خصوصی شناخته نشد و لذا خودتنظیمی به‌عنوان راه جایگزین این روش انتخاب گردید.

1. Children Online Privacy Protection ACT
2. https://www.ftc.gov/tips-advice/business-center/guidance. 7/7/2019.
3. Federal Trade Commission, available at:
http://www.ftc.gov/os/1999/9910/64fr59888.htm.8/7/2019.
4. Global Electronic Commerce

در روش خودتنظیمی حریم خصوصی در فضای مجازی، معماری‌های خاصی وجود دارند که برای حفاظت از حریم خصوصی طراحی شده‌اند و گاه با نام فناوری‌های ارتقای حریم خصوصی[۱] یاد می‌شوند. واضح است که این معماری‌ها نمی‌توانند مسئلهٔ بغرنج و پیچیدهٔ حریم خصوصی را کاملاً حل کنند؛ اما آیا امکان دارد دستگاه‌هایی را ساخت که به کاربران، حد معقولی از کنترل حریم خصوصی را ارائه دهند؟ متداول‌ترین بستر معماری، نرم‌افزار ترجیحات حریم خصوصی[۲] است. نرم‌افزار ترجیحات حریم خصوصی پروتکلی است که کنسرسیوم وب جهان‌گستر[۳] طراحی کرده است؛ این کنسرسیوم مقایسه بین سیاست‌های حریم خصوصی وب‌سایت‌ها و ترجیحات کاربران را درمورد حریم خصوصی استاندارد می‌سازد. پروتکل نرم‌افزار ترجیحات حریم خصوصی شامل قوانینی است که به وب‌سایت‌ها اجازه می‌دهند سیاست‌های حریم خصوصی خود را به زبان قابل‌خواندن توسط ماشین ترجمه کنند.[۴] این سیاست‌ها تعیین می‌کنند آیا سایت از کوکی‌ها استفاده می‌کند یا داده‌ها را با اشخاص ثالث به اشتراک می‌گذارد یا خیر. پروفایل حریم خصوصی کاربران در نرم‌افزار مرورگر ایشان تعبیه شده و موارد استفاده مجاز و غیرمجاز داده‌های شخصی ایشان را تعیین می‌کند. نرم‌افزار ترجیحات حریم خصوصی به کاربران اجازه می‌دهد داده‌های شخصی خود را تنها به سایت‌هایی ارائه کنند که با ترجیحات مذکور سازگارند. اگر مقدار حفاظت حریم خصوصی ارائه‌شده در وب‌سایتی کمتر از مقدار مطلوب کاربر باشد، این نرم‌افزار به وی هشدار می‌دهد و از انتقال اطلاعات شخصی جلوگیری می‌کند؛ اما گزینهٔ نادیده گرفتن ترجیحات حریم خصوصی کاربران و انجام کار برمبنای شرایط فروشنده را نیز ارائه می‌دهد. هدف نرم‌افزار ترجیحات حریم خصوصی توانمندسازی کاربران برای اخذ تصمیمات آگاهانه درمورد تراکنش یا عدم تراکنش کاری با هر وب‌سایت براساس سیاست‌های حریم خصوصی آن وب‌سایت است.[۵]

به‌وضوح، نرم‌افزار ترجیحات حریم خصوصی تنها در صورتی مؤثر خواهد بود که وب‌سایت‌های تجاری این استاندارد را به کار گیرند و سیاست‌های حریم خصوصی خود را به زبان

1. Privacy Enhancing Technology(PET)
2. Platform for privacy preferences (P3P)
3. World Wide Web Consortium
4. Clarke, R., "Platform for Privacy Preferences: A Critique". *Privacy Law & Policy Reporter*, 5(3), 1998, PP 46-48.
5. Electronic Privacy Information Center, Pretty Poor Privacy: An Assessment of P3P and Internet Privacy, 2000.
Avaiable at: https://epic.org/reports/prettypoorprivacy.html.

قابل‌خواندن توسط ماشین‌های مخصوص نرم‌افزار ترجیحات حریم خصوصی بیان کنند. فروشندگان اصلی نرم‌افزار همچون مایکروسافت وزن خود را پشت این استاندارد انداخته‌اند. مایکروسافت این پروتکل را در نسخه ۶ مرورگر اینترنت اکسپلورر[1] خود گنجانده است. به‌علاوه، برخی از بزرگ‌ترین شرکت‌های اینترنتی همچون ای او ال،[2] تایم وارنر،[3] آی بی ام[4] و ای‌تی اند تی[5] تعهدی استوار به نرم‌افزار ترجیحات حریم خصوصی دارند و عهد بسته‌اند وب‌سایت‌های خود را با نرم‌افزار ترجیحات حریم خصوصی سازگار کنند؛ اما دیگر شرکت‌ها، همچون آمازون و دیزنی، درحال‌حاضر از نگرش ایستادن و تماشا کردن استفاده کرده‌اند. قطعاً علاوه بر نرم‌افزار ترجیحات حریم خصوصی، فناوری‌های دیگری نیز برای ارتقای حریم خصوصی وجود دارند. یکی از شرکت‌های نرم‌افزاری نیویورک، با نام پونویی،[6] نرم‌افزاری را توسعه داده است که به وب‌سایت‌ها اجازه می‌دهد دسترسی بی‌نام در اختیار مصرف‌کنندگانشان قرار دهند؛ یعنی بدون نیاز به افشای هویت یا آدرس آی پی خود، به نقل از ریکاردو،[7] «نرم‌افزار پونویی به شرکت‌ها اجازه می‌دهد نوعی ویژگی را بر روی وب‌سایت‌های خود قرار دهند که کاربران را قادر به جست‌وجو و گردآوری اطلاعات در فضایی خصوصی می‌سازد– یعنی بدون اینکه اطلاعات ایشان بر روی هیچ‌یک از رایانه‌های بیرونی ذخیره شوند». نرم‌افزار ترجیحات حریم خصوصی و سایر ابزارهای حریم خصوصی مطمئناً راه‌حلی عام برای حفاظت حریم شخصی نیستند. حتی اگر وب‌سایت‌های تجاری از این معماری به‌طور گسترده‌ای استقبال کنند و کلیهٔ خطاهای آن رفع شود، محدودیت‌هایی دارد. نرم‌افزار ترجیحات حریم خصوصی در شکل کنونی خود تنها ترجیحات عام حریم خصوصی کاربر را غربال‌گری می‌کند و هنوز سؤالاتی راجع به توانایی این پروتکل برای «درک» سیاست‌های عمیق حریم خصوصی وجود دارد. همچنین مناقشه‌ای مداوم بر سر تنظیمات پیش‌فرض نرم‌افزار ترجیحات حریم خصوصی وجود دارد که سطح حداقلی از حریم خصوصی را به‌خصوص برای کاربران ساده‌دل تضمین می‌کند. درمورد مرورگر اینترنت اکسپلورر، مایکروسافت این تنظیمات پیش‌فرض را تعیین می‌کند و برخی از مدافعان حریم خصوصی از این

1. Internet Explore
2. AOL
3. Time Warner
4. IBM
5. AT&T
6. Ponoi
7. Ricardo

روش ایراد می‌گیرند. مشکل این تنظیمات پیش‌فرض آن است که مصرف‌کنندگان باید از سایت‌های مذکور بازدید، و از قرارگیری کوکی صرف‌نظر کنند و برخی افراد ممکن است چنین اقدامی را صورت ندهند.[۱] این نقایص نرم‌افزار ترجیحات حریم خصوصی شک و تردیدهایی راجع به تأثیرگذاری آن به‌عنوان راهکاری معقول و البته جزئی برای حفاظت از حریم شخصی مصرف‌کنندگان ایجاد کرده‌اند.[۲]

پیاده‌سازی مسئولانه و اخلاقی نرم‌افزار ترجیحات حریم خصوصی بدین معناست که اطلاعاتی خاص و شفاف راجع به اشتراک‌گذاری اطلاعات شخصی قابل‌شناسایی مصرف‌کنندگان و نیز کاربردهای اولیه و ثانویه این اطلاعات در اختیار ایشان قرار می‌گیرد.[۳] بنابراین، نرم‌افزار ترجیحات حریم خصوصی این توانایی را دارد که به راه‌حل کد محور قابل دفاعی تبدیل شود؛ چون کاربران را قادر می‌سازد ترجیحات خود را به‌صورت قوانینی بیان کنند و درصورتی‌که ترجیح می‌دهند، دسترسی را محدود سازند.[۴]

در این راستا می‌توان به واتس‌اپ به‌عنوان یکی از مهم‌ترین پلتفروم‌هایی که درحال‌حاضر مورد استفاده بسیاری از کاربران قرار می‌گیرد و به روش خودتنظیمی کنترل می‌شود، اشاره کرد. واتس‌اپ کانال ارتباطی میان کاربران را با رمزنگاری سرتاسری،[۵] کدگذاری می‌کند. درک این موضوع الزامی است که اطلاعات ذخیره‌شده در فرادادهها تنها برای حفظ حریم خصوصی کاربران مهم است. شرایط حقوقی شرکت اجازه می‌دهد آنها اطلاعات مرتبط با پیام‌های تحویل‌شدهٔ موفق مانند زمان تحویل، شماره تلفن همراه مندرج در پیام، محتوای دیجیتالی مبادله‌شده میان دو طرف را ذخیره کنند. همچنین، این برنامه کاربر را تشویق می‌کند تا کل محتوای خود را با آن به اشتراک بگذارد. درحالی‌که فرادادهها در طول انتقال رمزنگاری می‌شوند، شماره‌های تلفن، مدت زمان اتصال، و همچنین مکان کاربر در سرورهای شرکت ذخیره می‌شوند. این فرادادهها

1. Hetcher Steven, "Changing the Social Meaning of Privacy in Cyberspace", *Harvard Journal of Law & Technology* Vol.15, 2001, p179.
2. Clausing, J., "New Technology Is Aimed at Incresing web Privacy", *New York Times*, 22 June, C 6.
Available at: https://archive.nytimes.com/www.nytimes.com/library/tech/reference/index-privacy.html.8/8/2019.
3. Cohen, J., "Examined Lives: Informational Privacy and the Subject as Object", *Stanford Law Review52*, 2000, p1392.
4. *Ibid*, p 1393
5. End to End Encryption

برای ایجاد یک نمایه و دستیابی به استنباط‌های قوی میان طرفین ارتباط کافی هستند و همان‌گونه که اغلب می‌بینیم، هم دولت‌ها و هم هکرها می‌توانند به این فراداده‌ها دست یابند.[1]

۲.۳. رویکرد اتحادیه اروپا: تنظیم‌گری مشارکتی حریم خصوصی در فضای مجازی

نهادهای حفاظت از حریم خصوصی داده‌ای در اروپا به راهکارهای خودتنظیمی محض بی‌اعتمادند و استفاده از راهکارهای تنظیم‌گری مشارکتی را که نهاد حفاظت از حریم خصوصی داده‌ای در هر دو زمینهٔ تدوین مقررات و اجرای آنها مشارکت دارد، ترجیح می‌دهند. نهادهای حفاظت از حریم خصوصی داده‌ها در اروپا بر تنظیم‌گری مشارکتی تأکید می‌کنند که این امر گواهی بر اولویت تنظیم‌گری مشارکتی است.

در این راستا لازم به توضیح است، شورای اروپا پس از جنگ جهانی دوم برای کمک به متحدکردن اروپا برای تقویت روابط نزدیک بین دولت‌های متعلق به جامعهٔ اروپا، تضمین پیشرفت اقتصادی و اجتماعی با اقدام مشترک برای از بین بردن موانع تقسیم اروپا... و ترویج دمکراسی براساس حقوق اساسی شناخته شده در قانون اساسی و قوانین کشورهای عضو، کنوانسیون اروپایی حمایت از حقوق بشر و آزادی‌های اساسی را تشکیل داد.[2] این کنوانسیون حقِ حریم خصوصی را به‌عنوان یکی از حقوق اساسی بشر به رسمیت می‌شناسد.[3] قوانین حفاظت از داده در اروپا عموماً به علت چهار ویژگی درخور توجه هستند: این قوانین معمولاً هم در بخش عمومی و هم در بخش خصوصی کاربرد دارند؛ این قوانین در طیف وسیعی از فعالیت‌ها، از جمله جمع‌آوری، ذخیره، مصرف و انتشار داده، به کار می‌روند؛ این قوانین منجر به تحمیل تعهدات ایجابی (از جمله، اغلب ثبت‌نام در نهادها و سازمان‌های ملی) به هر فردی می‌شوند که بخواهد به این فعالیت‌ها بپردازد و این قوانین، فارغ از موضوع داده، اگر محدودیت‌هایی هم در بخش‌های خود اعمال کنند، محدودیت‌هایی اندک است.

در سال ۱۹۹۵، شورای اروپا دستورالعمل حفاظت از افراد راجع به پردازش داده‌های شخصی و نیز در خصوص گردش آزاد چنین داده‌هایی[4] منتشر کرد. این دستورالعملْ کشورهای عضو

1. Rastogi, Nidhi, Hendler, James, **WhatsApp security and role of metadata in preserving privacy**, 2017, p 6. Available at: https://arxiv.org/abs/1701.06817/
2. Cate, Fred H., "The EU Data Protection Directive, Information Privacy and the Public Interest", *Iowa Law Review*,1995, p 431.
3. *Ibid*, p 432.
4. 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/

اتحادیهٔ اروپا را ملزم به تصویب قوانین حاکم بر پردازش داده می‌سازد. این دستورالعمل، به نحوی بی‌طرفانه و اجمالی، «پردازش» را این‌گونه تعریف می‌کند: «هرگونه عملیات یا مجموعه‌ای از عملیات جمع‌آوری، ثبت، سازمان‌دهی، ذخیره، انطباق یا جرح‌وتعدیل، بازیابی کردن یا در دسترس قرار دادن، مرتب‌سازی یا ترکیب، مسدودسازی، حذف یا تخریب»، خواه این عملیات به‌صورت خودکار باشد یا غیر خودکار، ولی محدود به این موارد نمی‌شود. تعریف «داده‌های شخصی» به‌طور بی‌طرفانه و کلی عبارت است از: «هرگونه اطلاعات مرتبط با شخص حقیقیِ شناسایی‌شده یا قابل‌شناسایی». این اطلاعات نه‌تنها اطلاعات نوشتاری را در برمی‌گیرد، بلکه شامل عکس‌ها، تصاویر صوتی، تصویری و ضبط صدای شخص حقیقیِ شناسایی‌شده یا قابل‌شناسایی نیز می‌شود.[1]

در ماه ژانویه ۱۹۹۹، همان‌طور که انتظار می‌رفت، اتحادیهٔ اروپا نتیجه‌گیری کرد که براساس شرایط مندرج در دستورالعمل فوق، قوانین حریم خصوصی در ایالات‌متحده ناکافی هستند. درنتیجه، کلیه انتقالات داده به ایالات‌متحده را از ژوئن ۲۰۰۱ ممنوع ساخت. ازآنجاکه دهه‌هاست تفاوت‌های واضحی میان رویکردهای آمریکایی‌ها و اروپایی‌ها درخصوص حریم خصوصی وجود دارد، این تفاوت‌ها زمانی جدی‌تری شد که اتحادیهٔ اروپا «دستورالعمل حفاظت از داده» را در سال ۲۰۱۶ به تصویب رساند. این دستورالعمل مستندی جامع و پیچیده است؛ اما مشخصات برجستهٔ متعددی دارد. ازجمله آنکه طبق مواد مذکور در آن، هر فرد حق دارد از پردازش داده‌های خود مطلع شود؛ به این داده‌ها دسترسی داشته و اشتباهات موجود در آن را اصلاح کند و از انتقال داده‌ها به اشخاص ثالث برای مقاصد بازاریابی جلوگیری کند. همچنین، داده‌های افراد باید صحیح باشند و درصورت لزوم به‌روز نگه‌داشته شوند. بنابر این دستورالعمل، شرکت‌های اروپایی باید افراد را از کاربردهای موردنظر داده‌های شخصی خودآگاه کنند و این داده‌ها را بدون رضایت فرد برای مقاصد دیگر استفاده یا افشا نکنند. اصل پایه این است که داده‌های شخصی نباید بدون رضایت کاربر پردازش شوند؛ مگر «پردازش برای عملکرد قراردادی که فرد مالک اطلاعات خود یکی از طرفین آن است». به‌علاوه، این دستورالعمل ایجاد نهادی ملی برای حفاظت از حریم خصوصی و اعمال کلیه مقررات فوق را الزامی می‌سازد.[2] این امر در اغلب کشورهای اروپایی

1. https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A31995L0046. 20/9/2019.
2. 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→

مشکل بزرگی نیست؛ چون اغلب این کشورها قبلاً هم از بوروکراسی‌های مربوط به حریم خصوصی برخوردار بوده‌اند. درنهایت، این دستورالعمل انتقال داده‌های شخصی مربوط به شهروندان اتحادیه اروپا را به کشورهای فاقد قوانین «کافی» حریم خصوصی ممنوع می‌سازد. لازم به ذکر است در کشورهای اتحادیه اروپا کدهای خودتنظیمی در حوزهٔ حریم خصوصی وجود دارد که توسط سازمان‌های خودتنظیم استفاده قرار شوند.[۱] اما برای معنی‌دار بودن، این کدها باید برخی از مناطقی را پوشش دهند که تحت پوشش قانون نیستند یا درغیراین‌صورت استاندارد بالاتری از حفاظت از حریم خصوصی را تأمین کنند. از کدهایی چون گمنام‌سازی (حذف اطلاعات هویتی شخصی درجایی که به آن نیاز نیست)، مستعارسازی (جایگزینی داده‌های قابل‌شناسایی شخصی با شناسه‌های ساختگی) و رمزگذاری (رمزگذاری پیام‌ها به‌نحوی‌که تنها به‌وسیله مقام صلاحیت‌دار قابل‌شناسایی باشد) استفاده می‌شود. تقاضا برای رمزنگاری قدرتمند به‌عنوان ابزاری برای تضمین محرمانه بودن ارتباطات از راه دور افزایش یافته است. نرم‌افزارهایی که از طریق اینترنت آزادانه در دسترس هستند، رمزگذاری را چنان قوی تولید می‌کنند که میلیون‌ها سال طول می‌کشد رایانه‌های فعلی بتوانند کلیدها را تنها به‌صورت چندصد رقم رمزگشایی کنند. پیام را هنوز هم می‌توان ره‌گیری کرد، اما بدون کلید رمزگشایی، چیزی جز یک سری از نمادهای ظاهراً بی‌معنی نخواهد بود.[۲]

درخصوص کاربرد عملی روش اتخاذ شده در اتحادیهٔ اروپا می‌توان به موضوع توافق‌نامهٔ بندرگاه امن[۳] ایالات متحده- اتحادیه اروپا اشاره کرد. این توافق‌نامه راهی برای پل زدن بین دو قانون مختلف در باب حریم خصوصی است. دستورالعمل اروپایی در باب حفاظت از داده‌ها، انتقال اطلاعات شخصی به کشورهای خارج از اتحادیه اروپا را که از استاندارد «کفایت» برخوردار نیستند، منع می‌کند. بااین‌حال، وزارت بازرگانی ایالات متحده و اتحادیه اروپا برای انتقال داده‌ها به این کشور، این توافق‌نامه را توسعه دادند که به شرکت‌ها اجازه می‌دهد سطح حفاظت مشابهی

←on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *Official Journal of the European Union*, Vol.59, 2016, p 1.

1. Ang, Peng H., "The Role of Self- Regualtion of Privacy and The Internet", *Journal of Interactive Advertising*, 2001, p 3.

2. *Council of Europe, Handbook on European data protection law*, Publications Offce of the European Union, 2014, p 45.

3. Safe Harbor

را تصدیق نماید. درصورتی‌که شرکت‌ها به هفت اصل حفظ حریم خصوصی پایبند باشند، می‌توانند در این برنامه شرکت کنند و گواهی‌نامه‌ای مبنی بر تأیید خود دریافت کنند.[۱]

تمام ۲۷ کشور عضو اتحادیه اروپا این گواهی‌نامه را قبول دارند و با مشاهدهٔ آن به‌طور خودکار از الزامات قبلی انتقال داده‌ها صرف‌نظر می‌کنند. پیوستن به توافق‌نامه بندرگاه امن داوطلبانه است و به شرکت‌های آمریکایی اجازه می‌دهد اطلاعات مربوط به مشتریان، پیمانکاران یا کارمندان اتحادیه اروپا را به‌دست آورند.[۲]

۱. ارزیابی سیستم با نخستین معیار یعنی کاراکتر مشارکتی آغاز می‌شود. این دستورالعمل در پارلمان اتحادیه اروپا به تصویب رسید و چارچوب توافق‌نامه بندرگاه امن بین وزارت بازرگانی ایالات متحده و یک کارگروه فعال در اتحادیه اروپا مورد مذاکره قرار گرفت. این کارگروه که از کمیسیون‌های حفظ حریم خصوصی کشورهای عضو تشکیل شده است، مسائل را قبل از تصمیم‌گیری یا اظهارنظر با عموم مردم به اشتراک می‌گذارد. این امر باعث ایجاد یک ارتباط همکاری بین تنظیم‌کنندگان و مصرف‌کنندگان می‌شود. وزارت بازرگانی ایالات متحده به منافع شرکت‌ها اهمیت می‌دهد، اما درحال‌حاضر آنها فقط می‌توانند بدون تعامل با تنظیم‌کننده در یک سیستم مشارکت کنند. این یعنی که سیستم به کاراکتر مشارکتی پایبند است، اما تعامل بین تنظیم‌کننده‌ها و صنعت ناچیز است.[۳]

۲. سیستم، الزامات راهنما و استانداردهای حداقلی را رعایت می‌کند و به‌جای مقررات دقیق و سخت‌گیرانه، از اصولی مانند «اقدامات احتیاطی منطقی»، «محافظت مؤثر» یا «زودیافت» استفاده می‌کند. این مسئله یک مزیت دارد و این است که صنعت می‌تواند مقررات مربوط به حریم خصوصی خود را به‌صورت جداگانه و انعطاف‌پذیر تنظیم کند. این چارچوب با اشاره به پیشرفت‌های تکنولوژیک، روند انتقال و پردازش داده‌ها را تسهیل کرده و ازاین‌رو، امکان پیشرفت مداوم تکنولوژی را فراهم می‌سازد.

1. ITA, *Welcome to the U.S.-EU & Swiss Safe Harbor Frameworks* http://www.export.gov/safeharbor/.10/10/2019.
2. Clausing, Jeri, Europe and U.S. Reach Data Privacy Pact, New York Times, March 15 2000.Available at: ww.nytimes.com/2000/03/15/business/europe-and-us-reach-data-privacy-pact.htm. 10/10/2019.
3. European Commission, Commission decisions on the adequacy of the protection of personal data in third countries http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm.

۳. قوانین مربوطه در دسترس عموم قرار دارند و وزارت بازرگانی ایالات متحده اسامی سازمان‌های مجاز را منتشر می‌کند. متأسفانه، فهرست اسامی شامل سازمان‌هایی است که دیگر وجود خارجی ندارند یا فاقد گواهی‌نامه معتبر هستند.
۴. سازمان‌ها باید سیاست‌های خود را در باب حفظ حریم خصوصی افشا کنند. بااین‌حال، سیاست‌ها در یک صفحه وب که باعث افزایش مقایسات می‌شوند، ذخیره نمی‌شوند. تصمیمات کارگروه و گزارش‌های سالانه به‌صورت آنلاین در دسترس عموم قرار می‌گیرند.
۵. پاسخگویی به واسطهٔ نقش اجرایی بخش خصوصی و قوانین دولتی تضمین می‌شود. بدنهٔ اصلی یک سازمان متعلق به بخش خصوصی است که به حل اختلافات، ممیزی کدها و راه‌حل‌ها می‌پردازد. به‌علاوه، سازمان‌ها می‌توانند صرفاً مقامات نظارتی دولت را انتخاب کنند یا با مقامات محافظت از داده‌های اروپا همکاری کنند.
۶. فرامین بخش خصوصی شامل انتشار موارد عدم انطباق، حذف داده‌ها، دستورهای تأکیدی، حذف نشان گواهینامه، جبران خسارات و تعلیق عضویت در برنامهٔ حریم خصوصی مربوطه است. آخرین مورد، تعلیق نهاد مربوطه از توافق‌نامه بندرگاه امن است. فرامین دولتی شامل دستورات اداری و مجازات‌های مدنی و اخراج از چارچوب بندرگاه امن است.
۷. بخش خصوصی که وظیفهٔ ضمانت اجرایی را بر عهده دارد، به‌عنوان یک نهاد شاکی برای کاربران عمل می‌کند. سازمان‌ها می‌توانند در احکام خود تجدیدنظر کنند. به‌علاوه، کارمندان اتحادیه اروپا می‌توانند شکایت خود را به مقامات حفاظت از داده‌های ملی یا اداره کار در کشور خود ارائه کنند و آن را به وزارت بازرگانی ایالات متحده ارجاع دهند.
۸. این سیستم دارای نمایندهٔ مصرف‌کنندگان است.
۹. تفکیک قدرت بین نهادهای خودتنظیم و بخش دولتی وجود دارد؛ زیرا فرایند احراز هویت به‌صورت شخصی انجام می‌گیرد: سازمان‌ها سیاست حفظ حریم خصوصی خود را تدوین می‌کنند و با ارائهٔ فرم درخواست عضویت در بندرگاه امن به وزارت بازرگانی، به‌طور خودکار احراز هویت می‌شوند. تأیید توسط یک نهاد خارجی می‌تواند استانداردها و انطباق کامل با اصول موجود را بهبود بخشد. اما باید توجه داشت که تفکیک قوا بین نهادهای خودتنظیم و بخش دولتی وجود دارد.

۱۰. اتحادیه اروپا و یک سرویس مشاوره خارجی به‌طور منظم سیستم را ارزیابی می‌کنند. این ارزیابی برخی از نقاط ضعف قبلی را برملا ساخته و لازمهٔ بهبود سیستم تنظیمی است. احراز هویت مجدد به‌صورت سالانه نیز یک مکانیزم خوب برای ارزیابی است، اما این ارزیابی توسط خودِ سازمان‌ها انجام می‌شود و کاربرد محدودی دارد.[۱]

۳. ارزیابی روش‌های تنظیم گری حریم خصوصی در فضای مجازی

از دست رفتن حریم خصوصی به‌منزلهٔ شکست بازار است. برای این شکست بازار چه باید کرد؟ آیا در پاسخ، نیازمند نهاد دولتی و قوانین سختیگرانه در این حوزه هستیم یا آنکه با استفاده از تنظیم‌گری بخش خصوصی می‌توان شکست بازار را جبران نمود؟ کدام نوع از مداخله دولت باعث افزایش رفاه می‌شود؟ لذا ازآنجاکه اگر تحلیل سیاست‌های حریم خصوصی نتواند آثار روش تنظیم‌گری را بررسی کند، تحلیلی غیرعملی و ناکامل است، در این قسمت از مقاله روش‌های تنظیم‌گری کنترل–دستوری، خودتنظیمی و تنظیم‌گری کنترل–دستوری ارزیابی خواهد شد.

۳.۱. گرایش موسع تقنینی و تاثیر آن بر ارزیابی تنظیم‌گری

استدلال در خصوص تنظیم‌گری کنترل– دستوری (قانون‌گذاری مستقیم) این است که اعتماد مصرف‌کننده، و درنتیجه تجارت را افزایش می‌دهد؛ اما کسانی که از دخالت کمتر دولت حمایت می‌کنند، استدلالشان بر این است که تنظیم‌گری کنترل–دستوری با کار بازار آزاد تداخل دارد. همچنین یکی از منابع اصلی عدم کارایی ساختار کلاسیک تنظیم‌گری کنترل–دستوری عدم ارائهٔ اطلاعات از سوی نهاد تنظیم‌گر است. عدم ارائهٔ اطلاعات می‌تواند منجر به اتخاذ تصمیمات قانون‌گذاری ضعیف شود و قانون‌گذاری ضعیف منجر به افزایش هزینه و تحمیل این هزینه بر جامعه می‌شود. با توجه به اندازهٔ این هزینه‌ها، احتمال ناکارآمدی تخصیصی اغلب قوانین و مقررات دولتی ایجاد می‌شود.[۲]

1. Connolly, C., The US Safe Harbor – Fact of Fiction? ,2008.Available at: http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf /

2. Swire, Peter P., Litan, Robert E.," None of Your Buisiness: World Data Flows, Electronic Commerce and The European Privacy Directive", *Harvard Journal of Law & Technology*, Vol. 12, No 3, 1999, p 690.

۳.۲. گرایش به عدم تقنین و تاثیر آن بر ارزیابی تنظیم‌گری

هرچند در ایالات‌متحده آمریکا بر فلسفهٔ خودتنظیمی تکیه شده است ازآنجاکه روش خودتنظیمی بدون همکاری وب‌سایت‌های تجاری کار نمی‌کند و اگر شرکت‌های مذکور در امر خودتنظیمی جدی باشند، باید کار خود را از توسعهٔ نوعی سیاست حریم خصوصی دقیق و ظریف شروع کنند، سیاست مذکور باید درنهایت برای کاربرد در نرم‌افزار ترجیحات حریم خصوصی و سایر فناوری‌ها، به فرمت قابل‌خواندن توسط ماشین تبدیل شود. باوجوداین، نظامی که حول این مفهوم تنظیم شده است، نرم‌افزار ترجیحات حریم خصوصی است. نرم‌افزار ترجیحات حریم خصوصی از یک پروتکل توسعه‌یافته توسط ائتلاف وب جهان‌گستر، به نام پلتفرم انتخاب محتوای اینترنت،[1] استفاده می‌کند.[2] در مفهوم آن، پلتفرم انتخاب محتوای اینترنت برای حمل برچسب‌هایی طراحی‌شده بود که محتوای آن را برای کاربران توصیف می‌کرد.

طبق پروتکل انتخاب محتوای اینترنتی، مالک سایت، سطح حریم خصوصی سایت را بیان می‌کند. همچنین کاربر دارای اولویت حریم خصوصی تنظیم‌شده بر روی مرورگر وب خواهد بود. اگر سطح حریم خصوصی در وب با حریم خصوصی مرورگر منطبق باشد، کاربر به‌صورت شفاف به آن دسترسی پیدا می‌کند؛ اما اگر حریم خصوصی در سایت در سطح پایین‌تری نسبت به آنچه کاربر ترجیح می‌دهد قرار گیرد، پنجره‌ای باز می‌شود و می‌پرسد که آیا کاربر آماده است تا بخشی از فقدان حریم خصوصی را برای این سرویس از دست دهد؟ بنابراین نرم‌افزار ترجیحات حریم خصوصی به صاحب سایت و کاربر اجازهٔ مذاکره درمورد یک سطح قابل‌قبول از حریم خصوصی را می‌دهد.

انتقادهای زیادی درخصوصِ نرم‌افزار ترجیحات حریم خصوصی به‌عنوان ابزاری برای حفاظت از حریم خصوصی برای مصرف‌کننده وجود دارد. یکی از مهم‌ترین معایب استفاده از این روش عدم شفافیت شرکت‌های ارائه دهندهٔ خدمات اینترنتی و عدم پاسخگویی این شرکت‌ها است. همچنین استفاده از این روش تنظیم‌گری بیشتر به منظور برطرف شدن منفعت خصوصی بخش خصوصی و نه تأمین منفعت عمومی کاربران است.[3]

1. Platform for Internet Content Selection
2. Garfinkel, S., Can a Labeling System Protect Your Privacy, 2000. http:// www.Salon.com/technology/col. 12/10/2019.
3. *Ibid*, p 459.

۳.۳. گرایش مضیق تقنینی و تاثیر آن بر ارزیابی تنظیم‌گری

مشکل تنظیم‌گری به سبک اروپایی برای داده‌های کاربران، بالا بودن هزینه‌های معامله[۱] زیرساخت‌های تنظیم‌گری است که می‌تواند به نتایجی غیر کارآمد منجر شود. لکن فواید استفاده از این روش از تنظیم‌گری به شرح ذیل است:

تبادل اطلاعات می‌تواند محصول جانبی ارزشمند رژیم‌های تنظیم گری مشارکتی باشد. همان‌طور که در ادامه ملاحظه می‌شود، یکی از منابع اصلی عدم کارایی ساختار ِتنظیم‌گری کنترل–دستوری، عدم ارائهٔ اطلاعات از سوی نهاد تنظیم‌گر است؛ چراکه عدم ارائهٔ اطلاعات ممکن است منجر به اتخاذ تصمیمات قانون‌گذاری ضعیف شود. لکن سیستم تنظیم‌گری مشارکتی به‌گونه‌ای طراحی می‌شود که در آن اطلاعات به‌صورت شفاف از ناحیهٔ نهاد خودتنظیم در اختیار کاربران قرار می‌گیرد.[۲] همچنین وجود سطح مرکزی برای کمک به اجرای قوانینی که در سطح غیرمتمرکز تدوین شده‌اند، ضروری است؛ زیرا تنها دولت می‌تواند به اعمال قدرت مشروع متوسل شود. درنتیجه ساختارهای حکمرانی غیرمتمرکز و خودتنظیم امکان ایجاد نوآوری را که در چهارچوب قوانین متمرکز امکان‌پذیر نیست، با تصویب دستورالعمل‌هایی که امکان تغییر و به‌روز کردن آن را با دانش روز فراهم می‌کند.[۳] در هر یک از طرح‌های حکمرانی چندسطحی، همواره نهاد تنظیم‌گر دولتی به‌عنوان آخرین مرجع باید وجود داشته باشد که همهٔ نهادهای قانون‌گذار تحت نفوذ آن را تحت پوشش خود داشته باشد. این مرجع نهایی عبارت است از:

«مسئول جلوگیری از بروز ناسازگاری در میان استانداردها و بیشینه کردن پیامدهای مثبت شبکه در میان آنها و همچنین جلوگیری از تسخیر استانداردها توسط افراد یا گروهایی که در جستجوی استیلای خود هستند... این نهاد همچنین مسئول تضمین اجرای احکام تعیین‌شده در داخل تا زمانی است که این احکام به تحقق کارآمدی جمعی کمک کنند.»[۴] وجود توافق بین دولت و نهادهای خودتنظیم که مطابق با آن، دولت به اجرای مقررات توسط نهادهای خودتنظیم

1. Transaction Cost
2. Frydman, B., Hennebel, L., **Lewkowicz, G., Public strategies for Internet Co-Regulation in the United States**, Europe and China, Cambridge University Press, 2000, p 8.
3. Hirsch, Dennis D., "The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?" *Seattle University Law Review*, Vol. 34, No.439, 2011,p 464.
4. Scott, J., Trubek, D.M., "Mind the gap: law and new approaches to governance in the European Union". *European Law Journal,* Vol.8, 2002, p4.

تدوین شده‌اند، کمک می‌کند. درعوض، نهادهای خودتنظیم محدودیت‌های اعمال‌شده از سوی نهادتنظیم‌گر را در قبال این کمک می‌پذیرد. این مسئله به هر سطح از تنظیم‌گری اجازه می‌دهد تا یکدیگر را تقویت کنند. از این‌رو دولت‌ها همچنان از نقش تنظیم‌گری به میزان قابل‌توجهی برخوردارند و اختیارات نهادهای خودتنظیم محدود است. حتی نهادهای خودتنظیم از طریق نرم افزار کد به تنظیم‌گری این حوزه بپردازند.[1] در این راستا مراکز استاندارد اینترنت، اعم از دولت‌ها و نهادهای خودتنظیم، از انگیزهٔ مذاکره و همکاری برای حل تعارض بین استانداردها برخوردارند. قابلیت این مذاکره در جذب کاربران به نتیجه‌بخش کردن استاندارد از دید نهادهای خودتنظیم که به این امر مشغول‌اند، حائز اهمیت است. همان‌طور که در بالا اشاره شد، دولت‌ها نیز در زمانی که کارایی قوانین مرکزی خود را ارزیابی می‌کنند، باید استانداردهای خصوصی نهادهای خودتنظیم را مدنظر قرار دهند. بنابراین در این روش از تنظیم‌گری وابستگی‌های متقابل بین تنظیم‌گری کنترل–دستوری و خودتنظیمی وجود دارد. تنظیم‌گری کنترل–دستوری به‌عنوان پشتیبانی ضروری عمل می‌کنند که تعیین استانداردهای خصوصی و اجرای آنها به پشتوانهٔ آنها انجام می‌شود. در نظام ارزیابی تأثیر تنظیم‌گری مشارکتی تلاش‌ها معطوف به آن است که تدابیر نهادهای خودتنظیم منتهی به بهترین کارآمدی گردد.

بنابراین می‌توان گفت: در تنظیم‌گری مشارکتی تلاش بر این است تا دو مانع اصلی تنظیم‌گری کنترل– دستوری مانند دسترسی محدود به اطلاعات و عدم وجود انعطاف‌پذیری رفع می‌گردد. علاوه بر این، تنظیم‌گری مشارکتی می‌کوشد تا مانع اصلی خودتنظیمی چندجانبه تصحیح شود که این مانع، عدم وجود مشروعیت و اهداف منفعت عمومی در تعیین و اجرای قوانین زیربناست. مشارکت یک دستگاه یا نمایندهٔ تنظیم‌گر دولتی تضمین خواهد کرد که قوانین زیربنا اهداف منفعت عمومی را ضمن پذیرش انعطاف‌پذیری منعکس کند.[2]

1. Weiser, P., "The future of internet regulation". *University of California Davis Law Review*, 2009, p580.
2. Hirsch, Dennis D., *Op Cit*, p 479.

نتیجه‌گیری

پیش‌بینی آینده برای انسان‌های بسیار کمی امکان‌پذیر است، اما با اندکی هوشمندی و روشن‌بینی می‌توان به محو تدریجی حریم خصوصی اشخاص در سال‌های آینده پی برد؛ به‌نحوی‌که این احتمال چندان دور از ذهن نیست که طی ۱۰ یا ۱۵ سال آینده، به حریم خصوصی وافری که در این هزاره وجود داشت، با حسرت نگریسته شود. دلایل کمرنگ شدن و محو تدریجی حریم خصوصی پیچیده و متنوع‌اند که از بی‌تفاوتی و تنبلی محض تا اشتیاق اشخاص برای بهره‌مندی از مزایای عظیم اقتصاد جدید بدون محاسبهٔ هزینه‌های آن را در برمی‌گیرد. هزینهٔ چشم‌پوشی از حریم خصوصی ممکن است در ابتدا اندک به نظر برسد؛ چراکه امکاناتی مثل خرید راحت‌تر و امن‌تر را فراهم می‌کند؛ اما آن هنگام که تنها بخش اندک و محدودی از حریم خصوصی باقی می‌ماند، اشخاص از این مصالحه افسوس می‌خورند. حریم خصوصی همواره به‌عنوان ارزشی انتزاعی و تقریباً توصیف‌ناپذیر شناخته می‌شود و همین خصیصه موجب می‌شود تا اشخاص آن را ساده‌تر از امور دیگر در ازای منافع ملموس و آنی قربانی کنند.

بنابراین، از بین رفتن حریم خصوصی نه‌تنها شکست بازار است که شکست شخصی نیز محسوب می‌شود. کاربران برای حفظت از حریم خصوصی‌شان، ابزارها و قابلیت‌هایی در اختیار دارند که آنها را در پاسداشت حریم خصوصی که ارزشی قابل‌توجه است، کمک می‌کنند؛ برخی از این ابزارها همچون قابلیت غیرفعال کردن عملکرد کوکی مرورگر، ساده هستند، اما برای اغلب کاربران، انجام دادن این اقدامات احتیاطی به دردسر آن نمی‌ارزد. این موضوع را این‌گونه می‌توان تحلیل کرد که شاید مصرف‌کنندگان واقعاً چندان به حریم خصوصی اهمیت نمی‌دهند و اگر این‌طور باشد، چرا باید قوانین پرهزینه‌ای را برای پر کردن خلأ حریم خصوصی تصویب کنیم که مصرف‌کنندگان نسبت به آن بی‌تفاوت‌اند؟

براساس مجموع آنچه که در این مقاله ذکر شد، به نظر می‌رسد تدوین یک استراتژی ملی برای تنظیم‌گری حریم خصوصی در فضای مجازی ضروری است؛ اما باید توجه داشت که اجرای مطلوب و بهره‌برداری از مزایای بالای اجتماعی و اقتصادی آن، علاوه بر طراحی یک سیاست ملی مناسب، مستلزم تحقق عملی آن و تعامل صحیح و متعادل بخش دولتی و نهاد خودتنظیم است؛ چراکه نهاد خودتنظیم بدون حمایت و استانداردهای مقررشده از سوی دولت قادر به فعالیت

پایدار نیست و از طرفی دولت نیز باید در سیاست‌گذاری‌های خود اصل مقررات‌زدایی را اعمال کند و با از بین بردن قوانین سخت‌گیرانه و محدودکننده، سعی در تسهیل فعالیت نهادخودتنظیم بکوشد.

بنابراین می‌توان گفت: تنظیم‌گری حریم خصوصی در فضای مجازی در کشور ایران با خلأ جدی مواجه است؛ چراکه حتی قانون تجارت الکترونیک و قانون جرائم رایانه‌ای به‌عنوان تنها سند قانونی کشور در باب حمایت از داده‌های اشخاص در فضای مجازی نیز خالی از اشکال نیست و همین موضوع ضرورت اقدامات جدی در این خصوص را توجیه‌پذیر می‌سازد. لازمهٔ رفع خلأهای موجود و حمایت از دادهٔ اشخاص در مرحلهٔ اول این است که قانونی مستقل درزمینهٔ حریم خصوصی به تصویب نهاد قانون‌گذار در کشور برسد؛ چراکه اگرچه قانون تجارت الکترونیک دارای اشکالاتی است که می‌تواند اصلاح گردد، اما درنهایت این قانون به امور تجارتی اختصاص دارد و تصویب قانونی مستقل درزمینهٔ حریم خصوصی در کشور به‌شدت ضروری است.

فهرست منابع

الف) منابع فارسی

کتاب

۱.انصاری، باقر، **حقوق حریم خصوصی**، تهران: انتشارات سمت، ۱۳۹۰.

۲.جهانگرد، نصرالله و خسرو سلجوقی، **مجموعه قوانین و مقررات فنّاوری اطّلاعات و ارتباطات ایران**، دبیرخانه شورای عالی اطّلاع رسانی، ۱۳۸۳.

مقاله

۳.آقایی طوق و ناصر مسلم، «مهدی،چالش‌های حفاظت از داده‌های خصوصی در حوزه اینترنت اشیا: مطالعه تطبیقی حقوق ایران و اتحادیه اروپا»، *فصلنامه حقوق اداری*، سال هفتم، ش ۲۳، تابستان ۹۹، ص ۴۰.

۴.زرکلام، ستار، «حریم خصوصی ارتباطات اینترنتی (مطالعه در حقوق ایران و اتحادیه اروپا)»، *پژوهش‌نامه حقوق اسلامی*، ش ۲۵، ۱۳۸۶.

۵.فتحی، یونس و خیراله شاهمرادی، «گستره و قلمرو حریم خصوصی در فضای مجازی»، *مجله حقوقی دادگستری*، سال هشتاد و یکم، ش ۹۹، پاییز ۹۶.

ب) منابع انگلیسی

Books

6.Council of Europe, **Handbook on European data protection law**, Publications Office of the European Union, 2014.

Articles

7.Kang, J.,” Information Privacy in Cyberspace Transactions”, *Stanford Law Review*, 1998.

8.Chesterman, S., “After Privacy: The Rise of Facebook, the Fall of WikiLeaks, and Singapore’s Personal Data Protection Act 2012*”, Singapore Journal of Legal Studies*, 2012.

9. Kluger, Jeffrey," Extortion on the Internet; A daring hacker tries to blackmail an e-tailer and sparks new worries about credit-card cybertheft", *TIME*, 2000.
10. Warren, Samuel D., Brandeis, Louis D., "The Right to Privacy", *Harvard Law Review*, Vol. 4, No. 5, 1890.
11. Clarke, R., "Platform for Privacy Preferences: A Critique". *Privacy Law & Policy Reporter*, 5(3),1998.
12. Hetcher Steven, "Changing the Social Meaning of Privacy in Cyberspace", *Harvard Journal of Law & Technology*, Vol.15, 2001, p179.
13. Clausing, J., "New Technology Is Aimed at Incresing web Privacy"*, New York Times*, 22 June, C 6.
14. Cohen, J., "Examined Lives: Informational Privacy and the Subject as Object", *Stanford Law Review52*, 2000, p1392.
15. Cate, Fred H., "The EU Data Protection Directive, Information Privacy and the Public Interest", *Iowa Law Review*,1995, p 431.
16. Ang, Peng H., "The Role of Self- Regualtion of Privacy and The Internet*", Journal of Interactive Advertising*, 2001.
17. Clausing, Jeri," Europe and U.S. Reach Data Privacy Pact", *New York Times*, March 2000.
18. Swire, Peter P., Litan, Robert E., "None of Your Buisiness: World Data Flows, Electronic Commerce and The European Privacy Directive", *Harvard Journal of Law & Technology*, Vol. 12, No 3, 1999, p 690.
19. Frydman, B., Hennebel, L., "Lewkowicz, G., Public strategies for Internet Co-Regulation in the United States, Europe and China", Cambridge University Press, 2000.
20. Hirsch, Dennis D., "The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?" *Seattle University Law Review*, Vol. 34, No.439, 2011,p 464.
21. Scott, J., "Trubek, D.M., Mind the gap: law and new approaches to governance in the European Union". *European Law Journal*, Vol.8, 2002, p4.
22. Weiser, P.," The future of internet regulation". *University of California Davis Law Review*, 2009.

Regulation and document

23. OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, The OECD Privacy Framework, OECD ,2013.
24. 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.
25. 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, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union, Vol.59, 2016.

Judicial Precedent

26. ITA**,** Welcome to the U.S.-EU & Swiss Safe Harbor Frameworks http://www.export.gov/safeharbor

Sites

27. Rastogi, Nidhi, Hendler, James, WhatsApp security and role of metadata in preserving privacy, 2017, p 6 Available at: https://arxiv.org/abs/1701.06817/
28. Connolly, C., The US Safe Harbor – Fact of Fiction? ,2008.Available at:http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf.
29. http://citizensrights.ir/. 6/7/2019.
30. https://rc.majlis.ir/fa/legal_draft/show/809338. 6/6/2019.
31. https://www.ftc.gov/tips-advice/business-center/guidance. 7/7/2019.
32. https://epic.org/reports/prettypoorprivacy.html/
33. https://archive.nytimes.com/www.nytimes.com/library/tech/reference/index-privacy.html.8/8/2019.
34. https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A31995L0046. 20/9/2019.
35. http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm.