

## چالش‌های قانونگذاری حقوق کاربران در فضای مجازی؛ مطالعه تطبیقی دو تجربه متفاوت<sup>۱</sup>

سیدمحمد مهدی غمامی<sup>۲</sup>؛ حمید فعلی<sup>۳</sup>

تاریخ ارسال: ۱۴۰۱/۰۷/۱۶ تاریخ پذیرش: ۱۴۰۱/۱۱/۰۸

### چکیده

حقوق کاربران در فضای مجازی همواره مورد تعرض و تضییع قرار می‌گیرد و قانونگذاران موظفند، الزامات قانونی برای حمایت از آنها در مقابل سوداگری‌ها را ایجاد کنند. هرچند سوداگران دسترسی به قانونگذاری هم دارند و مانع حمایت از شهروندان می‌گردند؛ کما اینکه بخش ۲۳۰ قانون نزاکت آمریکا ۱۹۹۶ مانع اصلی مهار خودسری پلتفرم‌های (سکوه‌های نشر) بزرگ مثل گوگل، توئیتر، اینستاگرام و... است. در مقابل تجربه قانونگذاری در اتحادیه اروپا برای کنترل پلتفرم‌ها علیرغم وجود کاستی‌ها، توفیقاتی نیز داشته است؛ اما در سوی دیگر در ایران قانونگذاری در این حوزه بسیار ضعیف و مغایر تجربیات جهانی بوده است. سؤال اصلی اینجاست که چه الگویی در قانونگذاری نسبت به حقوق کاربران سکوه‌های نشر می‌تواند در ایران کارآمد باشد؟ این مقاله با رویکردی تطبیقی به دو نظام قانونگذاری ایالات متحده آمریکا و اتحادیه اروپا، با روشی توصیفی و تحلیلی پاسخ این پرسش را ارائه می‌کند. یافته‌های پژوهش نشان می‌دهد برخلاف تجارب کشورهای دیگر قانونگذاری در ایران هم در جهت حمایت از توسعه سکوه‌های نشر داخلی با رعایت اصول رقابت و هم در جهت صیانت از حقوق کاربران سکوه‌های نشر با اشکالاتی مانند خلط سیاست‌گذاری و تنظیم‌گری و خودتنظیم‌گری، تشدید چالش قانونگذار، بی‌ثباتی مقررات اقتصادی فعالان اقتصاد مجازی و عدم تصریح به حقوق کاربران منجر به آسیب‌هایی در این حوزه شده است.

### واژه‌های کلیدی

فضای مجازی، حقوق کاربران، سکوه‌های نشر (پلتفرم‌ها)، حفاظت از داده‌ها، قانونگذاری

۱. این مقاله براساس نظر گروه دبیران و سردبیر فصلنامه، پژوهشی است.

۲. دانشیار گروه حقوق عمومی، دانشکده معارف اسلامی و حقوق، دانشگاه امام صادق (علیه السلام)، تهران،  
ghamamy@isu.ac.ir ایران.

۳. دانشجوی دکتری، گروه حقوق عمومی، دانشکده معارف اسلامی و حقوق، دانشگاه امام صادق (علیه السلام)،  
تهران، ایران. (نویسنده مسئول).  
hamidfeli@gmail.com

## مقدمه

سرعت گسترش و پیشرفت اینترنت و فضای مجازی و ایفای نقش آن در همه ابعاد زندگی بشریت در دهه‌های اخیر به حدی بالا بوده است که گاه سایر پدیده‌ها و علوم بشری به تناسب آن رشد نکرده و پاسخگویی کاملی به اقتضای مسائل ناشی از بسط فضای مجازی نداشته است. به تعبیر برخی نویسندگان، قرن بیست و یکم قرن «مرگ فاصله‌ها» است و طبیعی است که با مرگ فاصله‌های زمانی و مکانی میان انسان‌ها از طریق فضای مجازی، درگیری بین انسان‌ها بیشتر شده و حقوق شهروندان نیز بیشتر در معرض تعرض قرار می‌گیرد؛ لذا دفاع از این حقوق، تدابیر و قوانین لازم را ضروری می‌کند. (اسماعیلی، ۱۳۹۱، ۳۶۲)

از میان کاربردهای مختلف اینترنت و فضای مجازی، شبکه‌های اجتماعی و پلتفرم‌های دیجیتال با استقبال مضاعفی در سراسر دنیا مواجه شده‌اند. به نحوی که رشد فزاینده تعداد کاربران آنها در سال‌های اخیر در سطح جهان و ایران به صورت بی‌سابقه‌ای روابط انسان‌ها با یکدیگر و حتی سبک زندگی افراد را تحت تأثیر قرار داده است. با توجه به اینکه روز به روز ورود سکوها‌های نشر به روابط حقوقی بین اشخاص و زندگی و حریم خصوصی آنها در ایران و جهان بیشتر می‌شود، برای پیشگیری از سوء استفاده‌های غول‌های بزرگ دیجیتال از اطلاعات مردم بایسته است قوانین لازم در این زمینه به تصویب برسد. همچنین با توجه به قانون‌گذاری سایر کشورها از جمله آمریکا در این حوزه باید توجه داشت که قوانین هر کشوری مبتنی بر مبانی حقوقی آن کشور تنظیم شده است؛ اما به جهت اینکه قانونگذاری در مسائل جدید بدون بهره‌گیری از تجارب سایر کشورها بسیار مشکل است و آسیب‌هایی دارد، در کنار توجه به مبانی و مبادی و منابع و روش‌های خاص نظام حقوقی خودمان، به نحوی که قانون جدید برگرفته از حقوق بیگانه وصله‌ای ناهم‌رنگ نشود، (شفیعی سروستانی، ۱۳۸۵: ۱۶۷) باید به قوانین کشورهای پیشرو در آن زمینه نیز توجه داشت و از تجارب بشری غافل نبود.

در این زمینه تجارب قانون‌گذاری متفاوت اتحادیه اروپا و ایالات متحده آمریکا به عنوان نمونه‌هایی قابل تأمل مطرح هستند که اتحادیه اروپا با رویکرد صیانت

چالش‌های قانونگذاری حقوق کاربران در فضای مجازی؛ مطالعه تطبیقی دو تجربه متفاوت

حداکثری از حقوق کاربران سعی بر امن‌تر کردن فضای مجازی برای کاربران داشته است و آمریکا با رویکرد مصونیت ارائه‌دهندگان خدمات اینترنتی به ویژه در فضای وب ۲ و شبکه‌های اجتماعی و سکوه‌های نشر دیجیتال تلاش کرده است مانع رشد و توسعه تکنولوژی در کشور خود نشود و قدرت خود را در این عرصه از دست ندهد. اما آنچه که عملاً سکوه‌های نشر ناگزیر از محدودیت در قالب آن هستند قوانینی است که با از بیرون بر آنها تحمیل می‌شود و یا به‌ناچار باید خود را محدود کنند و دست به خودتنظیم‌گری بزنند تا کاربرانشان احساس امنیت داشته باشند و از شبکه‌های آنها گریزان نشوند. آنچه که محل سؤال اصلی این پژوهش است این است که کدام یک از الگوهای قانونگذاری در دنیا در عرصه حقوق کاربران در فضای مجازی الگوی موفق‌تری بوده است و می‌تواند برای قانونگذاری در ایران مورد توجه قرار گیرد؛ اتحادیه اروپا یا آمریکا؟

به موضوع قانون‌گذاری در زمینه حفاظت از داده‌ها یا قوانین مربوط به شبکه‌های اجتماعی و پلتفرم‌های دیجیتال تاکنون در آثار علمی بعضاً توجهاتی شده است. برای مثال مقاله «چالش‌های حفاظت از داده‌های خصوصی در حوزه اینترنت اشیا: مطالعه تطبیقی حقوق ایران و اتحادیه اروپا» به طور خاص به حوزه اینترنت اشیا و حفاظت از داده‌ها صرفاً در این حوزه اختصاص دارد و مقاله «اصول تدوین قوانین و مقررات برای اینترنت با تأکید بر مصوبات یونسکو و شورای اروپا» (۱۳۹۲) نیز که به حوزه قانونگذاری نسبت به فضای مجازی مرتبط است و بررسی تطبیقی نیز داشته است از یک سو پیش از تصویب مقررات عمومی حفاظت از داده‌ها در اروپا نگارش شده است و از سوی دیگر تجربه متفاوتی مثل قانونگذاری در نظام حقوقی آمریکا را مورد مذاقه قرار نداده است و از سوی دیگر طرح‌های فعلی در دست تصویب در مجلس نسبت به حقوق کاربران فضای مجازی مربوط به زمان انتشار آن نیست، و بر حقوق کاربران فضای مجازی نیز متمرکز نیست. مقاله «حریم خصوصی ارتباط اینترنتی (مطالعه در حقوق ایران و اتحادیه اروپا)» نیز که به حقی در فضای مجازی پرداخته است، به این حوزه از تقنین در آمریکا توجه نداشته است و به سایر حقوق کاربران غیر از حریم خصوصی توجه ندارد. همچنین است مقاله «حق فراموش شدن در ترازو؛ نیاز ناشی از فضای مجازی یا تهدیدی برای آزادی بیان؟!». بنابراین پژوهش حاضر به نظر می‌رسد از وجه بداعت و نوآوری در این حوزه برخوردار باشد.

چالش‌های قانونگذاری حقوق کاربران در فضای مجازی؛ مطالعه تطبیقی دو تجربه متفاوت

ضرورت قانون‌گذاری و ضابطه‌مند کردن فعالیت‌های سکوه‌های نشر مجازی (پلتفرم‌ها)

۱- ضرورت مقابله با سوء استفاده سکوه‌های نشر (پلتفرم‌ها) از اطلاعات کاربران و کاربران از یکدیگر در ابعاد اجتماعی، اقتصادی و فرهنگی

رشد بی‌سابقه آمار کاربران سکوه‌های نشر مزیت نسبی شدیدی برای آن‌ها نسبت به سایر عرصه‌های ارتباطات ایجاد کرده است که منشأ قدرت بسیار قابل توجهی برای مالکانشان شده و در نتیجه زمینه سوء استفاده از این قدرت و نقض حقوق شهروندی بسیار بیشتر شده است.

مقایسه رشد آمارهای کاربران فضای مجازی در دهه‌های اخیر گویای این قدرت است و ضرورت قاعده‌مند کردن و تحت انضباط قانونی درآوردن دو سویه رفتارهای سکوه‌های نشر و کاربران فضای مجازی را بیش از پیش روشن می‌کند. در حال حاضر شبکه‌های اجتماعی حدود چهار میلیارد و ۲۰۰ میلیون نفر کاربر فعال<sup>۱</sup> دارند که در دسامبر ۲۰۱۷ فیس‌بوک با ۲ میلیارد حساب ثبت‌شده و ۲/۱۳ میلیارد کاربر فعال<sup>۲</sup>، واتس‌اپ در ژانویه ۲۰۱۸ با ۲ میلیارد حساب ثبت‌شده و فعال<sup>۳</sup> و اینستاگرام با ۸۰۰ میلیون حساب ثبت‌شده و کاربر فعال در اوت ۲۰۱۷ از پرتعدادترین سکوه‌های نشر در جهان بوده‌اند که هر سه سکوه متعلق به شرکت فیس‌بوک آمریکاست<sup>۴</sup> و از این بین برای مثال واتس‌اپ تا مارس ۲۰۲۰ به ۲ میلیارد کاربر رسیده است<sup>۵</sup> و فیس‌بوک (با نام فعلی «متا»<sup>۶</sup>) در فصل اول ۲۰۲۲ به ۲ میلیارد و ۹۳۶ میلیون کاربر رسیده است.<sup>۷</sup>

در بین ایرانیان نیز مطابق گزارش مرکز آمار ایران در سال ۱۳۹۹ بیش از (۶۵٪) افراد ۱۵ ساله به بالا عضو شبکه‌های اجتماعی بوده‌اند که به ترتیب از شبکه‌های

۱. کاربر فعال کاربری است که بیش از یک ماه از عدم حضورش در یک پلتفرم نگذشته باشد.

2. [Newsroom.fb.com/company-info/](https://newsroom.fb.com/company-info/)

3. [Techcrunch.com/2018/31/01/whatsapp-hits-15-billion-monthly-users-19b-not-so-bad/](https://techcrunch.com/2018/31/01/whatsapp-hits-15-billion-monthly-users-19b-not-so-bad/)

4. [B2n.ir/a31347](https://b2n.ir/a31347) (fa.wikipedia.org)

5. [Statista.com/statistics/260819/number-of-monthly-active-whatsapp-users/](https://statista.com/statistics/260819/number-of-monthly-active-whatsapp-users/)

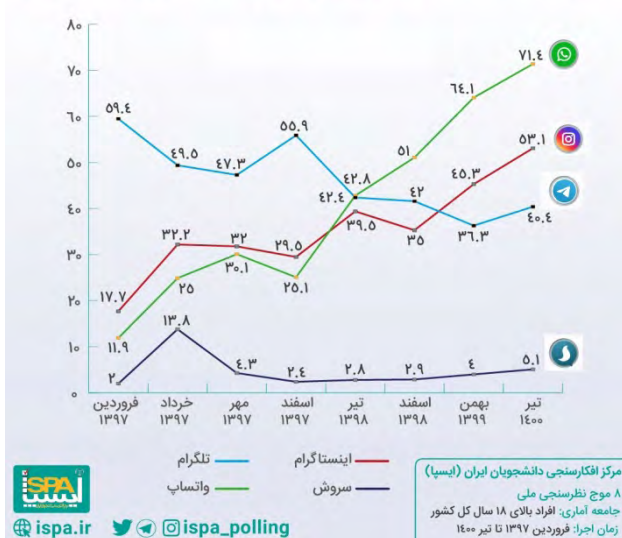
6. Meta

7. [statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/](https://statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/)

چالش‌های قانونگذاری حقوق کاربران در فضای مجازی؛ مطالعه تطبیقی دو تجربه متفاوت

اجتماعی واتس‌آپ (با ۸۸/۵٪ کاربر) و اینستاگرام (با ۶۸/۳٪ کاربر) بیشترین استفاده را کرده‌اند.<sup>۱</sup> همچنین روند استفاده از پلتفرم‌های مختلف به جز برخی موارد مانند تلگرام که با پالایش و فیلترینگ مواجه شده‌اند، افزایش شدیدی داشته است به ویژه کاربران سکوه‌های نشر خارجی که تفاوت محسوسی با کاربران داخلی داشته‌اند.

### روند استفاده مردم ایران از رسانه‌های اجتماعی



### منبع: نظرسنجی ایسپا<sup>۲</sup>

کسب و کارهای سکوه‌های نشر از جمله مهمترین عرصه‌های نفوذ این سکوها در بعد اقتصادی زندگی کاربران فضای مجازی هستند. در نقطه مقابل کسب و کارهای سنتی که با اصطلاح پایپ لاین<sup>۳</sup> یا کسب و کار خطی نیز شناخته می‌شوند، کسب و کار در بستر سکوه‌های نشر دیجیتالی با چالش‌هایی از قبیل ورود خسارت

۱. قابل مشاهده در نشانی زیر (آخرین بازدید: خرداد ۱۴۰۱):

amar.org.ir/Portals/0/amarmozuui/infographics/Virtual%20network\_99.pdf

۲. قابل مشاهده در تارنمای مرکز رصد فرهنگی کشور (ircud.ir) به نشانی زیر (آخرین بازدید خردادماه

b2n.ir/j62017 : (۱۴۰۱)

3. Pipeline

چالش‌های قانونگذاری حقوق کاربران در فضای مجازی؛ مطالعه تطبیقی دو تجربه متفاوت

به کاربران و به تبع آن مسئولیت مدنی سکوه‌های نشر مواجه هستند.

افزون بر اینکه نقض حریم خصوصی در مبادله اطلاعات با سامانه‌های رایانه‌ای می‌تواند بنا بر مواد ۱ و ۲ قانون مسئولیت مدنی ضمان‌آور باشد، ارائه اطلاعات غلط یا افشانشده از طریق شبکه‌های ارتباطی هم می‌تواند موجب صدمه به اعتبار تجاری یا شخصی شده یا نقض قواعد رقابت عادلانه باشد و با اعمال قواعد حمایت از رقابت سالم و شهرت تجاری در فضای مجازی، علاوه بر ضمان خاطی، تأمین‌کننده ارتباط اینترنتی هم با عدم دقت در بازرسی یا مدیریت داده‌های ورودی و خروجی می‌تواند مسئول شناخته شود که هرچند از نظر برخی مسئولیت اخیر در فضای مجازی قاعده جدیدی نمی‌طلبد؛ (السان، ۱۳۹۳، ۴۰-۴۱) اما از نگاه برخی دیگر قواعد حقوقی در فضای مجازی بعضاً از فضای واقعی متفاوت می‌شود. کما اینکه برخی بیان می‌کنند که در فضای مجازی برخلاف دنیای واقعی اصل بر حریم خصوصی نیست؛ بلکه اصل بر فضای عمومی است. (Basu & Jones, 2007, 2) لذا تفاوت دنیای واقعی و مجازی می‌تواند بر تغییر برخی قواعد عمومی از جمله قواعد مسئولیت مدنی در فضای مجازی نیز مؤثر باشد، کما اینکه همچنان که خواهیم گفت در بخش ۲۳۰ قانون نزاکت ارتباطات آمریکا اصل بر عدم مسئولیت پلتفرم‌ها در قبال کنش‌های کاربران است.

یکی از آخرین نمونه‌های سوء استفاده‌های سکوه‌های نشر دیجیتال از اطلاعات کاربران را می‌توان در پرونده شکایت یک متخصص حقوق رقابت و مشاور ارشد سازمان نظارت بر رفتار مالی انگلیس به نام لیزا لودال گرمسن علیه شرکت فیس‌بوک مشاهده کرد. فیس‌بوک به جهت سوء استفاده از اطلاعات خصوصی حدود ۴۵ میلیون کاربر بین سال‌های ۲۰۱۵ تا ۲۰۱۹ در این پرونده طرف شکایت قرار گرفته است بر این اساس که با تحمیل شرایط کاربری ناعادلانه به کاربران خود میلیاردها پوند درآمد داشته است و موقّق شده است اطلاعات خصوصی کاربران را از طریق امکانات این شبکه اجتماعی گردآوری کند که این شکایت دستجمعی به دنبال حداقل حداقل ۳/۲ میلیارد دلار غرامت است.<sup>۱</sup>

1. [openmarketsinstitute.org/publications/huk-class-action-suit-looms-over-facebook-insights-from-claimant-liza-lovdahl-gormsen](https://openmarketsinstitute.org/publications/huk-class-action-suit-looms-over-facebook-insights-from-claimant-liza-lovdahl-gormsen)

چالش‌های قانونگذاری حقوق کاربران در فضای مجازی؛ مطالعه تطبیقی دو تجربه متفاوت

بیش از این نیز برای اولین بار پرونده آلمانی فیس‌بوک تعامل بین حفاظت از داده‌ها و قانون رقابت بحث برانگیز شد. در این پرونده نظریه آسیبا دفتر کارتل فدرال آلمان<sup>۲</sup> که مربوط به نقض حریم خصوصی با تقویت قدرت بازار فیس‌بوک بود، پس از مناقشه در دادگاه تجدیدنظر این نظریه به وسیله دادگاه عالی فدرال آلمان<sup>۳</sup> تأیید شد. در نتیجه یک اقدام اجرایی علیه فیس‌بوک طبق ماده ۱۰۲ معاهده عملکرد اتحادیه اروپا (TFEU) رخ داد و ثابت شد که استراتژی فیس‌بوک با استفاده از سیاست حفظ حریم خصوصی، از مصرف‌کنندگان سوء استفاده می‌کند؛ زیرا باعث آسیب آشکار مصرف‌کننده در بازار شبکه‌های اجتماعی به شکل عدم انتخاب و کاهش کیفیت می‌شود. (Lodvdahl Gormsen, Tomas Llanos, 2021: 90) از آنجایی که ترجیح ذاتی مردم برای حفظ حریم خصوصی مانع رشد فیس بوک بود، فیس بوک برای دسترسی به داده‌های کاربر تا حد امکان به نفوذ در حریم خصوصی و فریب متوسل شد و در نتیجه قدرت بازار را به دست آورد. در حال حاضر، موقعیت غالب فیس‌بوک در بازار رسانه‌های اجتماعی به این معنی است که مهم نیست فیس‌بوک چقدر داده از کاربران استخراج می‌کند یا اینکه اطلاعاتش در مورد شیوه‌های پردازش داده‌هایش چقدر شفاف است و چقدر رسوایی‌های حفظ حریم خصوصی ناشی از مدیریت بی‌ملاحظه‌ی داده‌ها به وسیله فیس‌بوک است؛ زیرا کاربران هیچ جای دیگری برای رفتن ندارند، در نتیجه افزون‌تر حفاظت از کاربران و داده‌هایشان، اقدامات ضدّ انحصاری نیز ضروری است. (Lodvdahl Gormsen, Tomas Llanos, 2019: 1)

## ۱ - ۲. ضرورت حفظ استقلال سیاسی کشورها در مقابل سکوه‌های نشری بزرگ

قدرت بی‌سابقه شرکت‌های سکوه‌های نشری بزرگ در حدّی است که بر ابعاد حاکمیتی دولت‌ها نیز اثر می‌گذارند و حتّی می‌توانند به جریان‌های سیاسی و انتخابات و غیره در راستای منافع خود جهت‌دهی کنند که نقض استقلال کشورهای دیگر و خدشه به حاکمیت را نیز در پی دارد. در صورت فقدان پیش‌بینی‌های لازم در قوانین و مقرّرات هر کشوری، چالش‌ها و فسادهای کلانی رخ خواهد داد که

1. Theory of harm
2. Bundeskartellamt
3. Bundesgerichtshof

چالش‌های قانونگذاری حقوق کاربران در فضای مجازی؛ مطالعه تطبیقی دو تجربه متفاوت

اشخاص عادی از عهده احقاق خود یا حقوق عمومی بر نخواهند آمد و حتی دولت هم در این زمینه مشکلات عدیده‌ای خواهد داشت.

آنچه که پرونده رسوایی داده‌های فیس‌بوک و کمبریج آنالیتیکا نام دارد<sup>۱</sup> گویای توان سوءاستفاده سیاسی سکوه‌های نشری از اطلاعات کاربران است. در دهه ۲۰۱۰، اطلاعات شخصی میلیون‌ها کاربر فیس‌بوک بدون رضایت آنها به وسیله شرکت مشاوره بریتانیایی کمبریج آنالیتیکا جمع‌آوری شد که عمدتاً برای کمپین تبلیغات سیاسی استفاده می‌شد.<sup>۲</sup> این داده‌ها از طریق برنامه کاربردی به نام «این زندگی دیجیتال شماست»<sup>۳</sup> که به وسیله محقق علوم داده، الکساندر کوگان و شرکت او که در سال ۲۰۱۳ تأسیس شده است، جمع‌آوری شده بود. این برنامه شامل مجموعه‌ای از سؤالات برای ایجاد پروفایل‌های روان‌شناختی روی کاربران بود و اطلاعات شخصی دوستان فیس‌بوک کاربران را از طریق سکوی نشر «اوپن گراف فیس‌بوک» جمع‌آوری می‌کرد. این برنامه کاربردی اطلاعات ۸۷ میلیون پروفایل فیس‌بوک را جمع‌آوری کرده بود.<sup>۴</sup> کمبریج آنالیتیکا از داده‌ها برای ارائه کمک‌های تحلیلی به کمپین‌های ریاست‌جمهوری تد کروزر و دونالد ترامپ در سال ۲۰۱۶ استفاده کرد.<sup>۵</sup> این پرونده تا جایی پیش رفت که در ژوئیه ۲۰۱۹، اعلام شد که فیس‌بوک به دلیل نقض حریم خصوصی، قرار است ۵ میلیارد دلار به وسیله کمیسیون تجارت فدرال جریمه شود.<sup>۶</sup> در کشورهایی مثل آمریکا که دارند بزرگترین این شرکت‌هاست هرچند قوانینی مانند قانون نزاکت ارتباطات (The Communications Decency Act) سال‌ها قبل تصویب شده بود؛ اما تحوّل این شبکه‌های اجتماعی احساس نیاز تغییر به روز قوانین را در آنجا نیز ملموس کرده است.

1. Facebook-Cambridge Analytica data scandal

2. [businessinsider.com/cambridge-analytica-whistleblower-christopher-wylie-facebook-data-2019-1](https://www.businessinsider.com/cambridge-analytica-whistleblower-christopher-wylie-facebook-data-2019-1)

3. "This Is Your Digital Life"

4. [cnbc.com/2018/10/04/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html](https://www.cnbc.com/2018/10/04/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html)

5. [nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html](https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html)

6. [theguardian.com/technology/2019/jul/12/facebook-fine-ftc-privacy-violations](https://www.theguardian.com/technology/2019/jul/12/facebook-fine-ftc-privacy-violations)

## ۲ - نگاهی بر سابقه قانون‌گذاری فضای مجازی در اروپا و آمریکا و چالش‌های آنها

به طور کلی قانون‌گذاری حوزه فضای مجازی در الگوهای سایر نقاط جهان را در دو سطح منطقه‌ای و ملی می‌توانیم مشاهده کنیم. مراد از منطقه‌ای در اینجا حوزه‌ای متشکل از چند کشور است که در موضوعات مختلفی از جمله در حوزه فضای مجازی از قواعد حقوقی یکسان و مشابهی تبعیت می‌کنند که بارزترین مثال آن را می‌توان در قانون‌گذاری اتحادیه اروپا (European Union) ملاحظه کرد. از سوی دیگر با توجه به گسترش و توسعه بزرگترین شرکت‌های فضای مجازی در ایالات متحده آمریکا، این کشور را به عنوان مثالی برای قانونگذاری در سطح ملی برگزیدیم تا بتوان هر دو مدل قانونگذاری را با ایران مقایسه کرد.

### ۲ - ۱. تجربه قانونگذاری اتحادیه اروپا

اولین سند حقوقی الزام‌آور بین‌المللی برای حفاظت از داده‌ها، کنوانسیون شورای اروپا در خصوص حمایت از اشخاص در زمینه پردازش داده‌های شخصی بود که برای امضا در سال ۱۹۸۱ مفتوح گذاشته شد. دستورالعمل پارلمان و شورای اروپا نیز که در ماده (۲) «داده شخصی» را هرگونه اطلاعات مربوط به شخص حقیقی شناسایی‌شده یا قابل شناسایی تعریف می‌کند، در ماده (۸) استانداردهای بالاتری را برای پردازش داده‌های حساس با منشأ نژادی و قومی، عقاید سیاسی و مذهبی و یا فلسفی و عضویت در اتحادیه‌های تجاری و داده‌های مربوط به سلامتی یا زندگی جنسی ارائه می‌دهد که این الگوی حفاظت از داده‌ها علاوه بر توجه در قوانین ملی کشورهای عضو، مورد توجه بسیاری از کشورهای غیر اروپایی نیز بوده است. (کولزا، ۱۴۰۰: ۹۵-۹۶)

قانون حمایت داده‌ها (Data Protection Act (DPA)) مصوب ۱۹۹۸ انگلیس هشت اصل در مورد حمایت بدین شرح مقرر کرده بود: پردازش منصفانه و قانونی داده، منع پردازش مغایر با هدف تحصیل داده شخصی، منع فراتر رفتن از هدف پردازش داده، لزوم صحت و روزآمدی داده‌ها، منع نگهداری بیش از زمان لازم برای مقاصد خاص داده، لزوم پردازش داده مطابق حقوق شخص موضوع داده، اقدام سازمانی و فنی علیه پردازش غیرمجاز یا تخریب اتّفاقی داده و منع انتقال داده شخصی به خارج از محدوده اقتصادی اروپا مگر با حمایت آن کشور از حقوق و

آزادی اشخاص موضوع داده.

دستورالعمل ۱۹۸۱ اتحادیه اروپا نیز اصولی مشابه همین اصول در حمایت از داده‌ها مقرر کرده بود. (نوری، نجوانی، ۱۳۸۳: ۸۷-۸۸ و ۱۰۱) با تحوّل روزافزون فضای مجازی مقررات سابق در سطح اروپا کارایی لازم را نداشتند، لذا اتحادیه اروپا اقدام به وضع مقررات روزآمدتری نمود.

ازجمله جدیدترین اسناد حقوقی که اتحادیه اروپا به موجب آن صیانت از داده‌های شخصی را در برنامه خود قرار داده است، «مقرّرات عمومی حفاظت از داده‌ها» (General Data Protection Regulation (GDPR)) نام دارد. این مقرّرات که مصوّب ۱۴ آوریل سال ۲۰۱۶ و لازم‌الاجرا شده از تاریخ ۲۵ می ۲۰۱۸ است<sup>۱</sup> و جایگزین قانون حمایت از داده (DPA) شده است، اجرایش در کشورهای عضو اتحادیه منوط بر تصویب قوانین ملی نیست. ۲. بر اساس ماده (۳) این مقرّرات در صورتی که کنترل‌کننده (سازمانی که داده‌ها را از افراد مقیم اروپا گردآوری می‌کند)، یا پردازنده (سازمانی که داده را به نمایندگی از کنترل‌کننده پردازش می‌کند مانند فراهم‌کننده خدمات ابری)، یا موضوع داده (شخص) در اروپا باشد، مقرّرات قانون نافذ خواهد بود.<sup>۳</sup>

بر اساس ماده (۶) این مقرّرات پردازش داده‌ها تنها با تحقّق یکی از شروط زیر مجاز می‌شود:

۱. اگر شخص موضوع داده با پردازش داده‌های شخصی خود موافقت کرده باشد.

۲. برای تحقّق الزامات قراردادی با شخص موضوع داده یا برای ایفای تعهداتی که به واسطه درخواست شخص موضوع داده که در فرایند عقد قرارداد یا کنترل‌کننده داده قرارداد دارد.

1 . <https://gdpr-info.eu/art-99-gdpr/>

2 . Blackmer, W.S. (5 May 2016). "GDPR: Getting Ready for the New EU General Data Protection Regulation". Information Law Group. InfoLawGroup LLP. Archived from the original on 14 May 2018. Retrieved 22 June 2016.

3 . <https://gdpr-info.eu/art-3-gdpr/>

چالش‌های قانونگذاری حقوق کاربران در فضای مجازی؛ مطالعه تطبیقی دو تجربه متفاوت

۳. برای رعایت تکالیف قانونی کنترل‌کننده داده.

۴. برای حفاظت از منافع حیاتی شخص موضوع داده یا یک شخص دیگر.

۵. برای اجرای وظیفه‌ای در جهت منافع عمومی یا انجام وظیفه یک مرجع رسمی.

۶. برای منافع مشروع کنترل‌کننده داده یا یک شخص ثالث، مگر اینکه این منافع با منشور حقوق بنیادی اتحادیه اروپا در تعارض باشد. (به ویژه در مورد کودکان)

همان‌طور که مشاهده می‌شود، هیچ یک از کنترل‌کننده‌ها یا پردازنده‌های داده نمی‌توانند خارج از موارد مجاز مذکور از اطلاعات افراد استفاده‌ای کنند و ضمانت اجراهای لازم با وضع جریمه تا سقف ۲۰ میلیون یورو در مواد بعدی این مقررات نیز وضع شده است. علیرغم مزایایی که این مقررات نسبت به وضعیت پیش از آن داشته است، برخی کشورها مانند آمریکا برای الگوبرداری از این مقررات آن را مورد آسیب‌شناسی قرار داده‌اند و مواردی از قبیل نمونه‌های زیر را از نواقص این مقررات بر شمرده‌اند:

الف) اشکالات ناظر به حق رقابت عادلانه:

مقررات عمومی حفاظت از داده‌ها بزرگترین بازیگران فضای مجازی را تقویت می‌کند؛ (Layton, 2019: 3) زیرا اتفاقاتی رخ داده است؛ مانند اینکه شرکت‌های بزرگ بودجه ارتقای نرم‌افزار و به‌کارگیری متخصصان حریص خصوصی را دارند و کاربران، از سکوه‌های نشر جدید کمتر استفاده می‌کنند. (Campbell, 2015: 71) مقررات عمومی حفاظت از داده‌ها شرکت‌های کوچک و متوسط را تضعیف می‌کنند. مقررات عمومی حفاظت از داده‌ها برای بسیاری از شرکت‌ها هزینه بالایی دارند. (Layton, 2019: 3) امروزه برای انجام تجارت در اتحادیه اروپا، یک شرکت متوسط با حدود ۵۰۰ کارمند، باید حدود ۳ میلیون دلار هزینه کند تا از مقررات عمومی حفاظت از داده‌ها پیروی کند. (10-iapp report, 2019: 1)

سه اشکال یادشده در مقررات عمومی حفاظت از داده‌ها ناظر به تقویت انحصارگری شرکت‌های غول‌آسا به ویژه پنج‌گانه گام (گوگل، آمازون، فیس‌بوک،

چالش‌های قانونگذاری حقوق کاربران در فضای مجازی؛ مطالعه تطبیقی دو تجربه متفاوت

اپل و مایکروسافت) است که با اصول حقوق رقابت نیز در تعارض بوده و با سیاست‌های سایر کشورها در حمایت از رقابت‌پذیر بودن فعالیت شرکت‌های تجاری به ویژه شرکت‌های ارائه دهنده خدمات مجازی از جمله در ایران و حتی خود آمریکا که پنج غول بزرگ در آن قرار دارد، نیز سازگار نیست.

ب) اشکال ناظر به حق آزادی بیان:

مقررات عمومی حفاظت از داده‌ها آزادی بیان را محدود می‌کند به نحوی که از زمان اجرای آن تا حدود یک سال بعد بیش از ۱۰۰۰ سایت خبری اروپایی بسته شده‌اند. (South, 2018: 10) هرچند محدودیت آزادی بیان در اینجا مستقیم رخ نداده است؛ اما به صورت غیرمستقیم نیز دست کم برای کشورهای که حدود آزادی بیان در آنها با کشورهای محل اجرای مقررات عمومی حفاظت از داده‌ها تفاوت دارد، می‌تواند نقض آزادی قانونی و حقوق شهروندی به حساب آید. لذا به تناسب قوانین و مقررات هر کشور این مقررات باید بومی شود.

ج) اشکالات ناظر به حق امنیت کاربران:

مقررات عمومی حفاظت از داده‌ها خطر امنیت سایبری را افزایش می‌دهد. (Layton, 2019: 7) یک پیامد ناخواسته مقررات عمومی حفاظت از داده‌ها این است که شفافیت سیستم‌ها و معماری بین‌المللی اینترنت را تضعیف می‌کند. پروتکل پرسوجو و پاسخ هویز (WHOIS) برای نام‌های دامنه اینترنتی، آدرس‌های IP و سیستم‌های مستقل به‌وسیله مجریان قانون، متخصصان امنیت سایبری و محققان و دارندگان علائم تجاری و حقوق مالکیت معنوی استفاده می‌شود. (Tews, 2018) مقررات عمومی حفاظت از داده‌ها به هیچ وجه در مورد اطلاعات غیرشخصی اعمال نمی‌شود و بیان می‌کند که افشای حتی اطلاعات شخصی می‌تواند برای مواردی مانند حفاظت از مصرف کننده، امنیت عمومی، اجرای قانون، اجرای حقوق، امنیت سایبری و مبارزه با کلاهبرداری تضمین شود. مشکل هویز را می‌توان به عنوان تضاد بین حق حریم خصوصی افراد و حق دانستن عمومی توصیف کرد. همچنین می‌توان آن را در چارچوب مشکل «بیش از حد حریم خصوصی» درک کرد که در آن انگیزه برای محافظت از حریم خصوصی مطلق می‌شود، با سایر حقوق تعادل ندارد و ناخواسته نتایج بدتری برای حفظ حریم خصوصی و داده‌ها به همراه دارد. (Brkan, 2016: 81)

چالش‌های قانونگذاری حقوق کاربران در فضای مجازی؛ مطالعه تطبیقی دو تجربه متفاوت

(د) اشکالات ناظر به حریم خصوصی کاربران:

مقررات عمومی حفاظت از داده‌ها و قانون حریم خصوصی مصرف‌کننده کالیفرنیا (CCPA) خطراتی را برای سرقت هویت و کلاهبرداری آنلاین ایجاد می‌کند. مقررات عمومی حفاظت از داده‌ها اعتماد بیشتری به صورت آنلاین ایجاد نکرده است. مقررات عمومی حفاظت از داده‌ها و قانون حریم خصوصی مصرف‌کننده کالیفرنیا از تظاهر به کنترل مشتری برای افزایش قدرت دولت استفاده می‌کنند. (10-Layton, 2019: 8)

(ه) اشکالات ناظر به حق تحقیق و آموزش کاربران:

مقررات عمومی حفاظت از داده‌ها نوآوری و تحقیق را تهدید می‌کند. همچنین مقررات عمومی حفاظت از داده‌ها و قانون حریم خصوصی مصرف‌کننده کالیفرنیا نمی‌توانند به طور معناداری نقش ارتقای حریم خصوصی و نوآوری و آموزش مصرف‌کننده را در حفاظت از داده‌ها لحاظ کنند.<sup>۱</sup> (11-Layton, 2019, 6 & 10)

(و) اشکال ناظر به شفافیت در تصمیم‌گیری‌های الگوریتمی

زمانی که داده‌ها خودکار پردازش می‌شود، فرد موضوع داده حق دارد که از سوی کنترل‌کننده داده از «منطق» موجود در پس تصمیم‌گیری مطلع شود. (کری و ساندرز، ۱۳۸۶: ۲۸۲) در خصوص تصمیم‌گیری الگوریتمی یا خودکار در سامانه‌ها و پلتفرم‌های فضای مجازی علی‌رغم اینکه مقررات عمومی حفاظت از داده‌ها (GDPR) و دستورالعمل حفاظت از داده‌ها (Directive on Data Protection) این حق را به شخص موضوع داده می‌دهند که تحت یک تصمیم کاملاً خودکار از جمله نمایه‌سازی قرار نگیرد، استثنائات این حق به قدری زیاد است که خود استثنایها به یک اصل تبدیل می‌شوند. در حالی که شفافیت الگوریتمی می‌تواند مانع سوگیری‌های تبعیض آمیز در فرآیند تصمیم‌گیری شود و از سوی دیگر موجب شود که پاسخگویی بین توسعه‌دهنده و کاربر الگوریتم توزیع شود و با ارائه داده به وسیله کاربر، او نیز مسئول یادگیری الگوریتمی در سامانه‌های هوشمند باشد. (25-Brkan, 2019: 24)

۱. برای مطالعه بیشتر رجوع کنید به نشانی زیر:

<https://www.judiciary.senate.gov/imo/media/doc/Layton%20Testimony1.pdf>

علیرغم اشکالات فوق به دلیل تحولاتی که مقررات مزبور نسبت به حفاظت از داده‌ها در بر داشت مورد توجه برخی کشورهای دیگر یا حتی برخی ایالات در آمریکا قرار گرفت. در این زمینه ایالت کالیفرنیا قانون حفظ حریم خصوصی مصرف کنندگان کالیفرنیا (CCPA) را در ۲۸ ژوئن ۲۰۱۸ تصویب کرد که از ۱ ژانویه ۲۰۲۰ لازم‌الاجرا شد.<sup>۱</sup> این قانون حقوق شفافیت و کنترل جمع‌آوری اطلاعات شخصی به‌وسیله شرکت‌ها را به روشی مشابه مقررات عمومی حفاظت از داده‌ها اعطا می‌کند. دو ایالت دیگر نیز قوانین مشابهی را تصویب کرده‌اند: قانون حفظ حریم خصوصی داده‌های مصرف‌کننده در ۲ مارس ۲۰۲۱ در ویرجینیا (CDPA)<sup>۲</sup> و قانون حفظ حریم خصوصی کلرادو در ۸ ژوئیه ۲۰۲۱/۴<sup>۳</sup> جمهوری ترکیه نیز قانون حفاظت از داده‌های شخصی را در ۲۴ مارس ۲۰۱۶ مطابق با قوانین اتحادیه اروپا تصویب کرده است.

آخرین قانونی که در زمینه حقوق کاربران فضای مجازی به تصویب اتحادیه اروپا رسیده است، قانون خدمات دیجیتال (DSA)<sup>۴</sup> نام دارد که پیشنهاد قانونی کمیسیون اروپا برای نوسازی دستورالعمل تجارت الکترونیک<sup>۵</sup> در مورد محتوای غیرقانونی، تبلیغات شفاف و اطلاعات نادرست است. با تغییر فضای مبادلات در سکوه‌های نشر دیجیتال حقوق کاربران را نیز نمی‌توان با قواعد سنتی به شکل کاملی حمایت کرد که برای مثال می‌توان به جایگزینی مالکیت با حق دسترسی در فضای مجازی اشاره کرد که هم سکوه‌های نشر دیگر مالک محصول و کالای اصلی کسب و کارشان نیستند و هم کاربران به جای تملک کالا یا خدمات به هر کالا و خدماتی از هر نقطه‌ای دسترسی پیدا می‌کنند. (کدخدایی، فراهانی، ۱۴۰۱: ۱۹) لذا صیانت از این حقوق جدید قوانین جدیدی می‌طلبد و ضرورت تصویب قانون خدمات دیجیتال و قوانینی از این دست در سایر حوزه‌ها از این زاویه روشن‌تر می‌شود.

1 . California Consumer Privacy Act

2 . <https://b2n.ir/g17898>

3 . Consumer Data Protection Act

4 . [iapp.org/news/a/colorado-privacy-act-becomes-law/](http://iapp.org/news/a/colorado-privacy-act-becomes-law/)

5 . Digital Services Act

۶ . (e-Commerce Directive) یا (Electronic Commerce Directive) مصوب سال ۲۰۰۰ بوده و یک چارچوب بازار داخلی برای خدمات آنلاین ایجاد می‌کند که هدفش حذف موانع خدمات آنلاین فرامرزی در بازار داخلی اتحادیه اروپا و ایجاد اطمینان حقوقی برای مشاغل و مصرف‌کنندگان است.

چالش‌های قانونگذاری حقوق کاربران در فضای مجازی؛ مطالعه تطبیقی دو تجربه متفاوت

این قانون شبکه‌های رسانه‌های اجتماعی و بازارها را مسئول نظارت بر محتوای سایت‌هایشان می‌کند و تعهدات خدمات واسطه مانند IP و ثبت دامنه را در این موارد مقرر کرده است: گزارش شفافیت، الزامات مربوط به شرایط خدمات با توجه به حقوق اساسی، همکاری با مقامات ملی، نقاط تماس و در صورت لزوم نماینده قانونی، ممنوعیت تبلیغات برای کودکان، بررسی اعتبار تأمین کنندگان شخص ثالث و انطباق با طراحی، تعهدات مدیریت ریسک و واکنش به بحران، حسابرسی خارجی و مستقل، عملکرد انطباق داخلی، و پاسخگویی عمومی، انتخاب کاربر برای نداشتن توصیه‌هایی بر اساس پروفایل، به اشتراک‌گذاری داده‌ها با مقامات و محققان، کدهای رفتار و همکاری در واکنش به بحران.<sup>۱</sup> اغلب این تعهدات سکوه‌های نشر را ملزم به رعایت حقوق کاربرانشان در فعالیت‌های اقتصادی و تجاری کاربران در فضای مجازی می‌کند و حتی در رعایت حقوق کاربران به وسیله سایر کاربران نیز بی‌تأثیر نیست و از سوی دیگر سایر حقوق غیر اقتصادی کاربران نیز که به نحوی متأثر از روابط اقتصادی در فضای مجازی هستند از حمایت بی‌بهره نمی‌مانند.

## ۲ - ۲. تجربه قانونگذاری ایالات متحده آمریکا

در ایالات متحده آمریکا قوانین مختلفی به حقوق کاربران در فضای مجازی ارتباط پیدا می‌کند. برای نمونه می‌توان به ویژه به قوانینی که از جهت حمایت از حریم خصوصی چه به شکل عام که شامل فضای واقعی و مجازی باشد و یا به طور خاص با حریم خصوصی در فضای رقومی (دیجیتال) مرتبط باشد می‌توان اشاره کرد. اهم این موارد عبارتند از: قانون گزارش اعتبار (۱۹۷۰)، قانون حریم خصوصی (۱۹۷۴)، قانون حقوق آموزشی خانواده و حریم خصوصی (۱۹۷۴)، قانون حریم خصوصی تلویزیون کابلی (۱۹۸۴)، قانون حریم خصوصی ارتباطات الکترونیکی (۱۹۸۶)، قانون حمایت حریم خصوصی برخط کودکان (COPA)<sup>۲</sup> (۱۹۹۸)، قانون گرام - لیچ (۱۹۹۹)، قانون حریم خصوصی ارتباطات الکترونیکی (۲۰۰۰). این قبیل قوانین آمریکا از داده‌های بنگاه‌ها و دولت در مورد افراد حمایت نمی‌کنند، محدودیتی برای جریان داده بین شرکت‌ها ندارند و داده مردم را کالایی مصرفی تلقی می‌کنند؛ اما نهایتاً به حریم خصوصی پایبندند. (نوری، نخجوانی، ۱۳۸۳: ۱۰۴-۱۰۵)

1. en.wikipedia.org/wiki/Digital\_Services\_Act#cite\_note-ft202010283-

2. Child Online Protection Act

همچنین از دیگر قوانین آمریکا می‌توان به قانون محافظت اینترنتی از کودکان معروف به قانون سیپا (CIPA)<sup>۱</sup> مصوب ۲۰۰۰ در خصوص فیلترینگ در سطح فدرال و ایالتی، قانون میهن‌پرست آمریکایی معروف به پاتریوت<sup>۲</sup> مصوب ۲۰۰۱ (پس از انهدام برج‌های دوقلو) با هدف اعطای گسترده‌ترین اختیارات رصد و جاسوسی و کنترل به اداره تحقیقات کشوری (FBI)، قانون حمایت از مصرف‌کنندگان رسانه‌های دیجیتال<sup>۳</sup> اشاره کرد. در اینجا محوریت بحث ما بیشتر با قانون نزاکت ارتباطات آمریکا مرتبط است که در ادامه توضیح می‌دهیم.

### نسبت مسئولیت سکوهای نشر (پلتفرم‌ها) با بخش ۲۳۰ قانون نزاکت ارتباطات آمریکا

یکی از چالش‌برانگیزترین قوانین آمریکا بخش ۲۳۰ قانون نزاکت ارتباطات آمریکا (The Communications Decency Act Section 230) است که در سال ۱۹۹۶ به قانون نزاکت ارتباطات ۱۹۳۴ آمریکا الحاق شده است و در راستای تأمین مصونیت ارائه‌دهندگان خدمات اینترنتی که شامل سکوهای نشر و شبکه‌های اجتماعی امروزی نیز می‌شود، اینگونه مقرر کرده است: «با هیچ ارائه‌دهنده یا کاربر خدمات رایانه‌ای تعاملی نباید به مثابه ناشر یا سخنران اطلاعاتی که به وسیله دیگر ارائه‌دهنده محتوای اطلاعات فراهم شده است، برخورد شود.» این قانون که مدّت کوتاهی پس از همه‌گیر شدن اینترنت جهانی به تصویب رسید، افزون بر هدف تأمین آزادی بیان، در واقع در پی جذب کاربران سراسر جهان به شرکت‌های رسانه‌ای جدید بود و تا حدود زیادی در رسیدن به این هدف ایالات متحده موفق عمل نمود.

ازجمله آثار مصونیتی که با بخش ۲۳۰ برای فضای مجازی و به ویژه سکوهای نشر در این فضا به بار آمده است می‌توان به پیشرفت اینترنت و هوش مصنوعی اشاره کرد. این قانون به تعبیر برخی حقوقدانان حقوق فضای مجازی در آمریکا: «شاید اثرگذارترین قانون برای محافظت از نوآوری‌هایی است که به اینترنت اجازه

1. Children's Internet Protection Act
2. USA Patriot Act
3. Digital Media Consumers' Rights Act

چالش‌های قانونگذاری حقوق کاربران در فضای مجازی؛ مطالعه تطبیقی دو تجربه متفاوت

رشد داده است.» (Balkin, 2014: 2313) در دنیای «وب ۲»<sup>۱</sup> که کاربران را قادر به خلق محتوا در فضای مجازی می‌کند، عدم مسئولیت سکوه‌های نشر توسعه‌دهنده آنهاست. مثلاً در مورد نشان‌ها<sup>۲</sup> که به افراد کمک می‌کنند تا دریابند کدام کاربران بیشتر به آنها اطلاعات مفیدی می‌دهند و به صاحبان سایت اجازه می‌دهند تا اعضای انجمن را برای کمک به حفظ کنترل بر سیل رو به رشد اطلاعات توانمند کنند، بخش ۲۳۰ تا کنون کمک بزرگی بوده است؛ زیرا هم به طور کلی اجازه می‌دهد تا سایت‌های وب ۲ وجود داشته باشند و هم به طور خاص صاحبان سایت‌ها را برای استفاده از کاربران دارای نشان تشویق می‌کند. (HARV. L. REV., 2010: 1002) از سوی دیگر این قانون موجب نابرابری قدرت طرفین ارائه‌دهنده خدمات مجازی (پلتفرم‌ها) و کاربران، نیز شده است.

### مبنای مسئولیت و خودتنظیم‌گری<sup>۳</sup> سکوه‌های نشر (پلتفرم‌ها)

اختلاف نظرانی در مورد مبنای مسئولیت حقوقی سکوه‌های نشر در مقام دارندگان اطلاعات اشخاص وجود دارد. برخی حقوقدانان مثل بالکین آن‌ها را مانند وکلا و پزشکان امانتدار اطلاعات کاربران می‌دانند (Balkin, 2016: 1183) و در مقابل برخی دیگر مانند خان و پوزن در مقابل یک مدل امانتداری نوظهور، دیدگاهی شکاکانه از امانتداران اطلاعات، ارائه می‌دهند (Khan & Pozen, 2019: 497) و برخی دیگر مدعی‌اند که در نظر گرفتن سایر روابط امانتداری مانند رابطه امین و ذی‌نفع ممکن است مبنای محکم‌تری برای مدل امانتداری اطلاعاتی فراهم کند. (Haupt, 2020: 34) فارغ از اینکه کدام مینا را برای مسئولیت سکوه‌های نشر مجازی بپذیریم، اجمالاً حدی از مسئولیت را از نگاه‌های مختلف باید برای آنان قائل شد و قدر متقیّن در مواردی که سکوه‌های نشر در نگهداری از داده‌ها تقصیری مرتکب شده‌اند و از آنها سوءاستفاده کرده‌اند، مصونیت مطلق آنها بلاوجه است.

از سوی دیگر افزون بر مسئولیت نسبت به صاحبان داده‌ها، سکوه‌های نشر نسبت به اطلاعات منتشرشده به‌وسیله کاربران نیز دستکم در مواردی که آگاهانه

1. Web 2.0
2. Badges
3. Self-regulation

نه تنها مانع وقوع جرائم مجازی نشده‌اند، بلکه با عدم برخورد و تهدید کاربری مجرمان زمینه‌ساز ارتکاب جرم شده‌اند، مسئولیت دارند. توضیح آنکه با وجود مصونیت ناشی از بخش ۲۳۰ قانون نزاکت ارتباطات آمریکا وجود حدی از مسئولیت برای سکوه‌های نشر را نمی‌شد انکار کرد و از آنجا که این قانون برای نظام شبکه‌های اجتماعی تدوین نشده بود و در زمان قانونگذاری تعداد کمی از این شبکه‌ها وجود داشت و سکوه‌های نشر مهم نیز بیشتر در ایالات متحده مستقرند که میلیون‌ها کاربر در سایر کشورها دارند، به درخواست کشورها اطلاعات برخی کاربران حذف و فعالیتشان محدود شد و مثلاً توئیتر توئیتهای را حذف می‌کرد. برای پاسخ به این فشارها سکوه‌های نشر ناچار به تدوین سیاست‌های خود شدند و مثلاً برخلاف گوگل که از قانون چین پیروی نکرد و فعالیتش را در این کشور تعطیل کرد، لینکدین و توئیتر به آن قانون احترام گذاشتند. نمونه‌های مختلفی از تحدید فعالیت و حتی برخورد با شبکه‌های اجتماعی داخلی یا خارجی به‌ویژه آمریکایی را در کشورهای مختلفی مانند روسیه، فرانسه، ترکیه، لبنان، کویت، آرژانتین و غیره نیز می‌توان مشاهده کرد؛ اما آمریکا همچنان خودش به قانون بندرگاه امن (بخش ۲۳۰ مذکور) وفادار مانده است. (گیلسپی، ۱۴۰۰: ۲۵۱-۲۵۲) در نتیجه با توجه به گستردگی جهانی سکوه‌های نشر و تفاوت قوانین کشورها تعیین حدّ معینی از مسئولیت، هرچند دشوار اما ضروری است و می‌تواند با ابزارهایی مثل فیلترینگ یا سایر تهدیدها مواجه شود. بر این پایه برای ممانعت از سوء استفاده فعالان سیاسی، همجنسگراها و سایر موارد غیرقابل اجتناب، سکوه‌های نشر به‌ناچار باید قوانین خود را تدوین، اصلاح و به‌روز کنند (Bucher, 2012: 1177) به نحوی که در عین جلوگیری از ریزش کاربران گریزان از محیط جرم‌خیز و فاسد، با محدودیت‌های زیاد هم آنها را به سمت سکوه‌های نشر رقیب خود فراری ندهند و اینگونه است که بخشی از منافع سکوها در بند خودتنظیم‌گری داوطلبانه قرار می‌گیرد.

در کنار خودتنظیم‌گری یا به تعبیر برخی خودنظام‌دهی، دو قالب دیگر «نظام‌دهی مشترک با دولت» و «نظام‌دهی توسط دولت» نیز رایج است که در خصوص رسانه‌ها برخی محققان مطلوب‌ترین شیوه را خودنظام‌دهی می‌دانند به نحوی که گردانندگان رسانه رأساً و بدون مداخله دولت قواعد رفتاری و نهادهای

چالش‌های قانونگذاری حقوق کاربران در فضای مجازی؛ مطالعه تطبیقی دو تجربه متفاوت

تنظیم‌گر را مشخص کنند و حقوق و آزادی‌های دیگران را رعایت نمایند، هرچند نظام‌دهی با مشارکت دولت رایج‌تر است و نظام‌دهی صرفاً به‌وسیله دولت نیز منفورترین شیوه است. (انصاری، ۱۳۸۹، ۹۹) علت آن هم ضرورت آزادی عمل رسانه‌ها برای نظارت بر عملکرد دولت است. (رضایی، بابازاده مقدم، ۱۳۹۳: ۷۴) اما در خصوص سکوهای نشر دیجیتال به این قواعد عام قانونگذاری برای رسانه‌ها مطلوب به نظر نمی‌رسد؛ زیرا هدف اصلی سکوهای نشر، تجاری و کسب سود است و نه مانند رسانه‌هایی که سود مالی هدف اولیه و اساسی آنها نیست و مثلاً ممانعت از انحصارگری آنها ضروری است. ثانیاً در فضای وب ۲ که کاربران مختلف هر کدام خود ارائه‌کننده محتوا هستند، لزوماً در جهت آرمان‌های روشنگری و دفاع از منافع و آزادی‌های عمومی علیه دولت فعالیت نمی‌کنند که قانونگذاری به‌وسیله دولت برای آنها منفور باشد. لذا افزون بر خودتنظیم‌گری سکوهای نشر دیجیتال، وضع قوانین دولتی نیز برای کنترل آنها ضرورت دارد، به ویژه که سکوهای نشر بزرگ در کشورهایی مانند آمریکا قرار دارند که قواعد و مبانی نظام حقوقی آنها در بسیاری موارد با نظام حقوقی ما سازگاری ندارد.

خودتنظیم‌گری سکوهای نشر در عین حال که می‌تواند منجر به تصویب مقرراتی مغایر با برخی اصول و ارزش‌های اخلاقی و قانونی سایر کشورها یا کشور محل استقرار سکوی نشر باشد، مانند حذف پست‌ها و صفحات اجتماعی مربوط به شهید سلیمانی به‌وسیله سکوی نشر اینستاگرام که مغایر با قوانین ایران و اسناد بین‌المللی ضد تروریسم است، از سوی دیگر می‌تواند از ضمانت اجرایی قوی برخوردار باشد و علیه مقامات عالی‌رتبه کشور میزبان سکوی نشر هم کارآمد باشد که البته این قدرت ظرفیت ایجاد چالش‌هایی را نیز دارد. به عنوان مصداقی معین اوج چالش‌های مربوط به بخش ۲۳۰ قانون نزاکت ارتباطات آمریکا را باید در وقایع پس از انتخابات ۲۰۲۰ ریاست جمهوری آمریکا ملاحظه کرد.<sup>۱</sup> مدتی پس از آنکه توئیتر برای نخستین بار به توثیق ترامپ مبنی بر ادعای تقلب در انتخابات، برچسب «راستی‌آزمایی»، «نژادپرستانه»، «تحریک به خشونت» و «دروغ» زد، مصنوعیت شبکه‌های اجتماعی (فیسبوک، توئیتر و...) در مقابل پیگرد حقوقی و قانونی، با فرمان اجرایی رئیس‌جمهور وقت آمریکا، دونالد ترامپ لغو گردید. وی

1. [brookings.edu/research/the-politics-of-section-230-reform-learning-from-fostas-mistakes/](https://www.brookings.edu/research/the-politics-of-section-230-reform-learning-from-fostas-mistakes/)

این فرمان را «در راستای دفاع از آزادی بیان در برابر یکی از جدی‌ترین خطرات پیش روی خود در تاریخ آمریکا» خواند و گفت: «تعداد معدودی از شبکه‌های اجتماعی، بخش وسیعی از کل ارتباطات عمومی و خصوصی در ایالات متحده را در انحصار و کنترل خود دارند. ... آن‌ها قدرت بدون نظارتی برای سانسور، محدود کردن، ویرایش، شکل دادن، پنهان کردن و تغییر هر نوع ارتباط مجازی بین شهروندان و مخاطبان در عرصه عمومی دارند.» این مقطع، شفاف‌ترین صحنه مدیریت فضای مجازی به وسیله نهادهای امنیتی (FBI و NSA) بود، به نحوی که با وجود سردمداری قدرتمندترین فرد حکومت در اعتراضات، حفظ ساختار حکومت و مدیریت بحران در دستور کار قرار گرفت و مالکان شبکه‌های اجتماعی، در نقش مدیران بحران به کمک نهادهای امنیتی آمدند و در نتیجه حساب دونالد ترامپ، رئیس‌جمهور قانونی وقت، در شبکه‌های اجتماعی پرمخاطب، تعلیق یا به کلی مسدود و حذف گردید.<sup>۱</sup>

پس از چالش‌های مذکور علیرغم دست برتر شبکه‌های اجتماعی آمریکا نسبت به رئیس‌جمهور وقت، بحث کنترل شبکه‌های اجتماعی به صورت جدی‌تری مطرح شد و ضرورت تهدید اختیارات آنها نیز بیشتر احساس شد. از آنجا که هدف بخش ۲۳۰ ارائه همان استعاره بود که ارائه‌دهندگان خدمات اینترنتی (ISP ها)<sup>۲</sup> صرفاً توزیع کننده مطالبی مانند کتابفروشان هستند و نه ناشران، بنابراین نباید در قبال محتوایی که توزیع می‌کنند از ترس ایجاد تأثیر وحشتناک آزادی بیان، مسئولیتی داشته باشند. (Reynolds, 2019)<sup>۳</sup> با این مبنا بخش ۲۳۰ قانون نزاکت ارتباطات از چالش‌های تخلفات ارائه‌دهندگان خدمات اینترنتی در مقابل شکایاتی که مبنی بر مغایرت آن قانون با قانون اساسی طرح می‌شد، پیروز بیرون آمد<sup>۴</sup> تا اینکه در سال ۲۰۱۸ قانون فوستا - سیستا (FOSTA-SESTA Act)<sup>۵</sup> تصویب شد. به جهت افزایش روزافزون سوء استفاده جنسی علیه کودکان چه در قالب انتشار

۱. قابل مشاهده در نشانی: [b2n.ir/t24961](http://b2n.ir/t24961)

[nytimes.com/interactive/202107/06/technology/trump-social-media-ban.html](http://nytimes.com/interactive/202107/06/technology/trump-social-media-ban.html)

2. Internet Service Provider

3. [wired.co.uk/article/section-230-communications-decency-act](http://wired.co.uk/article/section-230-communications-decency-act)

4. [theverge.com/20146044679/19/8//the-six-lawsuits-that-shaped-the-internet](http://theverge.com/20146044679/19/8//the-six-lawsuits-that-shaped-the-internet)

5. The Stop Enabling Sex Traffickers Act (SESTA) and Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA)

چالش‌های قانونگذاری حقوق کاربران در فضای مجازی؛ مطالعه تطبیقی دو تجربه متفاوت

آنلاین تصاویر و یا عضویت در شبکه‌های اجتماعی (مثل چت‌روم‌های خصوصی سکوه‌های نشر)، به جهت اینکه ارائه‌دهندگان خدمات اینترنتی هم هیچ الزامی به حذف تصاویر سوء استفاده از کودکان نداشتند، خلأ قانونی محسوس در قوانین و داخلی و بین‌المللی وجود داشت (بادامی، ۱۳۹۹: ۴۸-۵۲) که از علل تصویب قانون فوستا - سیستا بود و مصونیت از مسئولیت را نسبت به خدماتی که علیه کاربرانی که آگاهانه در بهره‌کشی جنسی از کودکان یا قاچاق جنسی درگیر هستند، حذف کرده است. در این فضا بود که لایحه ریشه‌کنی تجاوز و مسامحه از فناوری‌های تعاملی (EARN IT)<sup>۱</sup> برای تهدید بخش ۲۳۰ قانون (CDA) در ۵ مارس ۲۰۲۰ به مجلس سنا ارائه شد تا مسئولیت اپراتورهای وب را در قبال انتشار سوء استفاده جنسی از کودکان بیشتر کند. نهایتاً پس از به نتیجه نرسیدن این لایحه، لایحه جدیدی به نام «قانون سرمایه‌گذاری در ایمنی کودکان» را در ماه مه ۲۰۲۰ پیشنهاد کردند که ۵ میلیارد دلار به وزارت دادگستری می‌دهد تا به جای تکیه بر شرکت‌های فناوری برای مهار این مشکل، مستقیماً به استثمران کودکان رسیدگی کنند.<sup>۲</sup>

نتیجه اینکه بخش ۲۳۰ قانون نزاکت ارتباطات آمریکا در حال حاضر با توجیهاتی مثل آزادی بیان، شخصی بودن جرائم و مجازات‌ها یا حتی توجیهات فنی مثل ضرورت رشد سریع تکنولوژی و نوآوری در فضای مجازی به نفع سکوه‌های نشر و ارائه‌دهندگان خدمات اینترنتی تفسیر می‌شود و آنها را از مسئولیت به در فضای وب ۲ نسبت به انتشار اطلاعات کاربران تیرئه می‌کند. این تفسیر موشع در عمل منجر به نقض مختلف شهروندان کاربر فضای مجازی به صورت مستقیم یا حتی حقوق غیر کاربران به صورت غیرمستقیم در افشار و زمینه‌ها و سطوح گوناگون شده است. بارزترین این حقوق، حق محرمانگی زندگی خصوصی اشخاص است که در قواعد نسل دوم حمایت از داده‌های شخصی در مواردی نظیر «حق خلوت» و «حق حریم خصوصی» مورد توجه بوده است. البته از سوی دیگر جریان آزاد اطلاعات که لازمه توسعه اقتصادی و اجتماعی است نیز تأمین شود و بین این دو تعادل برقرار باشد. (زرکلام، ۱۳۸۶: ۱۷۸ و ۱۸۶) اما در قوانین ملی آمریکا کفّه این

1. Eliminating Abuse and Rampant Neglect of Interactive Technologies
2. Keller, Michael (May 5, 2020). "A \$5 Billion Proposal to Fight Online Child Sexual Abuse". The New York Times.

ترازو به سمت جریان آزاد اطلاعات سنگین است که لاجرم منجر به نقض حقوق بشر در زمینه حریم خصوصی می‌شود. همچنین حق بر سلامت جسمی و روحی به ویژه در مورد کودکان که در ماده (۱۲) میثاق بین‌المللی حقوق اقتصادی، اجتماعی و فرهنگی مرد توجه است، از سویی می‌تواند با توسعه فناوری اطلاعات و آموزش در بستر مجازی در مواردی مانند تغییرات آب و هوایی و اقلیمی بهتر تأمین شود (بادامی، ۱۳۹۹: ۳۶-۳۷) و از سوی دیگر سلامت اخلاقی اشخاص به ویژه کودکان که با بهره‌گیری از وسایل نوین ارتباطی، هرزه‌نگاری و تشکیل دسته‌های قاچاق انسان و تبلیغ جرائم جنسی تسهیل شده است (السان، ۱۳۹۳: ۱۹۳) در معرض خطر قرار گیرد که مصونیت سکوه‌های نشر و ارائه‌دهندگان خدمات اینترنتی با استناد به بخش ۲۳۰ قانون نزاکت ارتباطات آمریکا زمینه‌ساز ترویج این جرائم و نقض حقوق بنیادین بشر است که در بند (ج) ماده (۱۹) میثاق بین‌المللی حقوق مدنی و سیاسی نیز بدان اشاره شده است. حق دیگری که با بی‌مسئولیتی سکوه‌های نشر نقض آن کراراً رخ می‌دهد، ناظر به حقوق مالکیت فکری در فضای مجازی است. مواردی مانند حق بر اثر (کپی‌رایت)، نام دامنه، اسرار تجاری در فضای مجازی، نرم‌افزارهای رایانه‌ای، علامت تجاری و پوشش تجاری، اختراع و مهندسی معکوس (السان، ۱۳۹۳: ۴۷-۱۱۹) در زمره حقوق معنوی قابل شناسایی در فضای مجازی هستند که با ابزارهایی مانند کوکی‌ها<sup>۱</sup> که سایت‌ها و پلتفرم‌ها می‌توانند از طریق آن با قراردادن فایل‌هایی در رایانه دیگران اطلاعات و رفتار آنها در شبکه را ذخیره کنند (نوری، نجوانی، ۱۳۸۳: ۶۳) و در جهت منافع خود بهره‌برداری کنند که بر مبنای بخش ۲۳۰ مزبور مسئولیتی هم در قبال آن ندارند. هرچند برخی از این حقوق با استناد به برخی قوانین دیگر آمریکا، در مقابل سوء استفاده یا قصور سکوه‌های نشر قابل صیانت است؛ مانند حقوق حمایت از داده‌های حوزه بهداشت و سلامت که در قانون فدرال (HIPAA)<sup>۲</sup> متکفل نحوه تحصیل و پردازش داده‌های مربوط به سلامتی اشخاص است (اصلانی، ۱۳۸۶: ۳۳۳) که بعضاً می‌تواند تخصیص‌زننده عمومیت بی‌مسئولیتی سکوه‌های نشر در بخش ۲۳۰ مزبور باشد.

1. cookie

2. Health Insurance Portability and Accountability Act of 1996

چالش‌های قانونگذاری حقوق کاربران در فضای مجازی؛ مطالعه تطبیقی دو تجربه متفاوت

در نهایت در مقام قیاس آمریکا و اروپا باید گفت قوانین اروپایی الگوی مطلوب‌تری در حمایت از داده‌ها و حقوق اشخاص در فضای مجازی ارائه می‌دهند؛ زیرا آن قوانین، برخلاف قوانین آمریکایی اصل را بر صیانت از عموم داده‌های فضای مجازی گذاشته‌اند و نه حمایت به موجب قانونی خاص و در حوزه‌ای خاص و با تفسیری مضیق از مسئولیت سکوه‌های نشر. همچنین از ضمانت اجرای قوی‌تری برخوردارند.

### ۳- چالش‌های قانون‌گذاری حقوق کاربران فضای مجازی در ایران

تا کنون در مواردی به صورت پراکنده در قوانین عمومی یا متمرکز در قوانین خاص حوزه فضای مجازی احکامی در جهت حمایت از حقوق کاربران در ایران وضع شده است که بررسی نقاط ضعف و قوت نظام حقوقی ما در این زمینه بدون بررسی آنها میسر نیست؛ لذا در ادامه اجمالاً وضعیت فعلی نظام حقوقی ایران را در این حوزه تبیین می‌کنیم، سپس چالش‌های قانونگذاری را در این حوزه واکاوی می‌کنیم.

#### تحلیلی از وضعیت قوانین فعلی

در نظام حقوقی ایران تنها سند حقوقی برای حفاظت از اطلاعات شخص موضوع داده مواد ۵۸ و ۵۹ قانون تجارت الکترونیک مصوب ۱۳۸۲ است که ابهام آنها نیز باعث مشکل در انعقاد قراردادهای حوزه تجارت الکترونیک میان تولید و مصرف‌کننده می‌شود؛ زیرا حکمی در مورد کیفیت جمع‌آوری داده‌ها و محدودیت‌های آن ندارد. به علاوه ماده ۵۸ پردازش داده‌های مربوط به ریشه‌های قومی مذهبی، نژادی، عقیدتی و اخلاقی و وضع جسمی و روانی و جنسی را منوط به شرایط مواد ۵۸ و ۵۹ نموده است که القای عدم شمول به سایر داده‌ها را می‌کند؛ لذا به اصلاح نیاز دارد. همچنین تعیین مرجع ذیصلاح ناظر بر انعقاد قراردادها و پیشگیری از تحدید مالکیت دارندگان در این قانون ضروری است. (آقایی طوق و ناصر، ۱۳۹۹: ۳۸-۳۹)

علاوه بر این، مفاد قانون تجارت الکترونیک از حقوق مصرف‌کنندگان در معاملات آنلاین حمایت قانونی کافی نمی‌کند. وبسایت‌های کسب و کار، اطلاعات را به صورت آنلاین جمع‌آوری می‌کنند؛ اما اکثر آنها مقرراتی در مورد رعایت حریم

خصوصی اشخاص ندارند؛ یا مقرراتشان در دسترس نیست. برخی از مقررات و خط‌مشی‌گذاری‌های رعایت حریم خصوصی نیز نامشخص و مبهم و مختصر هستند و در مفاد قانون تجارت الکترونیک یا هر قانون دیگری گنجانده شده‌اند. شرکت‌ها و حتی نظام بانکی در ایران هنوز نه از امنیت لازم برخوردارند و نه به اقدامات کافی برای حمایت از حقوق مصرف‌کننده در زمینه حفاظت از داده‌ها در معاملات آنلاین مجهز شده‌اند. همچنین سیاست‌های حفظ حریم خصوصی آنها ناامن است و با تعهدات قانونی مطابقت ندارند و برای مصرف‌کنندگان مضر است. مقررات قانون تجارت الکترونیک برای محیط الکترونیکی مناسب نیست. علاوه بر اینکه به قانون رقابت اشاره نمی‌کند، حفاظت از داده‌های تجاری را نیز پوشش نمی‌دهد. در مورد حفاظت از داده‌های خردسالان و به ویژه کودکان سکوت می‌کند. به اقدامات فنی و سازمانی کارآمد در تراکنش‌های آنلاین اشاره نمی‌کند و شرایط استثنایی مانند منافع عمومی را روشن نمی‌کند در حالی که با استناد به منافع عمومی ممکن است داده‌ها بدون رضایت شخص موضوع داده به دست آید و در مورد داده‌های شخصی مربوط به افترای مجرمانه به افراد سکوت می‌کند. همچنین قانون تجارت الکترونیک، ضمانت اجرای کیفی را فقط برای کلاهبرداری و جعل در مواد (۶۷) و (۶۸) پیش‌بینی می‌کند؛ در حالی که سایر اعمال مجرمانه مانند خرابکاری مستثنی هستند. موضوع سرقت هویت در معاملات آنلاین نیز پوشش داده نمی‌شود و کاربران اینترنت همچنان در معرض سوء استفاده قرار می‌گیرند. (Bagheri & Halili, 2016: 140)

افزون بر ایرادهای یادشده به نظر می‌رسد این قانون حمایت مطلوبی از حقوق کاربران متناسب با تغییر و تحولاتی که در روابط تجاری الکترونیکی در فضای شبکه‌های اجتماعی و سکوه‌های نشر اتفاق افتاده است، پیش‌بینی نکرده است. کما اینکه برای مثال در ماده (۶۲) این قانون که حقوق معنوی و مالکیت فکری آثار اشاره می‌شود، صرفاً تأکید بر حمایت از آنها مطابق قوانینی مانند قانون حمایت حقوق مؤلفان، مصنفان و هنرمندان مصوب ۱۳۴۸ می‌شود که طبعاً تناسبی با دوره تاریخی پیدایش وب ۲ و به‌ویژه کسب و کار در بستر سکوه‌های نشر دیجیتال ندارند. برخی ویژگی‌های خاص این سکوه‌های دیجیتال مانند اثر شبکه‌ای<sup>۱</sup> کاهش

1. Network effect

چالش‌های قانونگذاری حقوق کاربران در فضای مجازی؛ مطالعه تطبیقی دو تجربه متفاوت

هزینه‌های مبادله،<sup>۱</sup> جایگزینی مالکیت با دسترسی (اقتصاد دسترسی)،<sup>۲</sup> شکسته و خرد شدن عرضه و تقاضا و غیره تغییرات قابل توجهی کرده است که هرچند رگه‌هایی از آنها در بازارهای سنتی هم مشاهده می‌شود؛ اما حضور همزمانشان در سکوی نشر باعث بازار متمرکز و انحصارگرایی می‌شود، (کدخدایی و فراهانی، ۱۴۰۱، ۱۹-۱۷ و ۲۵) در حالی که قانون تجارت الکترونیک در موادی مانند (۶۴)، (۶۶) و (۷۵) صرفاً به علائم تجاری و اسرار تجاری برای حمایت از رقابت عادلانه پرداخته است؛ اما نیاز به قواعد جدید حقوق رقابت با انحصارگرایی روز افزون سکوهای نشر بزرگ بسیار محسوس است.

قانون جرائم رایانه‌ای مصوب ۱۳۸۸ نیز که با غلبه رویکردی امنیتی به تصویب رسیده است، در حمایت از حقوق کاربران فضای مجازی نواقصی دارد، از جمله اینکه صرفاً با توسل به جرم‌انگاری نسبت به جرائم این حوزه احکامی مقرر کرده است، حال آنکه لزوماً تمامی تخلفات نسبت به داده‌های کاربران فضای مجازی ماهیت جرم نداشته و بسیاری از آنها صرفاً جنبه جبران خسارت داشته و مسئولیت مدنی به بار می‌آورد.

به علاوه قانون یادشده با جرم‌انگاری‌های گسترده و کیفرگذاری‌های سنگین در جرائم رایانه‌ای تا مرحله تسامح صفر<sup>۳</sup> پیش رفته است که با عدم چشم‌پوشی نسبت به کوچکترین تخلف‌ها خود می‌تواند زمینه‌ساز جرم‌های مهمتری حتی علیه امنیت ملی باشد. (رایجیان اصلی، ۱۳۸۸، ۴۱۱) با تحول سکوهای نشر دیجیتال از زمان تصویب این قانون، نوع جرائم، زمینه‌های ارتکاب جرم و شکل‌گیری گروه‌های مجرمین و غیره در بستر سکوهای نشر دگرگونی‌های زیادی یافته است که بر این پایه هم بازبینی رویکرد پیشگیرانه با تنظیم‌گری در فضای دیجیتال در جهت صیانت از حقوق کاربران ضروری به نظر می‌رسد و هم بازنگری در مجازات‌ها و وضع مجازات متناسب با جرائم خاص این فضا.

ماده (۷۴۹) قانون مجازات اسلامی مصوب ۱۳۹۲ (جریمه‌های نقدی اصلاحی ۱۳۹۹) نیز راهکار سختی تحت عنوان پالایش (فیلتر) را نسبت به نقض ضوابط

1. Transaction Cos
2. Access economy
3. Zero tolerance

قنّی و فهرست مقرر از سوی کارگروه (کمیته) تعیین مصادیق محتوای مجرمانه اعم از محتوای ناشی از جرائم رایانه‌ای و محتوایی که برای ارتکاب جرائم رایانه‌ای به کار می‌رود، مقرر کرده است. طبعاً همان‌طور که در خصوص پلتفرمی مانند تلگرام تجربه‌ای به دست آمده است، پالایش صرف نرم‌افزار سکوی نشر نمی‌تواند راهکار چندان کارآمدی جهت جلوگیری از تخلفات ارائه‌دهنده خدمت اینترنتی باشد، کما اینکه کاربران ایرانی این سکوی نشر، هرچند پس از پالایش کاهش یافته‌اند،<sup>۱</sup> اما به هر حال تعداد بسیار زیادی از کاربران با استفاده از فیلترشکن (vpn) و پراکسی (proxy) همچنان به استفاده از آن سکوی نشر ادامه می‌دهند. پالایش در اینجا باعث می‌شود آن سکو از تحت نظارت قرار گرفتن به کُلّی خارج شود؛ به‌ویژه که در خصوص سکوهای نشر بیگانه به مالکان و اداره‌کنندگان آن دسترسی وجود ندارد و این موضوع خودش زمینه را برای سوء استفاده آن سکوی نشر از اطلاعات کاربران بیش از پیش فراهم می‌کند. هرچند پالایش را به کُلّی نمی‌توان به عنوان آخرین راهکار نفی کرد؛ اما تمسک به راهکارهایی مانند فشارهای دولت به شکل مستقیم یا از طریق نهادهای بین‌المللی یا نهادهای قانونی کشور محل استقرار سکوی نشر، راهکارهای قبل از پالایش کُلّی آن هستند.

## نسبت سیاست‌گذاری شورای عالی فضای مجازی در مورد حقوق کاربران با قانونگذاری مجلس

برخی اسناد حقوقی دیگر ابهامات و نواقص بارزی در تضمین و احصاء حقوق کاربران فضای مجازی دارند؛ مانند مصوّبه شورای عالی فضای مجازی با موضوع سیاست‌ها و اقدامات ساماندهی پیام‌رسان‌های اجتماعی مصوّب ۱۳۹۶ که هرچند نکات مثبتی مانند پشتیبانی از توسعه شبکه‌های اجتماعی داخلی را مقرر کرده است؛ اما وظایفی کُلّی را بر عهده دستگاه‌های ذی‌ربط گذاشته است و ضمانت اجرایی برای آن مقرر نکرده است.

با این حال به جهت اینکه شورای عالی فضای مجازی ماهیتاً نهادی سیاست‌گذار است و ورودش به جزییات با اصول قانونگذاری سازگار نیست؛ اما برای مثال بند (۳-۱) که تهیه و تدوین ضوابط و شرایط انتشار محتوا، تبلیغات،

چالش‌های قانونگذاری حقوق کاربران در فضای مجازی؛ مطالعه تطبیقی دو تجربه متفاوت

صیانت از داده‌ها، مواجهه با تخلفات، ناهنجاری‌ها و تهاجم فرهنگی را مانند برخی بندهای دیگر این ماده به کارگروهی اجرایی سپرده است، بدون قانونگذاری لازم نمی‌توان ضمانت اجراهای متناسب را در این حوزه مقرر کرد؛ زیرا برخی موارد مانند جرم‌انگاری مطابق اصل ۳۶ قانون اساسی نیاز به تقنین به‌وسیله مجلس دارند. بنابراین چالش اساسی در به رسمیت شناخته نشدن مصداقی حقوق کاربران ناشی از خلأ قانونگذاری در این حوزه نیز است.

شایان ذکر است که افزون بر ایرادهای ماهوی فوق در زمینه‌ی ارتباط سیاست‌گذاری فضای مجازی با قانونگذاری و مقررات‌گذاری از جهت تعیین تکلیف سلسله مراتب این هنجارهای حقوقی که تکلیفی مقرر شده در بند (۵) سیاست‌های کلی نظام قانونگذاری ابلاغی ۱۳۹۸ مقام معظم رهبری است، می‌تواند اثرات مثبتی در زمینه قانونگذاری در عرصه صیانت از حقوق کاربران فضای مجازی داشته باشد. کما اینکه در مواردی مانند طرح تنظیم مقررات فضای مجازی مشکلاتی از این دست باعث شده بود که مجلس اقدام به تصویب طرحی مغایر با برخی از مصوبات شورای عالی فضای مجازی کند که چالش‌هایی به دنبال داشت و اجمالاً در ادامه به برخی از آنها اشاره می‌کنیم.

### غفلت از حقوق کاربران در برخی طرح‌های در دست تصویب

طرح تنظیم مقررات فضای مجازی که ابتدا با عنوان طرح صیانت از حقوق کاربران فضای مجازی به مجلس ارائه شده بود، فارغ از مشکلاتی که از حیث تفویض آیین‌نامه به غیر وزیر و هیئت وزیران (اصل ۱۳۸)، مغایرت با مصوبات شورای عالی فضای مجازی (اصل ۵۷)، اعطای مسئولیت به نیروهای مسلح (اصل ۱۱۰)، تشکیل کمیسیون عالی از جهت ترکیب (اصول ۵۷ و ۶۰)، مغایرت با اصول ۷۵، ۷۷ و فصل حقوق ملت در قانون اساسی داشت، با عدم رعایت اصول قانونگذاری در بند (۹) سیاست‌های کلی نظام قانونگذاری به حقوق کاربران فضای مجازی توجهی جزئی نشان داده بود به نحوی که حکم بسیاری از حقوق کاربران در مواد مربوطه روشن نشده بود. این در حالی است که تجربه‌های قانونگذاری در این زمینه همانطور که در بخش‌های قبل توضیح داده شد، در کشورهای مختلف به ویژه در سطح اروپا در این زمینه وجود داشت.

چالش‌های قانونگذاری حقوق کاربران در فضای مجازی؛ مطالعه تطبیقی دو تجربه متفاوت

ماده (۱۵) این طرح برخی از حقوق کاربران را در این موارد شناسایی کرده است:

الف- حفاظت از حریم خصوصی کاربران و جلوگیری از دسترسی غیرمجاز به داده‌های آنها.

ب- احراز هویت معتبر کاربران و حفظ اطلاعات آنها مطابق قوانین موضوعه و سند هویت معتبر مصوب شورای عالی فضای مجازی.

پ- عدم انتقال داده‌های مرتبط با هویت کاربران ایرانی به خارج از کشور.

ت- ذخیره‌سازی و پردازش داده‌های کاربران ایرانی مطابق مصوبات شورا و ضوابط و مقررات مربوط.

ث- ارائه خدمات متناسب با نیاز کاربران ویژه از جمله کودکان، نوجوانان و توان‌یابان بر اساس سند صیانت از کودکان و نوجوانان در فضای مجازی و دیگر مصوبات شورا.

ج- عدم حذف حساب کاربران و محتوای مجاز مگر به درخواست مالک آن.

چ- رعایت مواد ۵۸ تا ۶۰ قانون تجارت الکترونیکی مصوب ۱۳۸۲/۱۰/۱۷ با اصلاحات و الحاقات بعدی و عدم درخواست اجازه دسترسی مغایر با این مواد از کاربران.

تبصره- در خصوص خدمات چندگانه، عدم ارائه داده‌های ضروری مربوط به یک خدمت به‌وسیله کاربر نباید موجب قطع کلی خدمات فضای مجازی موردنیاز وی شود.

ح- رعایت الزامات سالم‌سازی وفق مواد ۷۴۹ تا ۷۵۱ قانون مجازات اسلامی مصوب ۱۳۹۲ و اصلاحات بعدی آن و الزامات امنیتی و پدافند غیرعامل ابلاغی تنظیم‌گران.

خ- رعایت دستورالعمل پیشگیری، شناسایی و مقابله با جرم در خدمات فضای مجازی.

تبصره- دستورالعمل پیشگیری، شناسایی و مقابله با جرائم در خدمات فضای مجازی به‌وسیله دادستانی کل کشور با همکاری وزارت دادگستری، مرکز ملی فضای

چالش‌های قانونگذاری حقوق کاربران در فضای مجازی؛ مطالعه تطبیقی دو تجربه متفاوت

مجازی و معاونت پیشگیری از وقوع جرم قوه قضائیه ظرف مدت سه ماه از تاریخ ابلاغ این قانون تهیه می‌شود و به تصویب رئیس قوه قضائیه می‌رسد.

د- حمایت از حق مالکیت بر شناسه کاربری وفق قانون ثبت اختراعات، طرح‌های صنعتی و علائم تجاری مصوب ۱۳۸۶ و اصلاحات بعدی آن.

تبصره- دستورالعمل مربوط به این بند به وسیله کمیسیون عالی تصویب و ابلاغ خواهد شد.»

بندهای (ت) و (ث) این ماده حقی را برای کاربر تعریف نمی‌کند و صرفاً موضوعی را به مصوبه شورای عالی فضای مجازی احاله می‌دهد. بندهای (چ) و (ح) صرفاً به وجود حکمی در قوانین دیگر اشاره می‌کند که مواد قانون مجازات به شناسایی حقوق کاربران ارتباط ندارد و خلأ مواد مذکور قانون تجارت الکترونیک نیز که پیش از این نقد شد. تنها حق حریم خصوصی، حفظ اطلاعات هویتی، عدم انتقال داده‌ها به خارج از کشور، ارائه خدماتی به کودکان، عدم حذف حساب و محتوای مجاز و مالکیت شناسه کاربری ذکر شده است که اغلب هم بدون تعریف و تعیین حکمی به سایر قوانین یا اسناد حقوقی ارجاع شده است.

در حوزه قوانین مرتبط با حفاظت از داده‌های شخصی افراد هم در ایران خلأ قانونی داریم. در مقایسه با مقررات عمومی حفاظت از داده اتحادیه اروپا، در ایران با خلأهای قانونی در زمینه مدیریت حفاظت از داده‌های شخصی مواجهیم که از جمله می‌توان به قانون حاکم به دعاوی ناشی از این فرآیند، مفهوم‌شناسی داده‌های خصوصی، کیفیت اعطای مجوز به فعالیت پردازندگان و کنترل‌کنندگان، سازوکار مسئولیت‌پذیری، دادگاه صالح در رسیدگی به این دعاوی، حقوق دارنده اطلاعات و سازوکار تبادل داده اشاره کرد که ضرورت تصویب قانونی جامع را روشن می‌سازد. (آقایی طوق و ناصر، ۱۳۹۹: ۵۳)

طرحی که اخیراً در خصوص حفاظت از داده‌ها در مجلس تصویب شده است، موسوم به «طرح مدیریت داده‌ها و اطلاعات ملی» است که با ادغام طرح‌های «یکپارچه‌سازی داده‌ها و اطلاعات ملی» و «نظام جامع مدیریت داده‌های کشور تسهیل ارائه خدمات الکترونیکی به مردم» مورخ ۱۴۰۱/۱۱/۱۷ به تصویب مجلس رسیده است که در ماده (۲) وظیفه ذاتی شورای عالی فضای مجازی را مجدداً بر

چالش‌های قانونگذاری حقوق کاربران در فضای مجازی؛ مطالعه تطبیقی دو تجربه متفاوت

عده آن گذاشته است و برخی مواد دیگر نیز از این حیث مشابه این ماده است و موادی هم که حکم صیانت از داده‌ها را مشخص کرده است، موضوعش صیانت از داده‌های ملی کشور است که در بند (ت) ماده (۱) این طرح صرفاً داده‌های دستگاه‌های مشمول این طرح عنوان شده است. بنابراین اساساً در این طرح هم نسبت به حفاظت از داده‌های اشخاص خصوصی توجّهی نشان داده نشده است و حقوق مربوطه از طرح خروج موضوعی دارد.

### مصادیق حقوق ضروری کاربران فضای مجازی در قوانین

برخی از حقوق کاربران را که در قوانین موجود یا حتّی طرح‌های در دست تصویب مورد توجّّه قرار نگرفته یا به صورت ناقص ذکر شده‌اند، به شرح زیر می‌توان احصاء کرد:

#### سکوی نشر در احترام به سیاست‌های حریم خصوصی و شرایط خدمات

ضرورت اعلام خط‌مشی‌ها و مقرّرات سکوه‌های نشر و مصادیقی از آن در قوانینی مثل مقرّرات عمومی حفاظت از داده‌ها در اروپا اشاره شد؛ لذا سکوه‌های نشر باید کاملاً به طور شفاف سیاست حفظ حریم خصوصی و شرایط خدمات خود را طرح کنند و صادقانه به آن احترام بگذارند.

#### دسترسی به خط‌مشی‌ها و وضوح آنها

سکوه‌های نشر باید به نحو قابل اثباتی اطمینان بدهند که خط‌مشی‌ها، شرایط خدمات و تنظیمات به راحتی پیدا و به وسیله کاربر فهمیده می‌شوند. چرا که در صورت عدم دسترسی به آنها یا ابهام در متنشان، کاربر از حقوق خود در پلتفرم آگاهی پیدا نکرده و نمی‌تواند از خود دفاع نماید که این حق نوعی از حق استماع کاربر است.

#### آزادی بیان

سکوه‌های نشر نباید داده‌های کاربر را بدون یک خط‌مشی مشخص، منطقی، قانونمند و گام‌بندی شده، حذف کنند یا تغییر بدهند. بنابراین دولت و همه شبکه‌های اجتماعی چه در مرحله تنظیم مقرّرات حاکم بر سکوی نشر و کاربران

چالش‌های قانونگذاری حقوق کاربران در فضای مجازی؛ مطالعه تطبیقی دو تجربه متفاوت

و چه در مرحله اجرای آن مقررات، موّلف به تبعیت از «اصل صلاحیت محدود و شفاف» هستند تا آزادی بیان صیانت شود.

### توانمندسازی فنی سکوه‌های نشر

سکوه‌های نشر باید از فناوری‌های کمکی و دسترسی جهانی پشتیبانی کنند. البته در غیر این صورت به مرور در رقابت با سایر سکوه‌های نشر قوی‌تر کاربران آن‌ها ریزش می‌کنند. در این زمینه وظایفی را نیز برای دولت می‌توان برای حمایت از سکوه‌های نشر داخلی جهت توانمند شدن و دارا شدن قابلیت رقابت با نوع بیگانه خود قائل شد تا از یک سو سکوه‌های نشر بزرگ خارجی که تن به قوانین داخلی کشور ما نمی‌دهند و به تبع آن حقوق کاربران ایرانی را نیز نقض می‌کنند، در مسیر رقابت ناچار به پذیرش مقررات شوند و از سوی دیگر حق کاربران بر دسترسی به فناوری‌های پیشرفته‌تر تأمین شود.

### فناوری قوی‌تر در محافظت از حریم خصوصی کاربر

شبکه‌های اجتماعی و به طور کلی سکوه‌های نشر باید از فناوری‌های افزایش‌دهنده حریم خصوصی پشتیبانی کنند. هرچند با توجه به تجربه‌ای که از محققان آمریکایی در نقد مقررات عمومی حفاظت از داده‌ها (GDPR) نقل شد، مانند اینکه شرکت‌های بزرگ برخلاف سکوه‌های نشر کوچکتر، بودجه ارتقای نرم‌افزار و به‌کارگیری متخصصان حریم خصوصی را دارند (Campbell, 2015: 71) در نتیجه کاربران، سکوه‌های نشر جدیدتر و نوپاتر را کمتر استفاده می‌کنند. اما به هر حال این امر نافی حق کاربران بر استفاده از فناوری محافظ حریم خصوصی‌اش نیست.

### به حداقل رساندن داده‌ها

یک سکوی نشر باید اطلاعاتی که کاربر را الزام به ارائه آنها می‌کند و کاربر باید آنها را به اشتراک بگذارد، به حداقل برساند. این حق نیز به نوعی در جهت حق بر حریم خصوصی است؛ اما نوعی خاص از الزام به رعایت حریم خصوصی است که جای شناسایی مستقل در مقررات را دارد.

### حق کنترل داده‌ها به وسیله کاربر

شبکه اجتماعی و سکوه‌های نشر باید اجازه دهند که کاربر داده‌هایش را کنترل کند و اشتراک‌گذاری آن را تسهیل نماید؛ مگر اینکه در ابتدای پذیرش کاربر در سکوی نشر، محدودیت‌هایش را صریحاً بیان کند و خود کاربر موافقتش را بر محدودیت حق کنترل خود بپذیرد.

### پیش‌بینی‌پذیری تغییر مخاطبین کاربر

در بستر سکوه‌های نشر و شبکه‌های اجتماعی بعضاً مسائلی مانند خرید و فروش کاذب مخاطبین و از این قبیل مسائل رخ می‌دهد به نحوی که بعضاً مالک یک صفحه اجتماعی از تغییر آنها باخبر نمی‌شود که در موارد مشابه این یا مواردی که خود سکوی نشر تغییراتی را در مخاطبین کاربر می‌دهد، سکوی نشر قبل از تغییر قابل توجه افرادی که می‌توانند کاربر را ببینند، باید رضایت قبلی وی را دریافت کنند.

### قابلیت حمل داده‌ها

شبکه اجتماعی باید گرفتن یک کپی از داده‌های کاربر را برایش آسان کند.

### حفاظت از داده‌های کاربر به وسیله سکوه‌های نشر

با داده‌های کاربر به اندازه داده‌های محرمانه خود شبکه اجتماعی و حتی بیشتر ایمن رفتار شود، مگر اینکه کاربر عالماً و عامداً قصد افشا داشته باشد. به علاوه در صورت به خطر افتادن داده‌ها به کاربر اطلاع داده شود.

### حق دانستن

به کاربر نشان داده شود که چگونه از داده‌هایش استفاده می‌شود و به او اجازه دهد تا به نحو واضحی ببیند چه کسی و چه چیزی به آن داده‌ها دسترسی دارد. این حق همان حق بر سواد شبکه‌های مجازی است.

### حق تعریف هویت

سکوی نشر باید اجازه بدهد کاربر بیش از یک هویت ایجاد و از نام مستعار قابل ردیابی و پاسخگو استفاده کند.

### حق تجدیدنظرخواهی مؤثر و عادلانه

سکوی نشر باید به کاربر اجازه دهد که نسبت به اقدام تنبیهی شبکه اجتماعی اعتراض کند و پاسخ مکتوب و مشخصی را در بازه زمانی محدود دریافت کند. به علاوه آنکه سکوی نشر را تحت نظارت قضایی هم قرار دهد. این حق به وسیله بخش ۲۳۰ قانون نزاکت ارتباطات آمریکا (۱۹۹۶) به شدت تزییع شده است. این حق را می‌توان قسمی از حق دادخواهی کاربران علیه سکوهای نشر دانست که اغلب با حذف مدارک و اطلاعات لازم کاربری برای شکایت علیه سکوی نشر نیز تزییع می‌شود.

### حق برداشت<sup>۱</sup> (حق بر حذف)

به کاربر اجازه دهد حسابش را حذف و یا داده‌های مشخصی را حذف کند. از این حق تحت عنوان حق بر فراموش شدن<sup>۲</sup> یا حق بر حذف<sup>۳</sup> و یا حق بر پاک کردن<sup>۴</sup> نیز نام برده شده است. این حق در آمریکا در تعارض با حق آزادی بیان دانسته شده است و در ماده ۱۷ مقررات عمومی حفاظت از داده‌ها در اروپا شناسایی شده است. (قبولی درافشان، بختیاروند و آقامحمدی، ۱۳۹۷: ۱۱۵) این حق در ایران نیز در بند (ج) ماده (۱) طرح صیانت از حقوق کاربران فضای مجازی در شرف تبدیل شدن به قانون است.

### حق اصلاح، غیرفعال کردن و رد کوکی

کوکی<sup>۵</sup> یک فایل است که روی کامپیوتر یا موبایل یا تبلت ذخیره می‌شود و اطلاعاتی را برای سرور نگهداری می‌کند تا دسترسی‌ها و عملیاتش روی سیستم تسهیل و بدون اجازه کاربر انجام شود. بنابراین کاربر باید اجازه دسترسی و میزان دسترسی را در اختیار داشته باشد و هیچ سکوی نشری نمی‌تواند بدون اخذ اجازه از کاربر به اطلاعات دستگاه او دسترسی داشته باشد. این حق ذیل سیاست

1. Right to withdraw
2. Right to be forgotten (Right to oblivion)
3. Right to Delete
4. Right to Erasure
5. Cookie

تنظیم کوکی‌ها تشریح می‌گردد. حتی فراتر از این باید گفت سکوه‌های نشری که استفاده از خدمات خود را منوط بر صدور اجازه دسترسی به وسیله کاربر می‌کنند و یا بر سر دوراهی نقض حریم خصوصی و استفاده از خدمات سکوی نشر قرار می‌دهند که با این حق در تعارض است.

## حق کودکان

کودکان باید از حق حفاظت، دسترسی پاک و حذف فوری داده‌ها بهره‌مند باشند. این حق نیز در سند میانت از کودکان و نوجوانان در فضای مجازی مصوب شورای عالی فضای مجازی در ایران شناسایی شده است، در حالی که در برخی کشورها مثل آمریکا نیز تا حدود سال ۲۰۱۸ زمان تصویب قانون فوستا - سیستا (FOSTA-SESTA Act) چندان شناسایی نشده بود و در این قانون نیز امنیت اخلاقی کودکان در سکوه‌های نشر و فضای مجازی به نحو کاملی شناسایی نشده است، لذا نمی‌توان با اتکا به قوانین این کشور از قانونگذاری دقیق در این زمینه غافل شد.

## نتیجه‌گیری

در این مقاله با رجوع به سابقه تقنینی اروپا و آمریکا ثابت شد که در زمینه سیانت از حقوق کاربران در فضای مجازی قانونگذاری نقاط مختلف دنیا رویکردهای متفاوتی در پیش گرفته‌اند. از یک سو ابتدا در برخی کشورهای اروپایی مانند انگلیس شاهد پیشگاهی در این زمینه بودیم و با وضع قانون حمایت داده‌ها در ۱۹۹۸ با ارائه اصول هشتگانه حمایت از داده‌های شخصی الگویی ارائه شد. سپس در اتحادیه اروپا مقررات عمومی حفاظت از داده‌ها در سال ۲۰۱۶ تصویب و از ۲۰۱۸ لازم‌الاجرا شد که متناسب با تحولات پلتفرم‌ها و شبکه‌های اجتماعی روزآمد شده است؛ اما به هر حال به این قانون نیز انتقاداتی مانند در نظر نگرفتن اصول رقابت بین سکوه‌های نشر و آزادی بیان و حق امنیت کاربران یا شفافیت در تصمیم‌گیری‌های الگوریتمی سکوه‌های نشر وارد است.

در نظام حقوقی آمریکا قوانین متعددی در ارتباط با فضای مجازی تاکنون به تصویب رسیده است، اما آن قانونی که در حوزه سکوه‌های نشر و شبکه‌های اجتماعی اصل اساسی مصونیت آنها را از مسئولیت‌های ناشی از فعالیت کاربران

چالش‌های قانونگذاری حقوق کاربران در فضای مجازی؛ مطالعه تطبیقی دو تجربه متفاوت

در بستر شبکه آنها ایجاد کرده است، بخش ۲۳۰ قانون نزاکت ارتباطات آمریکا (الحاقی ۱۹۹۶) است. در نتیجه این قانون است که سکوه‌های نشر بزرگ آمریکایی که میلیون‌ها کاربر در سراسر دنیا دارند الزامی به رعایت بسیاری از حقوق کاربران ندارند؛ اما نهایتاً بنا بر جهاتی مانند قابلیت رقابت بین سکوه‌های نشر و فشارهای سایر کشورها بالاخره بعضی از آنها مجبور به پذیرش قوانین برخی کشورها یا خودتنظیم‌گری شده‌اند. ضمانت اجرای مقررات ناشی از خودتنظیم‌گری این شبکه‌های ارتباطی نیز در حدی قوی است که در چالش‌هایی مانند ترویج خشونت به وسیله ترامپ پس از انتخابات ریاست جمهوری بر وی غلبه کردند و حساب توئیتر او را مسدود کردند و استناد وی به آزادی بیان در قانون اساسی آمریکا راه به جایی نبرد.

در ایران هرچند تلاش‌هایی برای قانونگذاری در عرصه فضای مجازی شده و قوانینی مانند قانون جرائم رایانه‌ای و قانون تجارت الکترونیک به تصویب رسیده است؛ اما این قوانین به نحو مطلوبی نتوانسته‌اند حقوق کاربران فضای مجازی به ویژه در فضای وب ۲ و سکوه‌های نشر دیجیتال و شبکه‌های اجتماعی را شناسایی کنند و مورد حفاظت قرار دهند. طرح‌هایی که در این زمینه نیز در دست تصویب است مانند طرح صیانت از حقوق کاربران فضای مجازی (طرح تنظیم مقررات فضای مجازی) به نحوی بسیار ناقص به حقوق کاربران پرداخته است. از جمله حقوقی که پیشنهاد می‌شود در این دست طرح‌ها و لوایح گنجانده شود عبارت است از: دسترسی به خط‌مشی‌ها و وضوح آنها، صداقت سکوی نشر در احترام به سیاست‌ها، آزادی بیان، توانمندسازی قوی، فناوری قوی‌تر در محافظت از حریم خصوصی، به حداقل رساندن داده‌ها، حق کنترل داده‌ها، پیش‌بینی‌پذیری تغییر مخاطبین، قابلیت حمل داده‌ها، حفاظت از داده‌های کاربر به وسیله سکوی نشر، حق دانستن، حق تعریف هویت، حق تجدیدنظرخواهی، حق حذف، حق اصلاح، غیرفعال کردن و رد کوکی، حق کودکان به دسترسی پاک و حذف فوری داده‌ها.

## منابع

فارسی

اسماعیلی، محسن، (۱۳۹۱). گفتارهایی در حقوق رسانه، جلد اول، تهران: مؤسسه نشر شهر.

السان، مصطفی، (۱۳۹۳). حقوق فضای مجازی، تهران: مؤسسه مطالعات و پژوهش‌های حقوقی شهر دانش، چاپ اول.

بادامی، محمد مهدی، (۱۳۹۹). کودکان آنلاین و حق آنان بر امنیت همه‌جانبه در فضای مجازی (چالش‌ها و راهکارها)، تهران: پژوهشگاه قوه قضائیه، چاپ دوم.

شفیعی سروستانی، ابراهیم، (۱۳۸۵). قانون‌گذاری در نظام جمهوری اسلامی؛ آسیب‌ها و بایسته‌ها، قم: پژوهشگاه علوم و فرهنگ اسلامی.

کولزا، جوانا، (۱۴۰۰). حقوق بین‌الملل اینترنت، مترجم: میلاد فاتحی، تهران: مجد، چاپ اول.

نوری، محمدعلی و نجوانی، رضا، (۱۳۸۳). حقوق حمایت داده‌ها، تهران، کتابخانه گنج دانش، چاپ اول.

کری، پیتر و ساندرز، جو، (۱۳۸۶). حقوق رسانه، مترجم: حمیدرضا ملک محمدی، تهران: میزان، چاپ اول.

آقای طوق، مسلم و ناصر، مهدی، (۱۳۹۹). «چالش‌های حفاظت از داده‌های خصوصی در حوزه اینترنت اشیا: مطالعه تطبیقی حقوق ایران و اتحادیه اروپا»، فصلنامه حقوق اداری، سال هفتم، شماره ۲۳، ۳۳-۵۵.

رضایی، مهدی و بابازاده مقدم، حامد، (۱۳۹۳). «اصول تدوین قوانین و مقررات برای اینترنت با تأکید بر مصوبات یونسکو و شورای اروپا»، فصلنامه پژوهش حقوق عمومی، سال پانزدهم، شماره ۴۲، ۴۳-۸۲.

زرکلام، ستار، (۱۳۸۶). «حریم خصوصی ارتباط اینترنتی (مطالعه در حقوق ایران و اتحادیه اروپا)»، دوفصلنامه معارف اسلامی و حقوق، سال هشتم، شماره

چالش‌های قانونگذاری حقوق کاربران در فضای مجازی؛ مطالعه تطبیقی دو تجربه متفاوت

۲۵، ۱۷۳-۱۹۶.

قبولی درافشان، سید محمدهادی؛ بختیاروند، مصطفی و آقامحمدی، اکرم، (۱۳۹۷). «حق فراموش شدن در ترازو؛ نیاز ناشی از فضای مجازی یا تهدیدی برای آزادی بیان؟!»، فصلنامه پژوهش حقوق عمومی، سال نوزدهم شماره ۵۸، ۱۱۳-۱۳۵.

اصلانی، حمیدرضا، (۱۳۸۶). «درآمدی بر حقوق حاکم بر حمایت از داده‌های شخصی در حوزه بهداشت و سلامت»، فصلنامه رفاه اجتماعی، سال ششم، شماره ۲۵، ۳۲۱-۳۴۲.

گیلپسی، تارلتون، مترجم: محمدحسینی، ابراهیم، (۱۴۰۰). «از تنظیم‌گری در پلتفرم تا تنظیم‌گیری با پلتفرم (چالش قانونگذاری در فضای مجازی؛ چه کسی مسئول نشر مطالب نامناسب است)»، فصلنامه جامعه، فرهنگ و رسانه، دوره دهم، شماره ۳۹، ۲۴۵-۲۶۰.

کدخدایی، عباسعلی و فراهانی، محمدصادق، (۱۴۰۱). «حقوق رقابت در پلتفرم‌های دیجیتال؛ ضرورت بازنگری در قواعد سنتی»، فصلنامه پژوهش حقوق عمومی، تابستان، دوره ۲۴، شماره ۷۵.

انگلیسی

Balkin, Jack M., (2014). "Old-School/New-School Speech Regulation," Vol. 127, No.8, Harvard Law Review, 2296, 2342.

Balkin, Jack M., Information Fiduciaries and the First Amendment, 49 U.C. DAVIS L. REV. 1183, 1225 (2016)

Bucher, Taina. (2012). Want to be on the top? Algorithmic power and the threat of invisibility on Facebook. New Media & Society, 14(7), 1164-1180.

Bagheri, Parviz & Halili Hassan, Kamal, (2016), Data Privacy in Electronic Commerce: Analysing Legal Provisions in Iran, Journal of

Politics and Law; Vol. 9, No. 7, 133-141. doi:10.5539/jpl.v9n7p133

Layton, Roslyn, 2019, The 10 Problems of the GDPR The US can learn from the EU's mistakes and leapfrog its policy, Statement before the Senate Judiciary Committee On the General Data Protection Regulation and California Consumer Privacy Act: Optins, Consumer Control, and the Impact on Competition and Innovation, The American Enterprise Institute (AEI), p 1-19.

Campbell, James, Avi Goldfarb, and Catherine Tucker. "Privacy regulation and market structure." *Journal of Economics & Management Strategy* 24.1 (2015): 47-73.

HARV. L. REV, Feb 22, 2010, "Badging: Section 230 Immunity in a Web 2.0 World", *Harvard Law Review*, Vol 123, No 4, 981-1002.

International Association of Privacy Professionals, "IAPP-EY Annual Governance Report 2018," 2019, <https://iapp.org/resources/article/iapp-ey-annual-governance-report-2018/>

South, Jeff, "More Than 1,000 U.S. News Sites Are Still Unavailable in Europe, Two Months After GDPR Took Effect," *Nieman Lab*, August 7, 2018, <http://www.niemanlab.org/2018/08/more-than-1000-u-s-news-sites-are-still-unavailable-in-europe-two-months-after-gdpr-took-effect/>.

Khan, Lina M. & Pozen, David E., (2019). A Skeptical View of Information Fiduciaries, *Harvard Law Review*, Vol 133, No 2, 497-541.

Haupt, Claudia E. Oct 9, 2020 "Platforms as Trustees: Information Fiduciaries and the Value of Analogy; Responding to David E. Pozen & Lina M. Khan, A Skeptical View of Information Fiduciaries", *Harvard Law Review*, Vol 134, 34-41.

Tews, Shane, "How European Data Protection Law Is Upending the Domain Name System," AEIdeas, February 26, 2018. <https://www.aei.org/publication/how-european-data-protection-law-is-upending-the-domain-name-system/>

Lodvdahl Gormsen, Liza & Llanos, Jose Tomas, March 2022, Facebook's exploitative and exclusionary abuses in the two-sided market for social networks and display advertising, *Journal of Antitrust Enforcement*, Volume 10, Issue 1, Pages 90–132, Available at: <http://doi.org/10.1093/jaenfo/jnab004>

Lovdahl Gormsen, Liza and Llanos, Jose Tomas, Facebook's Anti-competitive Lean in Strategies (June 6, 2019). Available at SSRN: <https://ssrn.com/abstract=3400204> or <http://dx.doi.org/10.2139/ssrn.3400204>

Basu, Subhajit & Jones, Richard, 2007, Regulating Cyberstalking, *Journal of Information, Law and Technology*.

Brkan, Maja, 2016, "The Unstoppable Expansion of the EU Fundamental Right to Data Protection," *Maastricht Journal of European and Comparative Law* 23 no. 812.

Brkan, Maja, 2019, "Do Algorithms Rule the World? Algorithmic Decision-Making in the Framework of the GDPR and Beyond," *International Journal of Law and Information Technology*, 11 January 2019, DOI; 10.1093/ijlit/eay017

Blackmer, W.S. (5 May 2016). "GDPR: Getting Ready for the New EU General Data Protection Regulation". Information Law Group. InfoLawGroup LLP. Archived from the original on 14 May 2018. Retrieved 22 June 2016.

چالش‌های قانونگذاری حقوق کاربران در فضای مجازی؛ مطالعه تطبیقی دو تجربه متفاوت

Reynolds, Matt (March 24, 2019). "The strange story of Section 230, the obscure law that created our flawed, broken internet". See:

<https://www.wired.co.uk/article/section-230-communications-decency-act>

تارنماها

theguardian.com

newsroom.fb.com

wikipedia.org

statista.com

amar.org.ir

techcrunch.com

businessinsider.com

cnbc.com

nytimes.com

gdpr-info.eu

congress.gov

brookings.edu