Jurisprudence and Legal Studies of Media Journal
VOL. 8 / Autumn 2026 and Winter 2027 / NO. 2 (Serial 16)

Regulatory Imperatives for Social Media: An Analysis of European Union Legislation

Mohammad Mahdi Farajian[1] 0009-0002-7537-0359

Abstract

The challenge of regulating social media stems from the tension between state sovereignty to address harms and the protection of fundamental rights such as freedom of expression and user privacy. In response, the European Union has established a general framework comprising the GDPR, Digital Services Act, Digital Markets Act, and AI Act. However, the criminalization of specific instances of illegal content is deferred to the domestic laws of member states. The GDPR protects sensitive data including racial origin and political opinions. The DMA designates very large platforms as "gatekeepers" and prohibits monopolistic behaviors. The DSA creates a framework for platform liability regarding illegal content, emphasizing transparency and reporting mechanisms. Key harms necessitating regulation include defamation, hate speech, incitement to violence, terrorist content, child sexual abuse material, racial discrimination, misleading advertising, data breaches, excessive data collection, unauthorized processing, violation of user rights, and monopolistic practices. he effectiveness of this legal architecture depends on continuous cooperation between the European Commission, national authorities, and the platforms themselves.

Keywords: European Union, Media, Social media, Regulation

1- Associate Prof, Media Management Communication and Media IRIBU, Tehran, Iran
mahdi.farajian@iribu.ac.ir

دوفصلنامه
مطالعات فقه و حقوق رسانه
دانشکده غیردولتی – غیرانتفاعی رفاه

دوره ۸، شماره ۲ (پیاپی ۱۶)
پاییز و زمستان ۱۴۰۵
صص: ۳۵۷-۳۸۹

ضرورت‌های تنظیم‌گری رسانه‌های اجتماعی: تحلیلی بر قوانین اتحادیه اروپا

DOI: 10.22034/jlsm.2026.2084209.1089

نوع مقاله: مروری

تاریخ دریافت: ۱۴۰۴/۱۱/۱۴ **تاریخ بازنگری:** ۱۴۰۵/۰۳/۱۴ **تاریخ پذیرش:** ۱۴۰۵/۰۶/۲۱

محمدمهدی فرجیان[۱]

چکیده

چالش تنظیم‌گری رسانه‌های اجتماعی ناشی از تزاحم حق حاکمیت برای مقابله با کژکارکردها از یک‌سو و صیانت از برخی حقوق ذاتی مانند آزادی بیان و حریم خصوصی کاربران از سوی‌دیگر است. اتحادیه اروپا در پاسخ به این چالش، چهارچوبی کلی متشکل از مقررات عمومی حفاظت از داده، قانون خدمات دیجیتال، قانون بازارهای دیجیتال و قانون هوش مصنوعی تدوین کرده است؛ اما جرم‌انگاری مصادیق عینی محتوای غیرقانونی را به قوانین داخلی کشورهای عضو احاله می‌نماید. مقررات عمومی حفاظت از داده، اصول هفت‌گانه را تعیین کرده و داده‌های حساس نظیر منشأ نژادی و عقاید سیاسی را تحت حمایت ویژه قرار داده است. قانون بازارهای دیجیتال با رویکرد پیش‌دستانه، سکو(پلتفرم)های بسیار بزرگ را به‌عنوان دروازه‌بان شناسایی و رفتارهای انحصاری را ممنوع می‌کند. قانون خدمات دیجیتال نیز چهارچوبی جامع برای مسئولیت سکوها در قبال محتوای غیرقانونی ایجاد کرده و بر شفافیت و سازوکارهای گزارش‌دهی تأکید دارد. کژکارکردهایی که ضرورت تنظیم‌گری رسانه‌های اجتماعی را ایجاب می‌کنند، طیف گسترده‌ای از رفتارهای مجرمانه و آسیب‌زا را دربرمی‌گیرند. مهم‌ترین این موارد عبارت‌اند از: افترا، نفرت‌پراکنی، ترغیب به خشونت، محتوای تروریستی، سوءاستفاده از کودکان در قالب هرزه‌نگاری و بهره‌کشی جنسی و تبعیض نژادی که به‌عنوان مصادیق اصلی محتوای غیرقانونی شناخته شده‌اند. از دیگر کژکارکردها می‌توان به تبلیغات گمراه‌کننده و عدم شفافیت در کارزارهای انتخاباتی، قصور در حفاظت از اطلاعات و مقابله با حملات سایبری، جمع‌آوری بیش از حد داده‌ها، پردازش غیرمجاز داده‌های کاربران، تضییع حقوق کاربران، و رفتارهای انحصارطلبانه اشاره کرد که هر یک در قوانین مربوطه جرم‌انگاری شده‌اند.

واژگان کلیدی

رسانه‌های اجتماعی، تنظیم‌گری، رسانه.

---

۱. استادیار گروه مدیریت رسانه، دانشکده ارتباطات و رسانه، دانشگاه صدا و سیما، تهران، ایران.
mahdi.farajian@iribu.ac.ir

مقدمه

با گسترش فضای مجازی و افزایش نقش فعالانه کاربران در این فضا، موضوع رابطه حکومت‌ها با این عرصه بیش از گذشته مورد توجه قرار گرفته است. در دوران رسانه‌های مکتوب و الکترونیک، اگرچه بسیاری از بخش‌ها خصوصی شده بود؛ اما دولت‌ها از طریق ابزارهایی مانند کنترل فرکانس‌ها، ماهواره و مجوزهای قانونی، تسلط قابل‌توجهی بر محتوا داشتند. تولید محتوا در آن دوره، پس از سال‌ها تجربه و آزمون و خطا، عمدتاً زیر نظر حکومت‌ها صورت می‌گرفت و در نظام‌های سیاسی مختلف، برخورد با متخلفان از چهارچوب‌های تعیین‌شده کاملاً روشن بود؛ اما با ظهور شبکه‌های اجتماعی، هر کاربر به تولیدکننده‌ای بالقوه تبدیل شد و این امر به‌تدریج زمینه‌ساز برخی کژکارکردها شد. درنتیجه، تنظیم‌گری فضای مجازی به یکی از اولویت‌های مهم دولت‌ها تبدیل شده تا از اثرهای منفی احتمالی آن جلوگیری شود؛ لیکن این ورود حاکمیت، به‌دلایل مختلف به‌سادگی و بدون مقاومت نیست.

برخی از حقوق‌دانان ورود به این حوزه را در تزاحم با مواد قانونی ناظر به آزادی بیان توصیف می‌کنند. وفق رویکردی که در کشورهای اروپایی مانند آلمان و فرانسه بیش‌تر طرفدار دارد، آزادی بیان به آزادی در بیان عقیده و نظر از طریق وسایل ارتباط جمعی گفته می‌شود *(انصاری، ۱۳۹۳، ص. ۹)*، بر این‌اساس، مبتنی بر برخی مواد قانونی ناظر به آزادی بیان مانند ماده ۱۰ توافق‌نامه اروپایی حقوق بشر (*European Convention on Human Rights, Art. 10, 1950*) و ماده ۵ قانون اساسی آلمان، اساساً حاکمیت حق ورود به فضای مجازی و محتوای تولید شده در آن را ندارد.

همین تزاحم حقوق، در مورد قوانین ناظر بر حمایت از حریم خصوصی نیز وجود دارد. شورای اروپا در قطعنامه‌ای (۱۹۷۰) حریم خصوصی را این‌گونه تعریف می‌کند: حریم خصوصی مربوط می‌شود به زندگی خصوصی، خانوادگی و مسکن افراد، تمامیت جسمی، روحی، آبرو، اعتبار و شهرت و حیثیت افراد، اجتناب از ایکه چهره کاذبی از شخص ارائه داده شود، عدم افشای وقایع و حقایق نامربوط و آزاردهنده، افشای غیرمجاز تصاویر خصوصی افراد، حمایت از عدم افشای اطلاعاتی که در نتیجه اعتماد از سوی اشخاص

وصول شده و یا در اختیار آنها قرار گرفته است *(انصاری، ۱۳۸٦، ص. ۲۲۱)*.

بر این‌اساس تدوین قوانین در حوزه تنظیم‌گری رسانه فی‌ذاته با ملاحظات حقوقی فراوان همراه است. چه اینکه اگر شمول قوانین بخواهد از گستره یک کشور فراتر رفته و چندین کشور را زیر چتر حقوقی خود بگیرد، مسئله از این نیز پیچیده‌تر خواهد شد. اتفاقی که در تدوین قوانین این حوزه در اتحادیه اروپا رقم خورده است. قوانین موضوعه باید به‌گونه‌ای باشد که هم تزاحمات مذکور را لحاظ نماید و هم تفاوت‌های رویکرد کشورهای مختلف که برگرفته از مبانی حقوقی مختلف آن‌هاست. به همین دلیل است که در عمده قوانینی که در کمیسیون اتحادیه اروپا وضع شده‌اند، عناوین تخلفات به‌صورت کلی تعریف و مصادیق به قوانین داخلی کشورها احاله شده است.

برای روشن‌تر شدن موضوع، مقوله «تحریک به تبعیض نژادی» را به‌عنوان مثالی در این خصوص مورد بررسی دقیق‌تر قرار می‌دهیم. نخست تحریک به تبعیض نژادی محل تلاقی آزادی بیان با اصل منع تبعیض است که هر دو از شأن و نقش برجسته‌ای در نظام بین‌المللی حقوق بشر برخوردارند *(انصاری و امام‌الطرقی، ۱۳۹۹)*. لیکن در خصوص مقوله تحریک به تبعیض نژادی در قوانین مربوطه اتحادیه اروپا (قانون *DSA*) اشاره مستقیم صورت نگرفته است و ذیل محتوای غیرقانونی در قانون مزبور دانسته شده است. تشخیص جرم‌انگاری آن و چگونگی این امر به قوانین هر کشور عضو اتحادیه ارجاع شده است؛ مثلا آلمان در این خصوص مبتنی بر قانون خود (قانون *NetzDG*) رویکرد «حذف اجباری و جریمه سنگین» را در پیش گرفته که به حذف افراطی محتوا انجامیده، درحالی‌که فرانسه به دلیل تأکید بیش‌تر بر آزادی بیان، در قانون خود*(Avia)* با رواداری بیش‌تری با این دست از محتوا برخورد کرده است. برخی کشورها مانند سوئد نیز دامنه قوانین را فراتر از نژاد، به مواردی مثل گرایش جنسی گسترش داده‌اند.

با این نگاه در پژوهش حاضر ابتدا مروری بر مهم‌ترین قوانین موضوعه در اتحادیه اروپا در خصوص تنظیم‌گری رسانه‌های اجتماعی خواهیم داشت. سپس با بررسی قوانین مذکور، به اقدامات تقنینی صورت گرفته در خصوص کژکارکردهای مهم رسانه‌های اجتماعی پرداخته خواهد شد.

چنانچه پیش‌تر نیز گفته شد، فهرست مدون و قابل‌اتفاقی از اقدامات ممنوعه و مجرمانه در حوزه رسانه‌های اجتماعی وجود ندارد و این موارد بسته به زیرساخت تقنینی هر کشور متفاوت است؛ لیکن برخی مصادیق عموماً از سوی کشورها به‌عنوان مواردی که ضرورت‌های تنظیم‌گری می‌باشد در قوانین مورد امعان نظر قرار گرفته است.

بر اساس آنچه پیش‌تر آمد، چالش اصلی تنظیم‌گری رسانه‌های اجتماعی در اتحادیه اروپا، تزاحمی دوسویه است: از یک‌سو ضرورت حاکمیت برای مقابله با کژکارکردهایی چون افترا، نفرت‌پراکنی، خشونت و تبعیض نژادی، و از سوی‌دیگر صیانت از حقوق بنیادینی مانند آزادی بیان و حریم خصوصی کاربران. حال این پرسش مطرح می‌شود که این چهارچوب کلی متشکل از کدام قوانین و مقررات است و هر یک از آنها چه جایگاهی در نظام تنظیم‌گری رسانه‌های اجتماعی دارند؟ در پاسخ به این پرسش، در بخش بعدی، مهم‌ترین قوانین موضوعه اتحادیه اروپا معرفی و تحلیل می‌گردند تا زیرساخت حقوقی برای شناسایی ضرورت‌های عینی تنظیم‌گری فراهم آید.

۱. مروری بر قوانین موضوعه در اتحادیه اروپا در حوزه تنظیم‌گری رسانه‌های اجتماعی

فضای مجازی به‌صورت عام و شبکه‌های اجتماعی به‌صورت خاص علاوه بر مزایای فراوانی که برای انسان‌ها فراهم کرده، مانند بسیاری از پدیده‌های بشری دس‌خوش برخی سوءاستفاده‌ها هم بوده است. برای آنکه بدانیم چه اقداماتی می‌تواند واجد سوءاستفاده و یا تبعات منفی لحاظ گردد، ابتدا مقررات موضوعه در حوزه تنظیم‌گری رسانه‌های اجتماعی در اتحادیه اروپا بررسی شده است. این قوانین در سطح اتحادیه اروپا وضع شده‌اند که برای همه کشورهای عضو این اتحادیه لازم‌الاتباع هستند. همچنین برخی از کشورهای عضو این اتحادیه نیز به‌صورت مجزا قوانینی را برای سامان‌دهی به این حوزه در قلمرو خود وضع کرده‌اند. در حال‌حاضر موارد زیر مهم‌ترین قوانین جاری اتحادیه اروپا در زمینه تنظیم‌گری رسانه‌های اجتماعی محسوب می‌شوند:

- مقررات عمومی حفاظت از داده در اتحادیه اروپا (*GDPR*[1])
- قانون بازارهای دیجیتال (*DMA*[2])
- قانون خدمات دیجیتال (*DSA*[3])
- قانون تنظیم‌گری هوش مصنوعی[4]
- دستورالعمل خدمات سمعی و بصری (*AVMSD*[5])
- قانون تقویت شبکه آلمان[6]
- قانون تأمین و تنظیم فضای دیجیتال فرانسه[7]

در پژوهش حاضر ابتدا معرفی اجمالی در خصوص آن دسته از قوانین فوق که در اتحادیه اروپا وضع شده‌اند ارائه می‌شود. سپس با بررسی محتوایی دقیق‌تر این قوانین در پی آن خواهیم بود تا مواردی که از سوی آنها جرم‌انگاری شده و یا هدف تنظیم‌گری واقع شده را احصاء نماییم که درواقع ضرورت‌های تنظیم‌گری رسانه‌های اجتماعی در اتحادیه اروپا محسوب می‌گردد.

۱-۱. مقررات عمومی حفاظت از داده در اتحادیه اروپا (*GDPR*)

اتحادیه اروپا در سال ۲۰۱۶ قانون «مقررات عمومی حفاظت از داده» را برای نظارت بر فعالیت کسب‌وکارهای دیجیتال تصویب کرد. این مقررات، یکی از مهم‌ترین و جامع‌ترین قوانین حفاظت از داده‌ها در سطح جهان محسوب می‌شود که از اواسط سال ۲۰۱۸ در همه کشورهای عضو اتحادیه اروپا لازم‌الاجرا و جایگزین دستورالعمل‌های قبلی شده است. هدف اصلی قانون، حمایت از افراد حقیقی در برابر پردازش داده‌های شخصی در بخش خصوصی و عمومی، و در عین‌حال تسهیل جریان آزاد داده‌ها در بازار واحد دیجیتال اتحادیه اروپا است. ماده ۵ این قانون اصول هفتگانه‌ای را تعریف کرده که همه فعالیت‌های

1. General Data Protection Regulation
2. Digital Markets Act
3. Digital Services Act
4. EU AI Act
5. Audiovisual Media Services Directive
6. Grundgesetz für die Bundesrepublik Deutschland
7. Loi SREN

پردازش داده باید از آن پیروی کنند. این اصول در جدول شماره ۱ آمده است:

جدول ۱: اصول هفت‌گانه مقررا حفاظت از داده در اتحادیه اروپا

اصل	توضیح
قانونمندی، انصاف و شفافیت	پردازش داده باید با مبنای قانونی معتبر و به‌صورت شفاف انجام شود
محدودیت هدف	داده‌ها فقط برای اهداف مشخص و قانونی جمع‌آوری شوند
حداقل‌سازی	داده‌فقط داده‌های ضروری برای هدف مورد نظر جمع‌آوری شوند
دقت	داده‌ها باید به‌روز و دقیق باشند
محدودیت نگهداری	داده‌ها بیش از مدت لازم نگهداری نشوند
یکپارچگی و محرمانگی	اقدامات امنیتی مناسب برای جلوگیری از دسترسی غیرمجاز
مسئولیت‌پذیری	سازمان باید توانایی اثبات انطباق با *GDPR* را داشته باشد

در ماده ٦ قانون *GDPR*، شش مبنای قانونی برای پردازش داده‌های شخصی تعیین شده است که عبارت‌اند از: نخست، رضایت[1] که بر اساس آن فرد باید به پردازش داده‌های خود برای یک یا چند هدف خاص رضایت داده باشد. دوم، اجرای قرارداد[2] که در آن پردازش برای اجرای تعهدات قراردادی ضروری است. سوم، تعهد قانونی[3] که به موجب آن پردازش برای رعایت یک تعهد قانونی لازم می‌گردد. چهارم، حفاظت از منافع حیاتی[4] که طی آن پردازش برای حفاظت از جان فرد ضروری تلقی می‌شود. پنجم، وظیفه عمومی[5] که بر اساس آن پردازش برای انجام وظایف عمومی یا اعمال قدرت رسمی صورت می‌پذیرد و ششم، منافع مشروع[6] که بر مبنای آن پردازش برای منافع مشروع کنترل‌کننده ضروری است، مگر اینکه حقوق فرد بر آن منافع اولویت داشته باشد. ماده ٦ این قانون همچنین تأکید می‌کند که رضایت باید آزادانه، مشخص، آگاهانه و بدون ابهام باشد و به همان سهولتی که داده شده است، قابل لغو باشد.

وفق ماده ۹ قانون *GDPR*، برخی داده‌ها به دلیل حساسیت بالا نیازمند محافظت بیش‌تری

1. Consent
2. Contract
3. Legal Obligation
4. Vital Interests
5. Public Task
6. Legitimate Interests

هستند و پردازش این داده‌ها نیازمند اجازه قانونی مضاعف (مانند رضایت صریح) است. این داده‌های حساس شامل منشأ نژادی یا قومی، عقاید سیاسی، باورهای مذهبی یا فلسفی، عضویت در اتحادیه‌های کارگری، داده‌های ژنتیکی، داده‌های بیومتریک برای احراز هویت منحصربه‌فرد، داده‌های سلامت و همچنین داده‌های مربوط به زندگی جنسی یا گرایش جنسی می‌باشند.

درنهایت وفق مواد ۱۲ تا ۲۳ قانون *GDPR*، حقوق متعددی برای افراد (صاحبان داده) در نظر گرفته شده است. این حقوق عبارت‌اند از: «حق دسترسی[1]» که بر اساس آن افراد می‌توانند به داده‌های پردازش‌شده خود دسترسی داشته باشند و از آن روگرفت تهیه کنند، «حق تصحیح[2]» به‌معنای تصحیح داده‌های نادرست یا ناقص، «حق حذف[3]» که همان حق فراموش شدن و حذف داده‌ها در شرایط خاص است، «حق محدودیت پردازش[4]» برای محدود کردن پردازش داده در هنگام اختلاف، «حق انتقال‌پذیری داده[5]» که امکان انتقال داده‌ها بین ارائه‌دهندگان مختلف خدمات را فراهم می‌کند، «حق اعتراض[6]» به پردازش به‌ویژه برای بازاریابی مستقیم و همچنین «حقوق مربوط به تصمیم‌گیری خودکار» که هدف آن محافظت از افراد در برابر تصمیم‌گیری‌های الگوریتمی با اثرهای قابل‌توجه است. شایان ذکر است که سازمان‌ها موظفند ظرف یک ماه به درخواست‌های افراد پاسخ دهند و به‌طور کلی نمی‌توانند برای اعمال این حقوق هزینه‌ای دریافت کنند.

نظام جرایم مقررات عمومی حفاظت از داده (*GDPR*) در بالاترین سطح در میان قوانین حفاظت از داده در جهان قرار دارد، به‌گونه‌ای‌که برای «تخلفات جزئی» نظیر عدم نگهداری سوابق مناسب، جریمه‌ای معادل ۱۰ میلیون یورو یا ۲ درصد از گردش مالی سالانه جهانی شرکت متخلف (هرکدام که بیش‌تر باشد) در نظر گرفته شده است. درمقابل، برای «تخلفات اساسی» مانند نقض اصول پردازش یا تضییع حقوق افراد، جریمه بسیار سنگین‌تری اعمال می‌شود که به ۲۰ میلیون یورو یا ٤ درصد از گردش مالی سالانه جهانی (باز هم هرکدام

1. Right of Access
2. Right to Rectification
3. Right to Erasure
4. Right to Restriction
5. Right to Data Portability
6. Right to Object

که بیش‌تر باشد) می‌رسد. این ساختار جریمه‌های پلکانی و بازدارنده، نشان‌دهنده عزم جدی اتحادیه اروپا برای تضمین بالاترین سطح حفاظت از داده‌های شخصی در فضای دیجیتال است (*Publications Office of the European Union, 2022*).

۱-۲. قانون بازارهای دیجیتال (*DMA*)

هدف اصلی قانون بازارهای دیجیتال (*DMA*)، ایجاد بازارهای رقابتی و عادلانه در بخش دیجیتال با تمرکز بر سکوهای بزرگ برخط است. این قانون با اتخاذ رویکرد «پیش‌دستانه» به جای بررسی پس از وقوع تخلف (مانند قوانین سنتی رقابت)، قواعد رفتاری مشخصی را برای سکوها تعیین می‌کند. اهداف کلیدی این قانون عبارت‌اند از: ایجاد محیط رقابتی‌تر برای کسب‌وکارهای کوچک و جدید، افزایش انتخاب و کنترل کاربران نهایی بر داده‌ها و تجربه دیجیتال خود، جلوگیری از سوءاستفاده سکوهای بزرگ از موقعیت مسلط آنها و درنهایت یکسان‌سازی قوانین در سراسر بازار واحد اروپا به‌منظور جلوگیری از تفرقه در قوانین ملی کشورهای عضو. در ماده ۳ این قانون نیز شرکت‌های بزرگ با احراز ویژگی‌های خاصی به عنوان «دروازه‌بان[1]» تعریف شده‌اند که این ویژگی‌ها به تفصیل در جدول شماره ۲ ارائه شده است.

جدول ۲: معیارهای قانون بازارهای دیجیتال برای تعیین شرکتها بعنوان دروازه‌بان

معیار	شرح
تأثیر قابل‌توجه بر بازار داخلی	گردش مالی سالانه در اتحادیه اروپا ≥ ۷.۵ میلیارد یورو یا ارزش بازار ≥ ۷۵ میلیارد یورو
تعداد بالای کاربران فعال[2]	حداقل ٤٥ میلیون کاربر نهایی فعال ماهانه در اتحادیه اروپا و ۱۰,۰۰۰ کاربر تجاری فعال سالانه
موقعیت تجاری بادوام	شرکت به مدت سه سال مالی متوالی دو معیار بالایی را داشته باشد

قانون *DMA* در ماده ۲ خود، ده دسته از خدمات دیجیتال را تحت پوشش مقررات خود قرار می‌دهد. این خدمات عبارت‌اند از: خدمات واسطه‌گری برخط نظیر فروشگاه‌ها و

1. Gatekeeper
2. Active User

بازارهای برخط، موتورهای جستجوی برخط، خدمات شبکه‌های اجتماعی برخط، خدمات سکوی اشتراک ویدیو، خدمات ارتباطی بین‌فردی بدون نیاز به شماره تلفن، سیستم‌های عامل مانند *iOS*، اندروید و *Windows*، مرورگرهای وب، دستیارهای مجازی، خدمات محاسبات ابری و درنهایت خدمات تبلیغات برخط. این طبقه‌بندی گسترده نشان‌دهنده رویکرد جامع قانون *DMA* در پوشش تمامی اجزای کلیدی اقتصاد دیجیتال است. کمیسیون اروپا تا کنون شرکت‌های آلفابت[۱] (گوگل)، آمازون[۲]، اَپل[۳]، تیک‌تاک[۴]، متا[۵]، ماکروسافت[۶] و بوکینگ دات کام[۷] را به‌عنوان دروازبان تعریف کرده است که الزامات مندرج در ماده ۵ و ٦ قانون را باید رعایت کنند (*European Commission,2023*) و در صورت تخلف ملزم به پرداخت جرائم مربوطه می‌شوند.

در صورت تخلف از مواد قانون *DMA*، جرائمی پلکانی و بازدارنده برای دروازه‌بانان در نظر گرفته شده است که در مواد ۳۰ تا ۳۳ این قانون تصریح گردیده است. برای تخلف اولیه، جریمه تا سقف ۱۰ درصد از گردش مالی کل سالانه جهانی شرکت تعیین شده است. در صورت تکرار تخلف، این جریمه تا ۲۰ درصد از گردش مالی کل سالانه جهانی شرکت افزایش می‌یابد. همچنین برای مواردی نظیر عدم ارائه اطلاعات، جریمه دوره‌ای تا ۵ درصد از میانگین گردش مالی روزانه جهانی شرکت اعمال می‌گردد. شایان ذکر است که وفق همین مواد، در مواجهه با تخلفات نظام‌مند، کمیسیون اروپا فراتر از جرایم نقدی، می‌تواند اقدامات رفتاری مانند اصلاح رویه‌های تجاری و حتی اقدامات ساختاری ازجمله جداسازی بخشی از کسب‌وکار شرکت را نیز نسبت به دروازه‌بانان اعمال نماید که این امر نشان‌دهنده رویکرد سختگیرانه و ساختارشکن اتحادیه اروپا در برابر انحصارهای دیجیتال است (*European Parliament and Council of the European Union, 2022*).

1. Alphabet
2. Amazon
3. Apple
4. TikTok
5. Meta
6. Microsoft
7. Booking.com

۱-۳. قانون خدمات دیجیتال (*DSA*)

قانون خدمات دیجیتال (*DSA*) که در ۱۹ اکتبر ۲۰۲۲ به تصویب رسید، یکی از مهم‌ترین و جامع‌ترین قوانین اتحادیه اروپا در زمینه تنظیم‌گری فضای مجازی محسوب می‌شود. درواقع *DSA* به همراه *DMA*، ستون‌های اصلی چهارچوب نظارتی اتحادیه اروپا بر اقتصاد دیجیتال و سکوهای برخط را تشکیل می‌دهند. اهداف کلیدی این قانون عبارت‌اند از: مقابله با محتوای غیرقانونی برخط بدون ایجاد محدودیت غیرضروری بر آزادی بیان، حفاظت از حقوق بنیادین کاربران نظیر آزادی بیان، حریم خصوصی و عدم تبعیض، ایجاد هماهنگی در قوانین در سراسر بازار داخلی اتحادیه اروپا به‌منظور جلوگیری از تفرقه در قوانین ملی کشورهای عضو، ایجاد شفافیت در مورد نحوه تعدیل محتوا و عملکرد الگوریتم‌ها و درنهایت مسئولیت‌پذیری سکوها در قبال ریسک‌های سیستمی مانند انتشار اطلاعات نادرست. این اهداف پنج‌گانه نشان‌دهنده رویکرد متوازن *DSA* در حفظ حقوق کاربران در عین الزام سکوها به پاسخگویی در قبال محتوای مضر است.

اتحادیه اروپا با تصویب قانون خدمات دیجیتال (*DSA*)، چهارچوبی جامع برای مسئولیت سکوهای برخط در قبال محتوای غیرقانونی و شفافیت عملیاتی آنها ایجاد کرده است. هدف اصلی این قانون، تأمین فضایی امن‌تر برای کاربران و حفظ حقوق اساسی آنان در عین فراهم آوردن بستری مناسب برای رقابت و نوآوری کسب‌وکارهاست.

محورهای کلانی *DSA* عبارت‌اند از:

۱. تعیین مسئولیت و رویه‌های مقابله با محتوای غیرقانونی: برای نخستین‌بار در این قانون، مسئولیت‌های حقوقی سکوها در قبال انتشار محتوای غیرقانونی روشن شده و مدل شفافی برای اقدام در هنگام شناسایی چنین محتوایی تعریف شده است.

۲. یکی از محورهای کلیدی قانون خدمات دیجیتال (*DSA*)، افزایش شفافیت و کنترل کاربران بر تجربه دیجیتال خود است. بر این‌اساس، سکوها موظف شده‌اند عملکرد الگوریتم‌های پیشنهاد محتوا (ازجمله در حوزه تبلیغات) را برای کاربران افشا کنند. همچنین کاربران باید این امکان را داشته باشند که سیستم‌های پیشنهاد مبتنی بر رخ‌نماسازی را در صورت تمایل غیرفعال نمایند. در مواردی نیز که سکو اقدام به حذف یا محدود کردن

محتوای تولیدشده توسط کاربر (*UGC*) می‌کند، ملزم است دلیل مشخص و روشنی برای این اقدام ارائه دهد. افزون‌براین، سکوها باید گزارش‌های عمومی مستندی از درخواست‌های حذف محتوا توسط مقامات ملی و همچنین از میزان دقت و خطای ابزارهای کنترل خودکار محتوا منتشر کنند تا فرایند تعدیل محتوا برای همگان قابل نظارت و ارزیابی باشد.

۳. ایجاد سازوکار سه‌لایه‌ای حل اختلاف: کاربران باید بتوانند ابتدا از طریق سازوکار درون‌پلتفرمی، سپس از طریق مراجع حل‌وفصل اختلاف خارج از دادگاه، و درنهایت از طریق مراجع قضائی، به اقدامات سکو اعتراض و خسارت دریافت کنند.

٤. ممنوعیت تبلیغات هدفمند بر اساس داده‌های حساس: نمایش تبلیغات بر مبنای داده‌های حساسی مانند گرایش جنسی یا سیاسی ممنوع شده است.

قانون خدمات دیجیتال (*DSA*) در کنار قانون بازارهای دیجیتال (*DMA*)، برای سکوهای بسیار بزرگی که نقش «دروازه‌بان» را ایفا می‌کنند (با معیارهایی نظیر ارزش بازار بالای ۷۵ میلیارد یورو یا داشتن حداقل ٤٥ میلیون کاربر ماهانه در اتحادیه اروپا)، مجموعه‌ای از تعهدات سخت‌گیرانه‌تر را وضع می‌کند. این تعهدات در دو دسته الزامات مثبت و ممنوعیت‌ها قابل تقسیم‌بندی هستند. در دسته الزامات مثبت، دروازه‌بانان موظف به همکاری با خدمات شخص ثالث از جمله فراهم کردن قابلیت تعامل پیام‌رسان‌های کوچک با سکوهای بزرگ، ارائه داده‌های تولیدشده به کسب‌وکارهای استفاده‌کننده و همچنین اجازه دادن به کسب‌وکارها برای عقد قرارداد مستقیم با مشتریان خارج از سکو می‌باشند. درمقابل، دسته ممنوعیت‌ها شامل خودبرتری‌جویی در رتبه‌بندی نتایج (یعنی ترجیح غیرمنصفانه خدمات خود بر رقبا)، جلوگیری از ارتباط کاربران با کسب‌وکارها خارج از سکو و ممانعت از حذف اپلیکیشن‌های پیش‌نصب‌شده می‌گردد. این ترکیب از بایدها و نبایدها، تلاشی نظام‌مند برای مهار قدرت نامتقارن سکوهای بزرگ و بازگرداندن تعادل به بازار دیجیتال اروپا محسوب می‌شود.

کمیسیون اروپا اختیار نظارت مستقیم بر سکوهای بسیار بزرگ و وضع جریمه را دارد. جریمه‌ها می‌تواند تا ۱۰درصد از درآمد جهانی سالانه شرکت و در صورت تکرار تا ۲۰

درصد باشد. در موارد نقض نظام‌مند، حتی امکان مسدودسازی موقت سکو در بازار اتحادیه اروپا وجود دارد.

این قوانین که در سال ۲۰۲۲ به تصویب نهایی رسیدند، نشان‌دهنده عزم اتحادیه اروپا برای بروزرسانی قواعد حکمرانی دیجیتال و شکل‌دهی به فضای دیجیتالی امن، منصفانه و رقابتی در محدوده خود هستند (*European Parliament and Council of the European Union, 2022*).

لازم به ذکر است مهم‌ترین سیاست‌گذاری در اروپا در زمینه کنترل اطلاعات گمراه‌کننده، در سال ۲۰۱۸ تحت عنوان «قانون جامع ملاحظات خودتنظیم‌گری بر اطلاعات گمراه‌کننده برخط[1]» شکل گرفت. این قانون که با توافق سران کشورهای اتحادیه اروپا تصویب شد، بر خودتنظیم‌گری محتوای گمراه‌کننده برخط تأکید داشت و استفاده از فناوری‌هایی مانند هوش مصنوعی را برای مقابله با این محتوا ضروری می‌دانست (*Marsden, 2019*). این قانون اولین سند از نوع خود در سطح جهان بود که برای مقابله با انتشار اطلاعات نادرست و گمراه‌کننده در فضای برخط طراحی شد و هدف اصلی آن ایجاد محیط دیجیتال امن‌تر و قابل اعتمادتر از طریق افزایش مسئولیت‌پذیری سکوهای برخط بود (*European Commission, 2018*). وفق قانون مذکور، سکوهای بزرگ (مانند گوگل، متا، مایکروسافت و تیک‌تاک) داوطلبانه پذیرفتند که به مجموعه‌ای از تعهدات برای مبارزه با اطلاعات نادرست پایبند باشند. «قانون جامع ملاحظات خودتنظیم‌گری بر اطلاعات گمراه‌کننده برخط» از جولای ۲۰۲۵، به‌طور رسمی در چهارچوب قانون خدمات دیجیتال (*DSA*) ادغام شد.

۱-۴. قانون هوش مصنوعی اتحادیه اروپا

استفاده از الگوریتم‌ها به‌ویژه هوش مصنوعی برای اخذ تصمیمات مختلف، مسائل و پرسش‌های حقوقی متعددی را برانگیخته است. یکی از این مسائل، تبعیض‌آمیز بودن تصمیمات الگوریتمی است. این تبعیض ممکن است در خصوص یک فرد یا گروه یا طبقه‌ای از افراد جامعه صورت گیرد. با توجه به وظیفه دولت‌ها برای مقابله با انواع تبعیض، شناسایی مصادیق و علل و تبعیض‌های الگوریتمی و ارائه راهکارهای مقابله با آنها به یکی

1. The EU Code of Conduct on Disinformation

از موضوعات حقوقی روز تبدیل شده است *(انصاری، ۱۴۰۱)*.

قانون هوش مصنوعی اتحادیه اروپا اولین و جامع‌ترین چهارچوب قانونی جهان برای تنظیم‌گری هوش مصنوعی است. این قانون در ۱۳ ژوئن ۲۰۲۴ توسط پارلمان اروپا و شورای اتحادیه اروپا تصویب شد. هدف اصلی این قانون، ترویج توسعه و پذیرش سیستم‌های هوش مصنوعی ایمن و قابل اعتماد در بازار داخلی اتحادیه اروپا، هم در بخش خصوصی و هم در بخش عمومی، و در عین‌حال تضمین سطح بالایی از حفاظت از سلامت، ایمنی و حقوق بنیادین شهروندان است.

قانون هوش مصنوعی اتحادیه اروپا بر چهار رویکرد اساسی استوار است. نخست، «رویکرد مبتنی بر ریسک[1]» که بر اساس آن هرچه ریسک ناشی از سیستم هوش مصنوعی برای جامعه بیش‌تر باشد، قوانین سخت‌گیرانه‌تری بر آن اعمال می‌شود. دوم، «انسان‌محوری[2]» که بر اساس آن هوش مصنوعی با هدف نهایی افزایش رفاه بشری باید همواره به عنوان ابزاری در خدمت انسان‌ها باشد نه جایگزین آنها. سوم، «جلوگیری از تفرقه در بازار» از طریق ایجاد قوانین یکسان در سراسر اتحادیه اروپا که مانع از وضع قوانین متفاوت ملی و در نتیجه تفرقه در بازار داخلی می‌گردد. چهارم، «حمایت از نوآوری» بدین‌معنا که این قانون با ایجاد محیطی امن و قابل پیش‌بینی برای توسعه سیستم‌های هوش مصنوعی، نوآوری را تشویق کرده و به ویژه بر حمایت از کسب‌وکارهای کوچک و متوسط (*SMEs*) تمرکز دارد. این چهار رویکرد به‌طور همزمان نشان‌دهنده تلاش اتحادیه اروپا برای ایجاد تعادل میان پیشرفت فناورانه، حفظ حقوق بنیادین و تضمین رقابت‌پذیری بازار است.

قانون *AI Act* سیستم‌های هوش مصنوعی را به چهار سطح ریسک تقسیم کرده و در ماده ۵، کاربردهای هوش مصنوعی با ریسک‌های غیرقابل قبول را ممنوع کرده است (*Publications Office of the European Union,2025*).

بررسی قوانین چهارگانه فوق یعنی مقررات عمومی حفاظت از داده (*GDPR*)، قانون بازارهای دیجیتال (*DMA*)، قانون خدمات دیجیتال (*DSA*) و قانون هوش مصنوعی (*AI Act*)

1. Risk-based approach
2. Human-centric

نشان می‌دهد که اتحادیه اروپا چهارچوبی چندلایه و پیش‌دستانه برای تنظیم‌گری رسانه‌های اجتماعی تدوین کرده است. این قوانین به‌ترتیب بر حمایت از داده‌های شخصی، مقابله با انحصار سکوهای بزرگ، شفافیت در مواجهه با محتوای غیرقانونی و مدیریت ریسک‌های ناشی از هوش مصنوعی متمرکز هستند. با این‌حال، صرفِ وجود چنین چهارچوب نهادی و هنجاری برای پاسخ به کژکارکردهای عینی و روزمره شبکه‌های اجتماعی کافی نیست؛ بلکه لازم است مصادیق مشخص و عینی رفتارهای مجرمانه و آسیب‌زا که این قوانین به دنبال مهار آنها هستند، به‌صورت تفکیک‌شده و نظام‌مند احصاء گردد. به عبارت‌دیگر، پس از آشنایی با ابزارهای حقوقی، باید «ضرورت‌های عینی تنظیم‌گری» را مبتنی بر همان قوانین شناسایی کنیم. ضرورت‌هایی که از قصور در حفاظت از داده‌ها و جمع‌آوری بیش‌ازحد اطلاعات گرفته تا محتوای غیرقانونی، نفرت‌پراکنی، سوءاستفاده از کودکان و انحصار را دربرمی‌گیرد. از این‌رو، در بخش سوم با استناد به قوانین معرفی‌شده، مهم‌ترین موارد ناظر به این کژکارکردها به‌صورت مجزا تحلیل خواهد شد.

۲. ضرورت‌های تنظیم‌گری شبکه‌های اجتماعی با نگاه به قوانین موضوعه

اولین موضوعاتی که باعث شد نیاز به کنترل بیش‌تر در شبکه‌های اجتماعی احساس شود، مقابله با توهین و افترا، نشر نفرت، خشونت‌ورزی و تبلیغات فریبنده در این سکوها بود. این موارد حداقل‌های ضروری از جنبه‌های سیاسی و اجتماعی بودند که نظارت بر آنها در فضای رسانه‌های اجتماعی اجتناب‌ناپذیر به نظر می‌رسید. به‌ویژه در دوره‌های انتخابات، مسائلی مانند شفافیت در تبلیغات انتخاباتی، رعایت قوانین حفاظت از داده‌ها و مقابله با حملات سایبری بیش از پیش اهمیت یافت.

در ادامه، پیشگیری از فعالیت‌های تروریستی نیز به یکی از اصلی‌ترین خواسته‌ها از نظام‌های نظارتی تبدیل شد و برای این‌منظور، از اقدامات پیشگیرانه و روش‌هایی مانند فیلترینگ محتوا استفاده شد (*Marsden, 2019*). به‌تدریج و با توسعه استفاده از این دست رسانه‌ها، موارد دیگر نیز به این فهرست افزوده شد که در ادامه به این موارد پرداخته شده است:

۲-۱. قصور در حفاظت از اطلاعات و مقابله با حملات سایبری

حفاظت از داده‌های کاربران یکی از اصول اساسی در فضای مجازی تلقی شده است که این امر، هم یک حق برای آحاد شهروندان محسوب می‌شود و هم یک تکلیف برای حاکمیت که با تنظیم‌گری مناسب بتواند به آن جامه‌ی عمل بپوشاند. طبق آنچه در حقوق اساسی اتحادیه اروپا آمده، تصریح شده است که حفاظت از داده‌های شخصی برای هر یک از شهروندان حقی محفوظ است. هر فردی حق دارد که از داده‌های شخصی خود حفاظت کند. همچنین حق دارد به این اطلاعات دسترسی داشته و آنها را عنداللزوم ویرایش نماید. در اروپا در سال ۲۰۱۶ به‌منظور آماده‌سازی این اتحادیه برای عصر دیجیتال، بسته حمایتی از داده‌ها اتخاذ شد. بیش از ۹۰درصد اروپایی‌ها می‌گویند که می‌خواهند حقوق مشابهی در زمینه حق نگهداری داده‌ها در اروپا داشته باشند، فارغ از اینکه داده‌های آنها کجا پردازش می‌شود. بر این‌اساس قانونی با عنوان «تنظیم‌گری عمومی حفاظت از داده‌ها» در اروپا شکل گرفت. این تنظیم‌گری برای حرکت به سمت توانمندسازی افراد برای استفاده از حق اساسی خود در عصر دیجیتال و تسهیل کسب‌وکارها با دسته‌بندی قوانین برای شرکت‌ها و حوزه عمومی بسیار اساسی است (*European Commission, 2023*). بنابراین، فرایندهای کسب‌وکاری که اطلاعات شخصی را مدیریت می‌کنند، باید بر پایه اصل محافظت از داده‌ها با طراحی و به‌صورت پیش‌فرض استوار باشند. این اصل ایجاب می‌کند که اطلاعات شخصی با استفاده از روش‌هایی مانند «مستعارسازی» یا «ناشناس‌سازی» ذخیره شوند تا هویت افراد تا حد ممکن پنهان بماند. همچنین بالاترین سطح محرمانگی باید به‌صورت پیش‌فرض رعایت شود، بدین معنا که داده‌ها بدون رضایت صریح فرد هرگز «عمومی نشوند» و بدون ارائه اطلاعات اضافی جداگانه، «قابل شناسایی نباشند». افزون‌براین، هیچ اطلاعات شخصی نباید پردازش شود، مگر آنکه بر اساس «مبنای قانونی مشخص» یا با «اجازه صریح و آزادانه» صاحب داده صورت گیرد. درنهایت، صاحب داده این حق را دارد که هر زمان بخواهد، اجازه داده شده را «لغو کند» و سکوها نیز موظف به پذیرش این لغو اجازه هستند. این چهار مؤلفه در کنار یکدیگر، نظامی حقوقی را شکل می‌دهند که در آن حفاظت از داده‌های شخصی نه یک اقدام واکنشی، بلکه یک الزام

پیش‌گیرانه و مستمر تلقی می‌شود (*European Commission, 2023*).

«حمله سایبری» به تلاش یک یا چند هکر برای نفوذ به یک سامانه یا شبکه گفته می‌شود. در تعریفی دیگر، حملات سایبری این‌گونه تعریف شده‌اند: رویدادهایی که به‌طور طبیعی یا توسط انسان (عمدی یا غیرعمدی) بر فضای مجازی تأثیر می‌گذارند، یا حوادثی که از طریق فضای مجازی رخ می‌دهند یا به نوعی با آن در ارتباط هستند. «فضای سایبری» نیز از سوی برخی کارشناسان به‌عنوان فضا و جامعه‌ای تعریف شده که توسط رایانه‌ها، اطلاعات و ابزارهای الکترونیکی، شبکه‌های دیجیتال و کاربران آن شکل می‌گیرد.

قانون عمومی حفاظت از داده‌ها، سنگ‌بنای اصلی تعهد امنیت داده‌ها است. عدم مقابله مؤثر با حملات سایبری که منجر به نقض داده می‌شود، عمدتاً نقض مواد زیر محسوب می‌گردد:

ماده ۳۲ قانون (*GDPR*) به‌صراحت مقرر می‌دارد که کنترل‌کننده و پردازشگر داده ملزم به اجرای اقدامات فنی و سازمانی مناسب برای تضمین سطح امنیتی متناسب با ریسک هستند. این شامل: الف) رمزگذاری (رمزنگاری) داده‌های شخصی؛ ب) تضمین محرمانگی، حفظ تمامیت، در دسترس بودن و انعطاف‌پذیری پایدار سامانه‌ها و خدمات؛ ج) امکان بازیابی دسترسی به داده‌ها و تداوم دسترسی به آنها پس از هر رویداد فیزیکی یا فنی و د) فرایند آزمون و ارزیابی منظم اثرگذاری اقدامات فنی و سازمانی. می‌شود. عدم اجرای این اقدامات، نقض مستقیم *GDPR* است.

همچنین وفق مواد ۳۳ و ۳٤، در صورت وقوع یک حمله سایبری که منجر به نقض داده شده، شبکه اجتماعی موظف است حداکثر ظرف ۷۲ ساعت پس از آگاهی، موضوع را به مقام ناظر (ماده ۳۳) و در صورت ریسک بالا برای حقوق افراد، به کاربران آسیب‌دیده (ماده ۳٤) اطلاع‌رسانی کند. عدم اطلاع‌رسانی به موقع یا پنهان‌کردن حمله، خود یک نقض جداگانه و بسیار جدی است. مجازات: نقض این مواد می‌تواند به جریمه‌هایی تا ۲۰ میلیون یورو یا ٤٪ از کل گردش مالی جهانی (هرکدام بالاتر است) منجر شود.

۲-۲. جمع‌آوری بیش از حد داده

این عمل نقض «اصل حداقل‌سازی داده » است که در ماده ٥ قانون *GDPR* آمده است. این اصل می‌گوید: داده‌های شخصی باید کافی، مرتبط و محدود به حداقل ضرورت، برای تحقق

اهدافی که برای آن‌ها پردازش می‌شوند، باشند. داده‌های شخصی فقط باید برای اهداف مشخص، صریح و قانونی جمع‌آوری شوند و نباید به شیوه‌ای ناسازگار با آن اهداف پردازش شوند. اقداماتی که ممکن است. وفق قانون *GDPR*، اقدامات متعددی می‌تواند مصداق «جمع‌آوری بیش از حد داده» محسوب شود. ازجمله این موارد می‌توان به جمع‌آوری داده‌ها برای نیازهای آینده بدون وجود هدف فعلی مشخص اشاره کرد که نقض مستقیم اصل محدودیت هدف است. همچنین درخواست فیلدهای اجباری غیرضروری در فرم‌های ثبت‌نام و فعال‌کردن پیش‌فرض همه مجوزها در اپلیکیشن‌های موبایل (مانند دسترسی به میکروفون، مخاطبان و گالری) بدون آنکه کاربر آگاهانه و آزادانه رضایت داده باشد، از دیگر مصادیق این تخلف به‌شمار می‌روند. افزون‌براین، ذخیره داده‌های حساس نظیر نژاد، باورهای مذهبی یا گرایش جنسی بدون وجود توجیه قانونی صریح و نیز نگهداری داده‌ها پس از پایان رابطه تجاری، برای مثال حفظ اطلاعات مشتریان قدیمی بدون هرگونه محدودیت زمانی، همگی در دسته جمع‌آوری و نگهداری بیش از حد داده طبقه‌بندی می‌شوند. این موارد نشان می‌دهد که اصل حداقل‌سازی داده نه‌تنها کمیت داده‌های جمع‌آوری‌شده، بلکه مدت و شرایط نگهداری آنها را نیز دربر می‌گیرد.

۲-۳. پردازش غیرمجاز داده‌های کاربران

این بخش، اولین و پایه‌ای‌ترین اصل در ماده ۵ قانون *GDPR* است. این اصل بر سه پایه استوار است که پیش‌تر به آنها اشاره شد. در صورت نقض این مواد از سوی یک سکو، وفق ماده ۸۳ قانون مذکور با حداکثر جریمه ۲۰ میلیون یورو یا ٤٪ از گردش مالی سالانه جهانی (هرکدام بیش‌تر باشد) مواجه خواهد شد.

۲-۴. تضییع حقوق کاربران پس از اخذ داده‌ها

کاربران پس از ارائه داده‌های خود دارای حقوقی خواهند بود که در بخش معرفی قانون *GDPR*به آنها اشاره شد و تضییع این حقوق در قانون مذکور با مجازات‌هایی همراه شده است. این مجازات‌ها شامل جریمه‌های مالی سنگین (وفق ماده ۸۳)، حق جبران خسارت برای کاربران (وفق ماده ۸۲) و برخی اقدامات اصلاحی و بازدارنده (وفق ماده ۵۸) است.

۲-۵. محتوای غیرقانونی

طبق ماده ۳ بند (*h*) قانون *DSA*، محتوای غیرقانونی به هرگونه اطلاعاتی اطلاق می‌شود که با قوانین اتحادیه اروپا یا قوانین هر یک از کشورهای عضو (که با قوانین اتحادیه اروپا مطابقت دارند) هماهنگ نباشد، صرف‌نظر از موضوع یا ماهیت دقیق آن قانون.

به‌عبارت‌دیگر *DSA* فهرستی از محتواهای ممنوعه ارائه نمی‌دهد بلکه چهارچوبی ارائه می‌کند که به کل نظام حقوقی اتحادیه اروپا و کشورهای عضو راجع است. این بدان‌معناست که قانون *DSA* محتوا را تنظیم یا تعریف نمی‌کند و مبنای قانونی مستقلی برای صدور دستور علیه محتوای غیرقانونی ایجاد نمی‌کند. درواقع، قانون حاکم در تعیین غیرقانونی بودن یک محتوا، قوانین ملی هر کشور عضو یا قوانین مستقیم اتحادیه اروپا است. به همین دلیل، مفهوم «محتوای غیرقانونی» بسیار گسترده است.

وفق «قانون سرویس‌های دیجیتال (*DSA*)» در ماده ۳ آمده: «محتوای غیرقانونی» به‌معنای هر اطلاعاتی است که خودش یا فعالیت مربوط به آن (ازجمله عرضه محصولات یا خدمات) بر اساس حقوق اتحادیه اروپا یا حقوق یکی از کشورهای عضو که قابل اعمال باشد، غیرقانونی است. در این قانون «محتوای غیرقانونی» شامل محتوایی است که طبق قوانین ملی کشورها (مثل قوانین مربوط به افترا، حریم خصوصی، ترغیب به خشونت و...) غیرقانونی باشد؛ بنابراین، برای‌مثال اگر افترا و نفرت‌پراکنی در قانون کشور آلمان جرم است، آن محتوا در آلمان «غیرقانونی» محسوب می‌شود و مشمول *DSA* می‌گردد و لازم است سازوکارهایی برای گزارش محتوای غیرقانونی در سکوها وجود داشته باشد. این قانون همچنین شفافیت در حذف محتوا را افزایش می‌دهد و تلاش دارد تا از بیان مجرمانه در مقابل انتقاد قانونی حفاظت نماید.

ماده ١٦ قانون مذکور، سکوها را موظف می‌کند تا سازوکاری ساده، قابل دسترس و کاربرپسند برای کاربران فراهم کنند تا بتوانند محتوای غیرقانونی را گزارش دهند. وقتی کاربری محتوایی را به عنوان «غیرقانونی» گزارش می‌دهد (مثلاً ادعا می‌کند یک پست افتراآمیز است)، سکو باید به‌سرعت، با دقت و بدون جانبداری آن را بررسی کرده و در صورت لزوم حذف یا دسترسی به آن را محدود کند.

از سوی‌دیگر وفق ماده ۱٤ قانون (*DSA*)، سکوها موظف به نظارت فعال و عمومی بر همه محتوای کاربران برای یافتن محتوای غیرقانونی نیستند. مسئولیت سکو پس از دریافت یک «اعلام » مشخص و معتبر آغاز می‌شود. این طراحی برای حفظ تعادل بین مبارزه با محتوای مضر و محافظت از آزادی بیان است.

هرچند قانون خدمات دیجیتال (*DSA*) فهرست بسته و محدودی از محتوای غیرقانونی ارائه نمی‌دهد؛ اما بر اساس قوانین ملی کشورهای عضو اتحادیه اروپا و قوانین مستقیم اتحادیه، می‌توان عمومی‌ترین مصادیق محتوای غیرقانونی را بدین شرح برشمرد: افترا که به آسیب‌زدن به آبرو و حیثیت افراد می‌انجامد، نفرت‌پراکنی که بر اساس آن احساسات خصمانه نسبت به گروه‌های نژادی، مذهبی یا قومی تحریک می‌شود، ترغیب به خشونت که شامل تشویق مستقیم یا غیرمستقیم به اعمال فیزیکی خشن می‌گردد، محتوای تروریستی که سازمان‌ها یا اقدامات تروریستی را تبلیغ یا تسهیل می‌کند، سوءاستفاده از کودکان و یا محتوای مضر برای ایشان که طیف گسترده‌ای از هرزه‌نگاری کودکان تا بهره‌کشی جنسی و نقض حریم خصوصی آنان را دربر می‌گیرد و درنهایت تبعیض نژادی و تحریک به آن که مبتنی بر برتری یا تنفر نژادی شکل می‌گیرد. در ادامه این بخش، هر یک از این مصادیق به‌صورت جداگانه و با جزئیات بیش‌تر مورد بررسی و تحلیل قرار خواهد گرفت.

۲-۵-۱. افترا

هرگونه بیانِ آسیب‌رسان به آبروی فرد دیگر، افترا محسوب می‌شود که به دو شکل افترای نوشتاری و افترای گفتاری ظاهر می‌گردد.

- افترای نوشتاری: شامل استفاده از ابزارهایی چون چاپ، نوشته، تصویر، نماد، طرح یا هر وسیله ارتباطی فیزیکی دیگر است که به آسیب زدن به اعتبار یا قراردادن فرد، کسب‌وکار یا حرفه او در معرض تنفر عمومی بینجامد.
- افترای گفتاری: بیانی است که معمولاً به شکل شفاهی منتشر می‌شود و شخص دیگری را هدف قرار می‌دهد. برخلاف افترای نوشتاری، برای اثبات افترای گفتاری نیاز به شکایت شاکی و ارائه مدرک است و به‌صورت فرضی قابل اثبات نیست *(Legal Information Institute)*.

افترای اینترنتی به رفتارهایی اشاره دارد که در آن افراد از طریق شبکه‌های رایانه‌ای، تلفن همراه یا سایر رسانه‌های نوین، اطلاعات نادرست و آسیب‌زننده به شهرت دیگران را منتشر می‌کنند. در مقایسه با افترای سنتی، افترای اینترنتی با ویژگی‌هایی همچون پنهان‌ماندن هویت، سرعت گسترش بالا، جلب توجه گسترده و هزینه قانونی پایین شناخته می‌شود. این ویژگی‌ها ارتکاب چنین جرایمی را آسان‌تر کرده و از سوی‌دیگر، پیگرد و ریشه‌کنی آن را دشوار می‌سازد. قوانین جزایی همواره در تلاش بوده‌اند تا از آزادی بیان شهروندان محافظت کنند، اما از سوی‌دیگر، این آزادی ممکن است منجر به آسیب دیدن آبرو و اعتبار دیگران شود. برقراری تعادل بین این دو حق، نیازمند وضع قوانین دقیق و موشکافانه در این حوزه است *(Xiaobing, 2018)*.

۲-۵-۲. نفرت‌پراکنی

در مورد نفرت‌پراکنی، بند ۲ ماده ۲۰ میثاق بین‌المللی حقوق مدنی و سیاسی *(ICCPR)* تصریح می‌کند: «هرگونه تبلیغ یا ترغیب به تنفر قومی، نژادی یا مذهبی که محرک تبعیض، دشمنی یا خشونت باشد، توسط قانون ممنوع است. واژه‌های «نفرت» و «دشمنی» به احساسات شدید، غیرمنطقی، ظالمانه و خصمانه نسبت به یک گروه هدف اشاره دارند. «ترویج» به‌معنای تشویق آشکار به تنفر علیه گروه هدف است و «تحریک» شامل اظهارنظرهایی درباره گروه‌های ملی، نژادی یا مذهبی می‌شود که خطر وقوع قریب‌به‌یقین تبعیض، خصومت یا خشونت علیه اعضای آن گروه‌ها را ایجاد می‌کند. ماده ۲۰ (*ICCPR*) یک آستانه بالا می‌طلبد که به‌راحتی محقق نشود چرا که اصل آزادی بیان باید همچنان باقی باشد و مخدوش نشود. در قانون اقدام رابات برای شش بخش زیر آزمون آستانه پیشنهاد می‌کند که برای اینکه یک مقوله مجرمانه تلقی شود ضروری است تحقق یابد:

۱- زمینه: در خصوص ارزیابی اینکه یک اظهارنظر آیا به تبعیض، خصومت یا جنایت نسبت به یک گروه هدف منجر می‌شود، بررسی زمینه بسیار اهمیت دارد و مستقیماً روی قصد و یا چرایی مؤثر است. تحلیل زمینه باید سخنان را در بافت اجتماعی و سیاسی خود قراردهد.

۲- گوینده: وضعیت یا حالت گوینده در جامعه باید مستقیماً به فرد یا سازمان در زمینه

مخاطب سخنان راجع باشد.

۳- قصد: برای اینکه موضوعی ذیل ماده ۲۰ (*ICCPR*) قرار گیرد بررسی قصد بسیار اهمیت دارد. اظهارات از روی غفلت یا بی‌تدبیری برای اینکه ذیل ماده ۲۰ قرار گیرد کافی نیست. برای این‌منظور لازم است یک رابطه مثلثی میان گوینده، موضوع سخن و مخاطب برقرار شود.

٤- محتوا و فرم: محتوای سخنان یکی از کانون‌های اصلی و عنصر اساسی تحریک است. تجزیه و تحلیل محتوا ممکن است شامل درجه‌ای باشد که سخنرانی تحریک‌آمیز و مستقیم بوده است. همچنین شکل، سبک و ماهیت استدلال‌ها در سخنرانی یا تعادل بین استدلال‌های به کار گرفته شده را نیز شامل می‌شود.

٥- وسعت اثر گفتار: گستره، شامل عناصری مانند دسترسی به سخنان، طبیعت عمومی آن، شدت و اندازه آن روی مخاطبان می‌باشد. سایر عناصر بدین شرح است: آیا سخنان عمومی بوده؟ چه ابزاری برای انتشار استفاده شده، برای مثال به‌وسیله یک جزوه انتشار انجام شده و یا با استفاده از برودکست و در رسانه اصلی یا اینترنت، تکرار آن، میزان آن چگونه بوده است؟ آیا در یک محیط محدود بوده و یا به‌صورت گسترده و برای عموم قابل دسترسی بوده است؟

٦- شرط احتمال وقوع و فوریت خطر: هر سخن تحریک‌آمیزی، صرفاً به دلیل محتوای آن، جرم محسوب نمی‌شود. برای اینکه چنین گفتاری قابل مجازات باشد، باید درجه‌ای از خطر واقعی آسیب در آن وجود داشته باشد. به عبارت دیگر، دادگاه‌ها بررسی می‌کنند که آیا احتمال منطقی وجود دارد که آن سخنان به اقدام عملی علیه گروه هدف بینجامد یا خیر؟ این رابطه علّی باید نسبتاً مستقیم و روشن باشد (*UNITED NATIONS HUMAN RIGHTS*).

۲-۵-۳. ترغیب به خشونت

خشونت شدیدترین شکل پرخاشگری است و می‌تواند به‌صورت تجاوز، زورگیری یا حتی قتل ظاهر شود. عوامل متعددی در بروز خشونت نقش دارند که ازجمله مهم‌ترین آنها می‌توان به احساس ناامیدی و سرخوردگی اشاره کرد که بستر روانی مناسبی برای بروز واکنش‌های خشن فراهم می‌آورد. همچنین مواجهه مکرر با محتوای خشونت‌آمیز در

رسانه‌ها و شبکه‌های اجتماعی، به‌تدریج حساسیت افراد را نسبت به خشونت کاهش داده و احتمال وقوع رفتارهای مشابه را افزایش می‌دهد. تجربه مستقیم خشونت در خانه یا محیط زندگی نیز یکی دیگر از عوامل مؤثر است؛ زیرا الگوهای رفتاری خشونت‌آمیز اغلب در محیط‌های آکنده از تنش و پرخاشگری بازتولید می‌شوند. افزون‌براین، تمایل به رفتار خصمانه با دیگران حتی در مواقعی که طرف مقابل هیچ رفتار خشونت‌آمیزی نشان نمی‌دهد، نشانگر وجود نوعی پرخاشگری زمینه‌ای و شخصیتی است که می‌تواند در فضای برخط و به‌ویژه در شبکه‌های اجتماعی، به شکل تهدید، فحاشی یا ترغیب دیگران به خشونت بروز پیدا کند. این عوامل در کنار یکدیگر، ضرورت تنظیم‌گری محتوای خشونت‌آمیز و ترغیب به خشونت در رسانه‌های اجتماعی را بیش از پیش آشکار می‌سازند. برخی شرایط خاص، خطر خشونت افراطی را افزایش می‌دهد مانند نوشیدن الکل، توهین و سایر تحریکات و عوامل محیطی اعم از گرما، ازدحام بیش از حد و ... (*American Psychological Association*).

۲-۵-۴. محتوای تروریستی

طبق شرایط استفاده و مقررات تمامی رسانه‌های اجتماعی اصلی، انتشار محتوای تروریستی به‌صراحت ممنوع اعلام شده است؛ برای‌مثال فیس‌بوک در استانداردهای خود تصریح کرده که سازمان‌های درگیر در فعالیت‌های تروریستی مجاز به ایجاد صفحه یا فعالیت در این سکو نیستند. همچنین استفاده از فیس‌بوک برای تسهیل یا سازماندهی اقدامات مجرمانه که منجر به آسیب فیزیکی یا مالی به افراد یا کسب‌وکارها شود نیز ممنوع است. همین قاعده در مورد تهدید به آسیب فیزیکی یا تشویق مجرمان محکوم‌شده نیز اعمال می‌شود. توییتر استفاده از خدمات خود را برای هرگونه مقاصد غیرقانونی ممنوع کرده است. این ممنوعیت شامل تهدید، تبلیغ تروریسم و همچنین عضویت یا حمایت از سازمان‌های تروریستی که مرتکب جنایت علیه شهروندان می‌شوند نیز می‌گردد.

یوتیوب در راهنمای کاربری خود تأکید کرده که سازمان‌های تروریستی به‌هیچ‌عنوان مجاز به استفاده از این سکو نیستند، چه برای جذب نیرو، چه برای انتشار محتوای مرتبط با تروریسم. این محدودیت شامل محتوایی که اقدامات تروریستی را تبلیغ می‌کند، جنایت را

تشویق می‌نماید یا حملات تروریستی را ستایش می‌کند نیز می‌شود (*Macdonald, 2019, p.183*).

۲-۵-۵. سوءاستفاده از کودکان و یا محتوای مضر برای ایشان

با افزایش حضور کودکان در فضای برخط، اینترنت بیش از هر رسانه دیگری برای اجتماعی شدن و برقراری ارتباط مورد استفاده آنان قرار گرفته است. نداشتن تجربه و آگاهی کافی درباره فناوری‌های نوین اطلاعاتی و ارتباطی، سوءاستفاده از کودکان در فضای مجازی را به یک نگرانی مشترک در سطح جهانی تبدیل کرده است. اشکال مختلف این سوءاستفاده، ضرورت پیشگیری از آن و نیز ترس کودکان از افشای موارد آزار برخط، از جمله مسائل مهمی هستند که نیازمند اقدامات پیشگیرانه جدی می‌باشند *(حسینی اکبرنژاد، ۱۳۹۹)*.

برخی از مهم‌ترین مخاطراتی که کودکان و نوجوانان را در فضای مجازی تهدید می‌کنند، عبارت‌اند از:

۱- سوءاستفاده جنسی مستقیم برخط از کودکان

در این حالت، کودک مجبور یا ترغیب می‌شود تا اقداماتی مانند ارسال عکس‌های برهنه یا جنسی از خود، برقراری ارتباط دیداری یا شنیداری جنسی از طریق وب‌کم یا تلفن همراه، گفت‌وگوی جنسی از طریق پیام‌رسان و موارد مشابه را انجام دهد.

۲- سوءاستفاده جنسی غیرمستقیم برخط از کودک

گاهی کودک به شکل غیرمستقیم مورد بهره‌برداری جنسی قرار می‌گیرد؛ مثلا فیلم یا تصاویر او با اهداف جنسی در فضای اینترنت منتشر می‌شود. این پدیده که امروزه با عنوان هرزه‌نگاری کودکان شناخته می‌شود، یکی از جدی‌ترین اشکال استثمار جنسی کودکان در فضای مجازی است. طبق بند ج ماده ۲ دستورالعمل توافق‌نامه حقوق کودک، هرزه‌نگاری کودکان به‌معنای هرگونه نمایش با هر وسیله‌ای است که کودک در آن به‌منظور بهره‌برداری جنسی به‌کار گرفته شود یا اندام تناسلی وی برای اهداف جنسی به نمایش گذاشته شود.

۳- بهره‌کشی تجاری و تبلیغاتی در فضای مجازی

ماده ۳۲ توافق‌نامه حقوق کودک، حق کودک برای محافظت در برابر استثمار اقتصادی و انجام کارهای زیان‌بار را به رسمیت می‌شناسد. پرسش اینجاست که آیا استخدام کودکان

در تبلیغات برخط به سلامت، آموزش یا رشد اخلاقی و اجتماعی آنان لطمه می‌زند؟ نکته مهم این است که ممنوعیت کار کودک تنها به‌دلیل آسیب‌های جسمی نیست بلکه بیش‌تر به‌خاطر سلب حقوق اولیه کودکی مانند بازی، آموزش و رشد سالم است. امروزه «کار کودک» تنها به اشتغال در کارخانه‌ها محدود نمی‌شود بلکه هر فعالیتی که از نظر روانی، جسمی یا اجتماعی برای کودک خطرناک باشد یا مانع تحصیل او شود، شامل این تعریف می‌گردد.

۴- نقض حریم خصوصی کودک در فضای مجازی

در برخی شبکه‌های اجتماعی، با انتشار عکس و فیلم‌های شخصی از زندگی کودک، صفحه‌هایی ایجاد می‌شوند که دنبال‌کنندگان زیادی جذب می‌کنند. با افزایش مخاطبان، شرکت‌های تجاری برای تبلیغات به‌سراغ این صفحات می‌روند. حتی اگر درآمدی در کار نباشد، انتشار این تصاویر ـ در مواردی که مغایر با مصالح عالیه کودک باشد ـ نقض حریم خصوصی او محسوب می‌شود.

۵- سوءاستفاده برخط و گردشگری جنسی کودک

این پدیده زمانی رخ می‌دهد که گردشگران از کشورهای توسعه‌یافته به کشورهای درحال‌توسعه سفر می‌کنند تا با کودکان بهره‌کشی جنسی کنند. امروزه اینترنت به ابزاری برای تسهیل گردشگری جنسی کودک تبدیل شده و متقاضیان از طریق فضای مجازی قربانیان خود را شناسایی و جذب می‌کنند. از دیگر پیامدهای سوءاستفاده برخط از کودکان می‌توان به قاچاق انسان، قاچاق اعضای بدن و جرائم مرتبط با مواد مخدر اشاره کرد که در آن‌ها کودکان اغلب به‌عنوان قربانیان اصلی مورد استفاده قرار می‌گیرند *(حسینی اکبرنژاد، ۱۳۹۹)*.

بر اساس دستورالعمل اتحادیه اروپا در مورد مبارزه با سوءاستفاده جنسی و استثمار جنسی کودکان و هرزه‌نگاری، کشورهای عضو موظفند مجموعه مشخصی از جرائم را در قوانین ملی خود بگنجانند. این جرائم شامل تولید، توزیع، انتشار و در دسترس قرار دادن محتوای سوءاستفاده جنسی از کودکان می‌شود که بارزترین مصداق آن هرزه‌نگاری کودکان است. همچنین تحریک یا فریب کودک برای انجام فعالیت جنسی، چه به‌صورت برخط و چه غیربرخط، و نیز آماده‌سازی کودک برای سوءاستفاده از طریق فضای مجازی، از دیگر مواردی هستند که باید جرم‌انگاری شوند. افزون‌براین، حتی تماشای صرف

محتوای سوءاستفاده جنسی از کودکان نیز در این دستورالعمل جرم تلقی شده است. دستورالعمل مذکور به‌طور صریح اعلام می‌دارد که انتشار هرگونه از این محتواها در شبکه‌های اجتماعی، صرف‌نظر از اینکه توسط کاربر عادی یا سکو منتشر شود، جرم محسوب می‌گردد و کشورهای عضو را ملزم به وضع مجازات‌های مؤثر، متناسب و بازدارنده برای این جرائم می‌کند.

در حوزه شبکه‌های اجتماعی، قانون خدمات دیجیتال (*DSA*)، مسئولیت را متوجه سکوهای شبکه اجتماعی می‌داند تا از انتشار و گسترش این محتوای از پیش جرم‌انگاری شده جلوگیری کنند. وفق ماده ۳، محتوای سوءاستفاده جنسی از کودکان، مصداق بارز «محتوای غیرقانونی» است. همچنین در ماده ١٦ (سازوکار اعلام و اقدام) مقرر داشته، سکوها باید امکان گزارش آسان این محتوا را فراهم کرده و به‌سرعت آن را حذف کنند. در ماده ۱۸ (تعهدات سکوهای بسیار بزرگ) نیز تصریح شده است، سکوهایی مانند اینستاگرام، تیک‌تاک یا اسنپ‌چت باید اقدامات فنی و سازمانی مناسب برای حذف و پیشگیری از دسترسی به محتوای سوءاستفاده جنسی از کودکان انجام دهند و نیز از نرم‌افزارها و شاخص‌های شناسایی برای کشف خودکار این محتوا استفاده کنند.

در مواد ٣٤ و ٣٥ قانون مذکور (ارزیابی و کاهش ریسک نظام‌مند) سکوهای بسیار بزرگ باید ریسک‌های مربوط به نقض حقوق کودک (ازجمله قرار گرفتن در معرض محتوای مضر) را ارزیابی و کاهش دهند و درنهایت در ماده ٤٨ (دستورالعمل‌های بحران) تأکید شده، در صورت افزایش ناگهانی تهدیدات علیه کودکان، کمیسیون اروپا می‌تواند اقدامات اضطراری فوری را الزامی کند.

این مهم در قانون عمومی حفاظت از داده‌ها (*GDPR*) نیز تأکید شده است. قانون مذکور از کودکان به‌عنوان اشخاص آسیب‌پذیر با حمایت ویژه یاد می‌کند. در ماده ۸ قانون شرایط سخت‌تری برای استفاده از خدمات جامعه شبکه اجتماعی تعیین شده است. همچنین در ماده ۲۵ (حریم خصوصی از طریق طراحی)، سکوها باید تنظیمات پیش‌فرضی را اعمال کنند که حریم خصوصی و امنیت کودکان را به حداکثر برساند (مثلاً رخ‌نماهای خصوصی پیش‌فرض).

۲-۵-۶. تبعیض نژادی و تحریک به آن

در توافق‌نامه بین‌المللی رفع کلیه اشکال تبعیض نژادی، تبعیض نژادی چنین تعریف شده است: «هرگونه تمایز، محرومیت، محدودیت یا اولویت‌گذاری مبتنی بر نژاد، رنگ، نسب یا اصل و نسب ملی یا قومی که هدف یا اثر آن، بی‌اعتبارسازی یا نقض شناسایی، بهره‌مندی یا اعمال برابر حقوق بشر و آزادی‌های اساسی در عرصه‌های سیاسی، اقتصادی، اجتماعی، فرهنگی یا هر حوزه دیگری از حیات عمومی باشد. در ماده ٤ همین توافق‌نامه، از دولت‌ها خواسته شده است که کلیه اشکال اشاعۀ افکار مبتنی بر برتری یا تنفّر نژادی و نیز هرگونه تحریک به تبعیض نژادی را جرم‌انگاری کنند. ازآنجاکه جرم‌انگاری این موارد، محدودیتی جدی بر آزادی بیان محسوب می‌شود، دولت‌ها هنگام تصویب، نگرانی خود را مبنی بر نقض احتمالی آزادی بیان ناشی از الزام مذکور ابراز داشتند. به همین‌جهت، به‌منظور پاسداری از حقوق و آزادی‌ها، در بند مقدماتی ماده ٤ تصریح شده که اجرای تعهدات ناظر بر این ماده، باید توأم با رعایت ملاحظات حقوق بشری نظیر آزادی بیان صورت پذیرد *(انصاری و امامی‌الطرقی، ۱۳۹۹)*.

چهار مؤلفه در خصوص این مقوله بیان شده است: اشاعۀ افکار مبتنی بر برتری یا تنفر نژادی، تحریک مستقیم به تبعیض نژادی، اعمال خشونت‌آمیز یا تحریک به آن بر اساس نژاد و تأمین مالی فعالیت‌های نژادپرستانه.

۲-۶. روش‌های تبلیغاتی گمراه‌کننده و عدم شفافیت در کارزارهای انتخاباتی

کسب‌وکارها اجازه ندارند با ارائه اطلاعات نادرست یا نامعتبر، تصویر یا برداشت گمراه‌کننده‌ای از محصولات یا خدمات خود ایجاد کنند. این قاعده در مورد تمامی تبلیغات، طراحی بسته‌بندی و هرگونه محتوایی که در رسانه‌های سنتی یا فضای برخط (مانند تارنما یا صفحات شبکه‌های اجتماعی) منتشر می‌شود، اعمال می‌گردد. به‌طورمثال، رسانه‌ها مجاز نیستند در مورد کیفیت، طرح، مدل یا پیشینه یک محصول یا خدمت ادعاهای کذب مطرح کنند. همچنین اظهارات نادرست درباره نو بودن کالاها، تأییدیه‌های دروغین، ویژگی‌های عملکردی غیرواقعی، لوازم جانبی یا مزایای ساختگی محصولات و خدمات از مصادیق دیگر این تخلف محسوب می‌شوند. افزون‌براین، ادعای نادرست درباره در دسترس بودن

خدمات پس از فروش یا قطعات یدکی، القای نیاز ساختگی مشتری به کالا یا خدمات خاص، و نیز مطرح کردن هرگونه حق انحصاری غیرواقعی روی کالا یا خدمات، همگی در زمره اقدامات گمراه‌کننده و غیرقانونی طبقه‌بندی می‌گردند. این قواعد با هدف حمایت از حقوق مصرف‌کنندگان و تضمین رقابت منصفانه در بازار طراحی شده‌اند و شامل تبلیغات در شبکه‌های اجتماعی نیز می‌شوند.

حتی اگر قصد فریب مشتری در کار نباشد، اگر تأثیر کلی تبلیغات یک کسب‌وکار باعث گمراهی مشتری شود، مثلاً در مورد قیمت، ارزش یا کیفیت کالا یا خدمات، این اقدام نقض قانون محسوب می‌شود.

تنها یک استثنا در این قانون وجود دارد. گاهی کسب‌وکارها ممکن است ادعاهای اغراق‌آمیزی مطرح کنند که به‌وضوح برای عموم غیرواقعی و اغراق‌شده به‌نظر می‌رسد و هیچ مصرف‌کننده معقولی آن را باور نمی‌کند؛ برای‌مثال، اگر رستورانی ادعا کند بهترین استیک روی کره زمین را ارائه می‌دهد. این نوع ادعاها تحت عنوان «تبلیغات پرطمطراق» شناخته می‌شوند و در دسته تبلیغات گمراه‌کننده قرار نمی‌گیرند (*AUSTRALIAN COMPETITION & CONSUMER COMMISSION*).

در اتحادیه اروپا قانون سرویس‌های دیجیتال (*DSA*) بار مسئولیت سنگینی بر دوش سکوها (شبکه‌های اجتماعی) می‌گذارد تا محیطی شفاف‌تر و امن‌تر ایجاد کنند و تبلیغات گمراه‌کننده را مهار کنند.

در ماده ۲۶ این قانون (*DSA*) که در خصوص شفافیت در تبلیغات است، سکوها باید به کاربران به‌روشنی و در لحظه نشان دهند که با یک آگهی تجاری مواجه هستند. همچنین باید مشخص کنند چه کسی هزینه آن تبلیغ را پرداخت کرده و چه معیارهای اصلی برای هدف‌گیری کاربر استفاده شده است. این شفافیت، خود مانعی در برابر فریب است.

همچنین در ماده ۳۰ قانون (*DSA*) هدف‌گیری تبلیغاتی بر اساس داده‌های حساس (مانند قومیت، عقاید سیاسی، جهت‌گیری جنسی، وضعیت سلامتی) به‌طور کلی ممنوع است. این نوع هدف‌گیری اغلب برای تبلیغات بسیار گمراه‌کننده یا استثماری استفاده می‌شود.

در ماده ۳۴ و ۳۵ قانون (*DSA*) سکوهای بسیار بزرگ (مانند فیسبوک، اینستاگرام،

تیک‌تاک، ایکس) موظفند به‌طور منظم ریسک‌های نظام‌مند خود ازجمله پخش محتوای غیرقانونی (مانند تبلیغات کلاهبرداری طبق قوانین ملی) و تأثیرات منفی بر حقوق مصرف‌کننده را ارزیابی و کاهش دهند.

درنهایت ماده ٣٦ قانون (*DSA*) مقرر داشته، سکوها باید سازوکاری برای گزارش محتوای غیرقانونی (ازجمله تبلیغات گمراه‌کننده) توسط کاربران ایجاد کنند. لازم به ذکر است قانون جرائمی هم برای عدم رعایت موارد موضوعه تعریف کرده که می‌تواند به جریمه‌هایی تا ٦ درصد از گردش مالی جهانی سکو مذکور را شامل شود.

۲-۷. انحصار

در اروپا «قانون بازارهای دیجیتال» (*DMA*) مستقیماً به مقابله با انحصار و رفتارهای ضدرقابتی سکوهای بسیار قدرتمند (دروازه‌بانان) می‌پردازد. هدف این قانون ایجاد بازارهای دیجیتال رقابتی‌تر و منصفانه‌تر با محدود کردن قدرت انحصاری شرکت‌های بزرگ فناوری است. چگونگی مقابله‌ی این قانون (*DMA*) با انحصار در شبکه‌های اجتماعی بدین‌شرح است:

۱. شناسایی دروازه‌بانان: *DMA* ابتدا با مجموعه‌ای معیارها که قبلاً ذکر شد، شرکت‌هایی که دارای موقعیت انحصاری و پایدار هستند را به‌عنوان «دروازه‌بان» تعیین می‌کند.

۲. الزام فهرستی از نبایدها و بایدها (ممنوعیت‌ها و تعهدات) برای دروازه‌بانان: برخی اقدامات که از پیامدهای مستقیم ضدانحصاری برخوردارند به دروازه‌بانان دیکته می‌شود. ازجمله آنها می‌توان به موارد زیر اشاره کرد:

قانون بازارهای دیجیتال (*DMA*) برای مقابله با رفتارهای انحصاری دروازه‌بانان، مجموعه‌ای از بایدها و نبایدها را تعیین کرده است. ازجمله مهم‌ترین ممنوعیت‌ها می‌توان به «ممنوعیت ترجیح‌دهی خود» اشاره کرد که بر اساس آن شبکه اجتماعی نمی‌تواند خدمات و محصولات خود را در نتایج جستجو یا رتبه‌بندی، بالاتر از خدمات رقبا قرار دهد (ماده ٦). همچنین «ممنوعیت قفل کردن کاربران» ایجاب می‌کند که کاربران بتوانند به‌راحتی اپلیکیشن‌های پیش‌فرض شده شبکه اجتماعی را حذف کنند (ماده ٦). در سوی‌دیگر، «الزام به تعامل‌پذیری» قرار دارد که به شبکه‌های اجتماعی کوچک‌تر اجازه می‌دهد درخواست تعامل با شبکه‌های

اجتماعی بزرگ (دروازه‌بان) را مطرح کنند. برای‌مثال کاربر یک شبکه کوچک باید بتواند با کاربر فیسبوک پیام رد و بدل کند (ماده ۷). «ممنوعیت ترکیب داده‌ها» نیز تصریح می‌کند که شبکه اجتماعی نمی‌تواند داده‌های کاربران را از خدمات مختلف خود (مانند فیسبوک، اینستاگرام و واتس‌اپ) بدون رضایت صریح کاربر ترکیب کرده و از این طریق انحصار اطلاعاتی ایجاد نماید (ماده ۵). افزون‌براین، «دسترسی منصفانه به داده‌ها برای کسب‌وکارها» تضمین شده است. بدین‌معنا که کسب‌وکارهای فعال روی سکو باید به داده‌های تولیدشده توسط فعالیت خودشان دسترسی داشته باشند (ماده ٦). درنهایت، «ممنوعیت محدود کردن کاربران در یافتن پیشنهادات بهتر» حکم می‌کند که شبکه اجتماعی نتواند مانع شود کاربران، قراردادها را خارج از سکو منعقد کنند یا از سرویس‌های دیگر استفاده نمایند (ماده ۵). این شش الزام در کنار یکدیگر، چهارچوبی جامع برای مهار انحصار، تضمین رقابت منصفانه و افزایش انتخاب کاربران در بازار دیجیتال اروپا فراهم می‌آورند.

۳. تعیین جرائم: درنهایت در قانون مذکور مجازات‌های بسیار سنگینی از قبیل جریمه‌های تا ۱۰ درصد از گردش مالی جهانی شرکت برای نقض قوانین و جریمه‌های دوره‌ای تا ۵ درصد از گردش مالی روزانه جهانی برای عدم تبعیت از موارد موضوعه و در صورت تکرار تخلفات، اصلاح ساختاری کسب‌وکار (مانند تفکیک بخش‌ها) تعیین شده است.

بررسی انجام‌شده در این بخش نشان داد که ضرورت‌های عینی تنظیم‌گری رسانه‌های اجتماعی در اتحادیه اروپا طیف گسترده‌ای از کژکارکردها را دربر می‌گیرد. از قصور در حفاظت از داده‌ها و حملات سایبری گرفته تا جمع‌آوری بیش از حد اطلاعات، پردازش غیرمجاز، تضییع حقوق کاربران، محتوای غیرقانونی (شامل افترا، نفرت‌پراکنی، ترغیب به خشونت، محتوای تروریستی، سوءاستفاده از کودکان و تبعیض نژادی)، تبلیغات گمراه‌کننده در کارزارهای انتخاباتی و درنهایت رفتارهای انحصارطلبانه. آنچه در این میان مشهود است، اتکای هر یک از این حوزه‌های تنظیم‌گری به قوانین مشخصی نظیر *GDPR*، *DSA* و *DMA* است که جرایم متناسب و سازوکارهای اجرایی خاصی را پیش‌بینی کرده‌اند.

در بخش پایانی پژوهش، ضمن جمع‌بندی یافته‌های حاصل از بررسی قوانین و کژکارکردها، به این پرسش اساسی که مهم‌ترین محورهای سیاستی حاکم بر تنظیم‌گری

رسانه‌های اجتماعی در اروپا کدام‌اند و آینده این نظام حقوقی با چه روندهایی روبه‌رو خواهد بود؟ پاسخ داده خواهد شد.

نتیجه‌گیری

شبکه‌های اجتماعی علی‌رغم مزایای فراوان، با کژکارکردهای متعدد و جدی‌ای مواجه شده‌اند که پاسخ تنظیمی قاطع و چندلایه‌ای را طلب می‌کنند. دولت‌ها از موضع بی‌طرفی خارج شده و با اتکا به اصولی مانند حمایت از حقوق بنیادین کاربران، حفظ امنیت ملی و تضمین رقابت منصفانه، وارد عرصه تنظیم‌گری شده‌اند. تنظیم‌گری رسانه‌های اجتماعی در اتحادیه اروپا مبتنی بر چهارچوبی چندلایه و پیچیده است که از ترکیب قوانین فراگیر در سطح اتحادیه و قوانین تکمیلی در سطح کشورهای عضو شکل گرفته است. مهم‌ترین ویژگی این نظام حقوقی، رویکرد «هماهنگ‌سازی حداقلی» است. بدین‌معنا که اتحادیه اروپا چهارچوب کلی و اصول اساسی را تعیین می‌کند؛ اما تشخیص و جرم‌انگاری مصادیق عینی محتوای غیرقانونی را به قوانین داخلی کشورهای عضو احاله می‌نماید. این رویکرد زمینه‌ساز شکل‌گیری تنوع قابل‌توجهی در رویه‌های قانونی کشورهای مختلف شده است. روند قانون‌گذاری از مقابله با واضح‌ترین آسیب‌ها (مانند افترا و محتوای مجرمانه) آغاز شده و به‌تدریج با پیچیده‌تر شدن اکوسیستم دیجیتال، حوزه‌های ظریف‌تری مانند شفافیت الگوریتمی، مدیریت داده‌های شخصی، انحصارزدایی و محافظت از گروه‌های آسیب‌پذیر (به‌ویژه کودکان) را دربر گرفته است. قوانینی مانند «مقررات عمومی حفاظت از داده» (*GDPR*) و «قانون خدمات دیجیتال» (*DSA*) در اروپا، نشان‌دهنده گذار از یک رویکرد واکنشی به یک چهارچوب حکمرانی پیش‌دستانه، نظام‌مند و مسئولیت‌آفرین برای سکوها هستند. محورهای کلان قوانین ناظر به تنظیم‌گری شبکه‌های اجتماعی در اتحادیه‌ی اروپا را می‌توان موارد زیر دانست:

۱. حمایت از شخصیت و امنیت کاربران: ممنوعیت و مقابله با محتوای مجرمانه (افترا، نفرت‌پراکنی، خشونت، تروریسم) از طریق سازوکارهای «اعلام و اقدام» و الزام سکوها به پاسخگویی.

۲. صیانت از حریم خصوصی و داده‌ها: تأکید بر اصولی چون حداقل‌سازی داده، پردازش قانونمند و شفاف، امنیت داده‌ها در برابر حملات سایبری، و اعطای حقوق گسترده به کاربران (دسترسی، اصلاح، حذف) تحت قانون (*GDPR*).
۳. شفافیت و سلامت فضای عمومی: مقابله با تبلیغات گمراه‌کننده، شفاف‌سازی در تبلیغات سیاسی و کارزارهای انتخاباتی، و افشای عملکرد الگوریتم‌های پیشنهاددهنده محتوا.
٤. رقابت و انحصارزدایی: هدف قرار دادن موقعیت مسلط «دروازه‌بانان» دیجیتال (طبق *DMA*) با ممنوعیت رفتارهای انحصاری مانند ترجیح خدمات خود، قفل کردن کاربران و ممانعت از تعامل‌پذیری.
٥. حفاظت ویژه از کودکان: جرم‌انگاری شدید تولید و توزیع محتوای سوءاستفاده جنسی از کودکان و تکلیف سکوها به پیشگیری فعال و حذف فوری چنین محتوایی.

یکی از مهم‌ترین چالش‌های فراروی تنظیم‌گری رسانه‌های اجتماعی، ایجاد تعادل میان ضرورت مقابله با محتوای غیرقانونی و حفظ حقوق بنیادین کاربران از جمله آزادی بیان و حریم خصوصی است. قوانین اتحادیه اروپا با اتخاذ رویکردی مبتنی بر ریسک و تأکید بر شفافیت و مسئولیت‌پذیری سکوها، در تلاش برای تحقق این تعادل هستند. در این‌راستا، الزام سکوها به ایجاد سازوکارهای گزارش‌دهی آسان برای کاربران، ارائه دلایل روشن در خصوص حذف محتوا و امکان اعتراض به تصمیمات سکو ازجمله راهکارهای پیش‌بینی شده می‌باشند.

حفاظت از داده‌های شخصی و حریم خصوصی کاربران به‌عنوان یکی دیگر از ارکان اساسی نظام تنظیم‌گری اروپا، بر پایه اصول قانونمندی، انصاف، شفافیت، محدودیت هدف، حداقل‌سازی داده و مسئولیت‌پذیری استوار است. همچنین مقابله با کژکارکردهایی نظیر نفرت‌پراکنی، تبعیض نژادی، افترا، ترغیب به خشونت، محتوای تروریستی، سوءاستفاده از کودکان، تبلیغات گمراه‌کننده و رفتارهای انحصارطلبانه از اولویت‌های اصلی تنظیم‌گری محسوب می‌شود.

تجربه اتحادیه اروپا نشان می‌دهد که حکمرانی مؤثر بر شبکه‌های اجتماعی نیازمند قوانینی جامع، الزام‌آور و فراملی است که بتوانند از قدرت نامتقارن سکوهای بزرگ بکاهند

و حقوق کاربران را در اولویت قرار دهند. موفقیت این چهارچوب‌ها در گرو هماهنگی بین مقررات ملی و فراملی، تعیین جریمه‌های بازدارنده مالی، و ایجاد سازوکارهای نظارتی مستمر است. آینده حکمرانی فضای مجازی به سمت تنظیم‌گری هوشمندتر، مبتنی بر ارزیابی ریسک نظام‌مند و حفظ تعادل دشوار میان آزادی بیان، امنیت، رقابت و حقوق بنیادین کاربران پیش می‌رود.

منابع

انصاری، باقر (۱۳۸٦). *حقوق ارتباط جمعی*، تهران: سازمان مطالعه و تدوین کتب علوم انسانی دانشگاه‌ها (سمت)، مرکز تحقیق و توسعه علوم انسانی.

انصاری، باقر (۱۳۹۳). *حقوق رسانه*، تهران: سازمان مطالعه و تدوین کتب علوم انسانی دانشگاه‌ها (سمت)، مرکز تحقیق و توسعه علوم انسانی.

انصاری، باقر و امام‌الطرقی، مهلا (۱۳۹۹). آزادی بیان و تحریک به تبعیض نژادی، *فصلنامه تحقیقات حقوقی*، شماره ۹۱

انصاری، باقر (۱٤۰۱). مطالعه حقوقی تبعیض الگوریتمی، *فصلنامه دانش حقوق عمومی*، سال یازدهم، زمستان ۱٤۰۱، شماره ۳۸ ص. ۱٤۷ تا ۱۷۸.

American Psychological Association, Access by ttps://www.apa.org/topics/gun-violence-crime

Australian Competition and Consumer Commission (2021), Google's dominance in ad tech supply chain harms businesses and consumers, 28 September.

European Convention on Human Rights, November 4, 1950.

European Commission. (2018). *Code of Conduct on Disinformation*. Retrieved from https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation

Europian Commission, Data protection in the EU, Accessed by: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

European Parliament and Council of the European Union (2022), Digital Markets Act, Official Journal of the European Union, L 265, 1–66. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R1925

European Commission (2023), Digital Markets Act: Commission designates six gatekeepers, https://digital-markets-act.ec.europa.eu/gatekeepers-portal_en

European Parliament and Council of the European Union (2022), Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Acthttps://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2065

Legal Information Institute, Cornell Law School, Access by: https://www.law.cornell.edu/

Macdonald Stuart, Sara Giro Correia and Amy-Louise Watkin, regulating terrorist content on social media: automation and the rule of law, Published online by Cambridge University Press: 20 June 2019

Marsden Chris, Meyer Trisha, Brown Ian (2019), Platform values and democratic elections: How can the law regulate digital disinformation? Computer Law and Security Review: The International Journal of Technology Law and Practice

Publications Office of the European Union (2022), *General data protection regulation (GDPR)*, Retrieved from https://eur-lex.europa.eu/summary/EN/LEGISSUM:310401_2

Publications Office of the European Union. (2025). Rules for trustworthy artificial intelligence in the EU. EUR-Lex. Retrieved from https://eur-lex.europa.eu/summary/EN/4762484

UNITED NATIONS HUMAN RIGHTS, Office of the High commissioner, One-page on "incitement to hatred"

www.gdpr-info.eu

Xiaobing Li, Yongfeng Qin (2018), Research on Computer Network Defamation Crime in China, 8th International Congress of Information and Communication Technology (ICICT-2018), Procedia Computer Science 131 (2018) 1217–1222