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

Cope and Boundaries of Liability of Copyright Infringement for Content Hosting Platforms: A Comparative Study and Formulation of a National Framework

Ali Yousefi Gorji[1] 0000-0003-0917-9249
Mohsen Arab[2] 0009-0002-2211-6613
Abdollah Rajabi[3] 0009-0002-2211-6613

Abstract

Cyberspace has become an inseparable part of modern human life and is expanding at an astonishing pace with the rapid emergence of various types of online intermediaries. The presence of numerous advantages and disadvantages has necessitated precise and specialized legislation in this area. Developed countries have gained valuable experience in this domain, and utilizing their regulatory approaches can significantly accelerate the secure and sustainable development of this field in Iran by addressing similar challenges. The findings of this comparative legal study of Iran, the United States, and the European Union demonstrate that Iran's current legal framework is not capable of keeping pace with the evolving needs of cyberspace. Given the inefficiency of existing regulations, a comprehensive, prompt, and coherent revision is essential to simultaneously safeguard individual rights and support the growth of domestic content-hosting platforms. Ultimately, this research analyzes the current legal situation in Iran, outlines the desirable regulatory framework, and identifies existing legislative gaps. It also proposes the essential prerequisites and requirements for formulating a practical and enforceable legal structure aimed at implementing the «Safe Harbor» Doctrine within Iran's digital environment. This proposed legal framework may pave the way for positive developments in the fields of national technology governance and digital law.

Keywords: Content Hosting Platform, Criminal and Civil Liability of the Platform, «Safe Harbor» Doctrine, Media Law.

1- Energy and International Trade Law, Faculty of Law, Farabi Faculties, University of Tehran, Qom, Iran ali.yousefigorji@ut.ac.ir
2- International Commercial and Economic Law Department, Faculty of Law, Alborz Campus, University of Tehran, Tehran, Iran mohsen.arab@aut.ac.ir
3- Department of Private Law, University of Tehran, Farabi Faculties, Qom, Iran (corresponding author of the article) rajabya@ut.ac.ir

دوفصلنامه
مطالعات فقه و حقوق رسانه
دانشکده غیردولتی – غیرانتفاعی رفاه

دوره ۸، شماره ۲ (پیاپی ۱۶)
پاییز و زمستان ۱۴۰۵
صص: ۳۰۱-۳۳۰

حدود و ثغور مسئولیت سکو(پلتفرم)های میزبانی محتوا: مطالعه تطبیقی و ترسیم راهکار ملّی با تمرکز بر نقض مالکیت ادبی هنری

نوع مقاله: ترویجی
DOI: 10.22034/jlsm.2026.2075431.1065

تاریخ دریافت: ۱۴۰۴/۰۷/۳۰ **تاریخ بازنگری:** ۱۴۰۵/۰۲/۰۹ **تاریخ پذیرش:** ۱۴۰۵/۰۲/۱۳

علی یوسفی گرجی[۱] محسن عرب[۲] عبدالله رجبی[۳]

چکیده

فضای مجازی به جزئی لاینفک از زندگی بشر امروز تبدیل شده که با ظهور روزافزون انواع واسطه‌های اینترنتی درحال بسط و گسترش حیرت‌انگیز است که وجود مزایا و معایب متعدد، موجب لزوم قانونگذاری دقیق و تخصصی در این حوزه شده است. کشورهای توسعه‌یافته تجربیات ارزشمندی در این حوزه کسب نموده‌اند که بهره‌گیری از آنها می‌تواند با کمک به یافتن راه‌حل برای چالش‌های مشابه، توسعه پایدار و امن این حوزه در کشورمان را تسریع نماید. نتایج حاصل از بررسی تطبیقی قوانین ایران، ایالات متحده و اتحادیه اروپا در این پژوهش، حکایت از این مهم دارد که رویکرد قوانین ایران توانایی حرکت متناسب با نیازهای روز فضای مجازی را نداشته و با توجه به ناکارآمدی قوانین موجود در این زمینه، ضرورت بازنگری جامع، سریع و منسجم در آنها مشهود است تا حمایت همزمان از حقوق اشخاص و گسترش سکو(پلتفرم)های میزبانی محتوا محقق شود. درنهایت، این پژوهش ضمن بررسی وضعیت موجود حاکم بر قوانین ایران، وضعیت مطلوب را تحلیل می‌کند و با تبیین خلأهای موجود، الزامات و پیش‌شرط‌های لازم برای تدوین چهارچوبی قانونی و قابل اجرا جهت اعمال دکترین «بندر امن» در فضای دیجیتال ایران را ارائه می‌دهد که می‌تواند زمینه‌ساز تحولات مثبت در حوزه فناوری و حقوق فضای مجازی باشد.

واژگان کلیدی

سکو(پلتفرم) میزبانی محتوا، حقوق رسانه، دکترین «بندر امن»، مسئولیت کیفری و مدنی سکو(پلتفرم).

---

۱. دانشجوی کارشناسی ارشد حقوق انرژی و تجارت بین‌الملل، دانشکده حقوق، دانشکدگان فارابی دانشگاه تهران، قم، ایران ali.yousefigorji@ut.ac.ir

۲. دانشجوی کارشناسی ارشد حقوق تجاری اقتصادی بین‌الملل، دانشکده حقوق، پردیس البرز دانشگاه تهران، تهران، ایران mohsen.arab@aut.ac.ir

۳. استادیار حقوق خصوصی، دانشکدهٔ حقوق، دانشکدگان فارابی، دانشگاه تهران، قم، ایران (نویسنده مسئول) rajabya@ut.ac.ir

مقدمه

گستره نفوذ اینترنت در زندگی بشر به‌گونه‌ای افزایش یافته است که شورای حقوق بشر سازمان ملل متحد، ضمن محکوم کردن اختلال عمدی دولت‌ها در دسترسی به اینترنت، اعلام داشته کلیه حقوقی که افراد در فضای حقیقی از آن برخوردارند، در فضای مجازی نیز باید مورد حمایت قرار بگیرد *(Human Rights Council, 2016, p.3)*. براین‌اساس، حق دسترسی به اینترنت به‌عنوان یکی از حقوق بشر معاصر شناسایی و تبیین شده است.

برقراری ارتباط، انجام معاملات و تبادل اطلاعات در بستر اینترنت، از طریق واسطه‌های اینترنتی امکان‌پذیر می‌شود. این واسطه‌ها با ارائه زیرساخت‌ها و خدمات دیجیتال، به‌مثابه پلی میان عرضه‌کنندگان و دریافت‌کنندگان محتوا، کالا یا خدمات عمل می‌کنند. واسطه‌های اینترنتی طیف متنوعی از خدمات از جمله «فراهم‌کردن دسترسی به اینترنت، ارائه خدمات میزبانی، انتقال یا ذخیره‌سازی داده‌ها و ایجاد بستر تعامل میان کاربران» را ارائه می‌دهند (*Gellert & Wolter, 2021, p.9*).

در این‌میان، سکو(پلتفرم)های ارائه‌دهنده خدمات دسترسی و میزبانی، نقش اساسی در ارائه خدمات اینترنتی و انتشار و اشتراک‌گذاری محتوا ایفا می‌کنند. ارائه‌دهندگان خدمات دسترسی که از آنها به‌عنوان فراهم‌کنندگان خدمات اینترنتی نیز یاد می‌شود، امکان ورود کاربران به اینترنت را از طریق فناوری‌های مختلفی همانند کابل و فیبر نوری فراهم می‌سازند. درمقابل، ارائه‌دهندگان خدمات میزبانی با عرضه خدمات پایدار به منظور ذخیره‌سازی داده‌ها روی سرورها، امکان نمایش و دسترسی به انواع محتوا را مهیا می‌نمایند *(رمضانیان سیاهکلرودی و دیگران، ۱۳۹۹، صص. ۲۸۱-۲۸۲)*.

این سکوها موجب شکل‌گیری جهانی غیرملموس در موازات دنیای فیزیکی و واقعی شده‌اند و انسان معاصر با خلق زیستگاهی نوین، بخش قابل‌توجهی از فعالیت‌های روزمره خود را در این فضا انجام می‌دهد. بدیهی است که در صورت فقدان مقررات مناسب و عدم تعیین چهارچوب‌های حقوقی روشن برای آزادی‌ها و محدودیت‌ها، توسعه این سکوها نه‌تنها آثار مثبتی به همراه نخواهد داشت، بلکه می‌تواند منجر به بروز زیان‌های جدی نیز بشود. ازاین‌رو، تبیین و تدوین سازوکارهای اجرایی برای نظارت و راهبری این پدیده نوظهور امری

اجتناب‌ناپذیر است؛ به‌گونه‌ای‌که ضمن حمایت از نوآوری، نحوه مسئولیت‌پذیری در قبال اعمال و وقایع رخ‌داده در این فضا نیز به‌صورت منسجم و قانونی تنظیم گردد.

در ادبیات فنی، میزبانی به معنای تأمین فضای ذخیره‌سازی است که به اشخاص حقیقی و حقوقی این امکان را می‌دهد تا محتوای خود را برای مخاطبان عرضه کنند *(Batura, 2020, p.13)*. در همین راستا، ماده ١٤ دستورالعمل تجارت الکترونیک اتحادیه اروپا در مقام تعریف ارائه‌دهندگان خدمات میزبانی و همسو با تعریف فنی این واژه بیان می‌نماید که: «ارائه‌دهنده خدمات میزبانی، ارائه‌دهنده‌ای است که اطلاعات فراهم‌شده توسط کاربران را ذخیره می‌کند».

براساس این تعریف می‌توان گفت که میزبانی به حالتی اطلاق می‌شود که سکو صرفاً زیرساخت فنی لازم برای ذخیره و نمایش محتوای کاربران را فراهم می‌کند، بدون آنکه در تولید یا گزینش محتوا مداخله کند. درحقیقت، نقش منفعلانه سکو موجب برخورداری از مصوّنیت است. درمقابل، هنگامی‌که سکو در ساماندهی، ترویج یا پالایش محتوا مداخلهٔ موثر داشته باشد، فعالیت آن از حالت میزبانی خارج شده و ماهیت انتشاری پیدا می‌کند؛ بنابراین معیار تفکیک میان این دو، حدّ مداخله و کنترل سکو بر محتوای کاربران است.

مسئولیت سکوهای میزبانی محتوا در ادبیات حقوقی بین‌المللی، متأثر از پیشرفت‌های فناورانه، دستخوش تحولات و فراز و نشیب‌های متعددی بوده است. پژوهش‌های انجام‌شده در این حوزه، درنهایت به شکل‌گیری دکترین «بندر امن» انجامیده است که براساس آن، سکوها در صورت عدم علم به نقض، عدم انتفاع مالی مستقیم و اقدام سریع جهت حذف محتوا، از مسئولیت‌های مدنی و کیفری مصون می‌مانند. در رویهٔ قضائی ایالات متحده، پرونده‌هایی همچون ویاکام علیه یوتیوب و آیو گروپ علیه وی‌ای‌او اچ نقش مهمی در تبیین و تحکیم این دکترین ایفا کرده‌اند که در بخش‌های آتی مورد بررسی قرار می‌گیرند. در اتحادیه اروپا نیز با تصویب «قانون خدمات دیجیتال» رویکردی فعال‌تر نسبت به کنترل محتوا اتخاذ شده و نظام مسئولیت از وضعیت منفعل به سمت مسئولیت مشارکتی حرکت کرده است. درنتیجه، محور اصلی پژوهش‌های بین‌المللی در این حوزه ایجاد تعادل میان آزادی بیان و مسئولیت ناشی از انتشار محتوای غیرقانونی بوده است.

در حقوق ایران، پژوهش‌های مرتبط، عمدتاً به‌صورت پراکنده و در قالب تفسیر از قوانین

موجود از جمله «قانون جرایم رایانه‌ای» مصوب ۱۳۸۸ و «قانون تجارت الکترونیکی» مصوب ۱۳۸۲ انجام شده و کمتر پژوهشی به تحلیل تطبیقی یا ارائه چهارچوب نظری منسجم پرداخته است؛ به‌عنوان‌نمونه، مرکز پژوهش‌های مجلس در گزارش تنظیمی در سال ۱٤۰۱ با عنوان «بررسی ابعاد مسئله اطلاعات، اخبار و محتوای خلاف واقع در فضای مجازی»، به تحلیل وظایف نهادهای تنظیم‌گر، سکوهای نشر و کاربران در مواجهه با انتشار محتوای نادرست پرداخته و بر ضرورت تفکیک مسئولیت میان سکو، درگاه نشر و کاربر تأکید کرده است. این گزارش همچنین ضعف چهارچوب قانونی موجود به‌ویژه در حوزهٔ ضمانت اجرا و فقدان نهاد نظارتی مستقل را برجسته می‌سازد. هرچند نقطه قوت این گزارش، اتخاذ نگاهی سیستمی به مسئولیت در فضای مجازی است؛ اما فقدان تحلیل تطبیقی و بحث نظری پیرامون مسئولیت مدنی از مناظر فقهی و حقوقی، ازجمله کاستی‌های آن به‌شمار می‌رود.

این خلأ تا حدودی در مقاله‌ای با عنوان «مسئولیت مدنی سکوهای آنلاین در قبال اعمال کاربران» مورد توجه قرار گرفته است. در این پژوهش مبانی فقهی و حقوقی مسئولیت سکوها در سیستم حقوقی ایران با سیستم‌های حقوقی ایالات متحده و اتحادیه اروپا مقایسه شده است. نویسندگان با استناد به قواعد اتلاف و تسبیب در فقه امامیه، نتیجه می‌گیرند که سکوها اصولاً از مسئولیت مبرا هستند، مگر آنکه سبب اقوی از مباشر احراز شود. همچنین با اشاره به اصل شخصی بودن مسئولیت، بر عدم مسئولیت سکو در قبال اعمال کاربران جز در فرض تقصیر یا سوءنیت تأکید می‌کنند. بااین‌حال، این مقاله فاقد چهارچوب سیاست‌گذاری و تحلیل کارکردی بوده و پیشنهاد مشخصی برای بهبود یا اصلاح نظام تقنینی ایران ارائه نمی‌دهد.

بررسی ادبیات حقوقی داخلی و خارجی نشان می‌دهد که تاکنون پژوهشی جامع که از یک‌سو بر دکترین «بندر امن» و از سوی‌دیگر بر ظرفیت‌های حقوقی ایران در طراحی الگویی بومی برای مسئولیت سکوها تمرکز داشته باشد، انجام نشده است. براین‌اساس، مقاله حاضر با مقایسه سیستم حقوقی ایران با ایالات متحده و اتحادیه اروپا به تحلیل سه‌گانهٔ مسئولیت مدنی، کیفری و نظارتی سکوها می‌پردازد و درنهایت، الگویی قابل بهره‌برداری

در سیستم حقوقی کشور برای تنظیم مسئولیت سکوها در چهارچوب دکترین «بندر امن» ارائه می‌دهد؛ الگویی که همزمان از آزادی بیان و نوآوری حمایت کرده و از گسترش محتوای غیرقانونی در سطح ملی جلوگیری می‌کند.

مسئولیت سکوها در قبال محتوای منتشر شده توسط کاربران، یکی از چالش‌برانگیزترین مسائل حقوقی در این حوزه به‌شمار می‌رود. در سیستم‌های حقوقی پیشرفته، سازوکارهای نسبتاً منسجمی برای مواجهه با این چالش طراحی شده است. درمقابل، در حقوق ایران چهارچوب قانونی مشخصی برای تعیین حدود و ثغور مسئولیت سکوهای میزبانی وجود ندارد و صرفاً در قانون جرایم رایانه‌ای مصوب ۱۳۸۸، از منظر کیفری، تکالیفی برای ارائه‌دهندگان خدمات اینترنتی پیش‌بینی شده است. این رویکرد به دلیل فقدان قوانین جامع و مدون، چالش‌های متعددی در مدیریت حقوقی فضای مجازی ایجاد کرده است. براین‌اساس، پرسش اصلی پژوهش این است که رویکرد حقوق ایران در زمینه مسئولیت سکوهای میزبانی، در مقایسه با قوانین ایالات متحده و اتحادیه اروپا در چه وضعیتی قرار دارد و تا چه میزانی قادر به پاسخگویی به نیازهای حقوقی فضای مجازی کشور است. برای پاسخ به این پرسش، ابتدا سیستم حقوقی ایالات متحده و سپس اتحادیه اروپا بررسی شده و درنهایت، وضعیت حقوق ایران مورد بررسی قرار گرفته و نتایج حاصل از آن ارائه خواهد شد.

۱. بررسی مسئولیت سکوهای میزبانی محتوا در ایالات متحده آمریکا

پذیرش این واقعیت که فراگیر شدن استفاده از اینترنت، چالش‌های حقوقی نوینی برای صاحبان حقوق و سکوهای فعال در فضای مجازی ایجاد می‌کند، کنگره آمریکا را به این نتیجه رسانید که قوانین قدیمی کپی‌رایت، پاسخ‌گوی تنظیم روابط در محیط دیجیتال نیستند. این امر درنهایت به تدوین قانون کپی‌رایت هزاره دیجیتال[1] (به اختصار *DMCA*) انجامید *(Ward, 2012, p.206)*. افزون‌براین، فرایند تقنین این قانون تا حد قابل‌توجهی تحت تأثیر پروندهٔ نتکام قرار داشت؛ پرونده‌ای که در آن، دادگاه استدلال نمود کسب‌وکارهایی که وظیفه

1. Digital Millennium Copyright Act (1998)

اصلی آن‌ها ارائه خدمات مبتنی بر اینترنت است، در صورت فقدان قصد و عمد، نباید به دلیل نقض تصادفی، مسئول نقض مستقیم کپی‌رایت شناخته شوند.[1]

یکی از مهم‌ترین نوآوری‌های قانون مذکور، بهره‌گیری از دکترین «بندر امن»[2] است. به موجب این دکترین، سرویس‌دهندگان اعم از ارائه‌دهندگان خدمات میزبانی یا خدمات دسترسی می‌توانند در صورت رعایت شرایط مقرر در قانون، از مسئولیت حقوقی ناشی از محتوای منتشرشده توسط کاربران خود معاف شوند.

در سیستم حقوقی ایالات متحده، به‌جای به‌کارگیری اصطلاح کلی «مسئولیت ثانویه»، غالباً از مفاهیم «مسئولیت نیابتی» و «مسئولیت مشارکتی» استفاده می‌شود. «مسئولیت ثانویه» ناظر بر وضعیتی است که شخص با آگاهی از فعالیت ناقض، به طور مادی در رفتار نقض‌کننده مشارکت کرده یا وی را ترغیب به نقض نماید. درمقابل، «مسئولیت نیابتی» یا «مسئولیت مشارکتی» زمانی مطرح می‌شود که شخص، درحالی‌که حق و توانایی نظارت بر فعالیت ناقض را دارد، به‌طور ناعادلانه از آن فعالیت منتفع شده و دارای منفعت مالی مستقیم باشد (*Farano, 2012, p.65*). به نظر می‌رسد مبنای عدم مسئولیت اولیه سکوها در حقوق ایالات متحده را باید در شرایط تحقق مسئولیت مشارکتی جست‌وجو کرد که تحقق آن مستلزم اجتماع دو عنصر «حق و توانایی کنترل نقض» و «منفعت مالی مستقیم» است (*Krokida, 2022, p.65*)؛ بنابراین سکو تنها درصورتی مسئول نقض حقوق مالکیت فکری است که اولاً، حق و توانایی کنترل نقض را داشته باشد، و ثانیاً، نفع مستقیم از نقض ببرد؛ در غیراین‌صورت، از مسئولیت معاف خواهد بود.

۱.۱. شرایط برخورداری از حمایت دکترین «بندر امن»

به موجب این قانون، سرویس‌دهنده در صورتی تحت حمایت دکترین «بندر امن» قرار می‌گیرد و به‌سبب محتوای منتشر شده توسط کاربر مسئول شناخته نمی‌شود که سه شرط زیر به‌صورت همزمان محقق باشد:

1. Religious Technology Center v Netcom On-Line Communication Services, Inc. (1995)
2. Safe Harbor Doctrine

۱.۱.۱. عدم آگاهی از محتوای ناقض حق

نخستین شرط آن است که سرویس‌دهنده از وجود محتوای ناقض حق آگاه نباشد. به‌بیان‌دیگر، سکو زمانی می‌تواند از مصونیت ناشی از دکترین «بندر امن»، بهره‌مند شود که علم واقعی نسبت به نقض نداشته باشد و یا آنکه از اوضاع و احوال و قرائن موجود، از فعالیت ناقض حق آگاهی پیدا نکند و به محض تحصیل علم یا اطلاع، فوراً نسبت به حذف محتوا و جلوگیری از دسترسی به آن اقدام نماید.

اهمیت معیار تشخیص آگاهی، به‌ویژه به دلیل حجم بالای دعاوی مطروحه درخصوص مسئولیت سکوها در دادگاه‌های ایالات متحده، دوچندان می‌شود. همان‌گونه که پیش‌تر اشاره شد، برخورداری سکو از مصونیت دکترین «بندر امن» مستلزم آن است که از نقض کپی‌رایت و یا از اوضاع و احوالی که به‌طور آشکار فعالیت ناقض را نشان می‌دهد، آگاهی نداشته باشد. سکو از طرق مختلفی مانند داشتن سیستم نظارتی بر محتواهای انتشار یافته، دریافت پست الکترونیک مبنی بر وجود محتوای ناقض، و یا استفاده شخصی از سکو و کشف محتوا می‌تواند علم حقیقی را به دست بیاورد.

در غیاب علم واقعی، سکو می‌تواند از طریق اوضاع و احوال و قرائن موجود، محتوای ناقض را کشف نماید. این معیار با عنوان «معیار پرچم قرمز»[1] شناخته می‌شود. براین‌اساس، اگرچه مطابق بخش *512(c)(1)* قانون *DMCA*، سکوها مکلف به پایش مستمر خدمات خود یا جستجوی فعالانه موارد نقض نیستند؛ اما درصورتی‌که از شرایطی مطلع شوند که نقض را آشکار می‌سازد و در حذف فوری محتوا اقدام نکنند، حق بهره‌مندی از حمایت دکترین «بندر امن» را از دست خواهند داد (*Ward, 2012, p.211*).

دادگاه در پرونده ویاکام علیه یوتیوب، در خصوص تفکیک میان علم واقعی و معیار پرچم قرمز استدلال کرد که علم واقعی، این حقیقت را آشکار می‌سازد که آیا سکو شخصاً از نقض اطلاع داشته است یا خیر؛ و درمقابل، معیار پرچم قرمز مشخص می‌کند که آیا سکو، نوعاً و از منظر یک فرد معقول و متعارف می‌توانست محتوای ناقض را تشخیص بدهد یا خیر؟ همچنین دادگاه در این پرونده بیان داشت که پست‌های الکترونیک داخلی

1. Red Flag Test

یوتیوب که ناظر بر جست‌وجوی درون تارنما بودند، می‌تواند به‌عنوان مدرکی دال بر وجود پرچم قرمز تلقی گردد.[۱]

اهمیت پرونده ویاکام از آن جهت است که به‌عنوان مبنای استدلال در پرونده‌های بعدی قرار گرفت؛ به‌طورمثال دادگاه در پروندهٔ کپیتال‌رکوردز، این موضوع را که کارمند خوانده برخی از آهنگ‌های ناقض حق را مشاهده کرده است، به‌عنوان علم واقعی یا دال بر وجود پرچم قرمز تلقی نکرد.[۲]

۲.۱.۱. نداشتن "منفعت مالی مستقیم" از فعالیت کاربر متخلف

چنانچه سرویس‌دهنده، حق و توانایی کنترل فعالیت کاربر متخلف را داشته باشد، نباید منفعت مالی مستقیمی از آن فعالیت تحصیل کند. شرط فقدان کسب منفعت مالی مستقیم، یکی از ارکان اساسی برخورداری از حمایت‌های دکترین «بندر امن» به‌شمار می‌رود؛ بدین معنا که سرویس‌دهنده نباید به‌طور مستقیم از نقض حقوق مالکیت فکری، نظیر فروش محتوای ناقض یا دریافت وجه در قبال نمایش آن، منتفع شود.

اگرچه دریافت هزینه در قبال ارائه خدمات میزبانی، شیوه‌ای قانونی برای کسب درآمد است؛ اما در عمل بسیاری از ارائه‌دهندگان خدمات میزبانی ازجمله یوتیوب، خدمات خود را به صورت رایگان در اختیار کاربران قرار داده و درآمد خود را از طریق فروش فضای تبلیغاتی به‌دست می‌آورند. دراین‌راستا، این پرسش مطرح می‌شود که آیا درآمد حاصل از این تبلیغات را می‌توان به‌عنوان منفعت مالی مستقیم ناشی از فعالیت ناقض تلقی کرد و آن را از مصادیق نقض دکترین «بندر امن» دانست؟

دادگاه‌های ایالات متحده از ارائه پاسخ صریح به این پرسش اجتناب کرده و به‌جای آن، با تمرکز بر این موضوع که آیا ارائه‌دهندگان خدمات میزبانی حق و توانایی کنترل موارد نقض را داشته‌اند یا خیر، واجد شرایط بودن آن‌ها برای بهره‌مندی از حمایت مقرر در قانون را بررسی می‌کنند (*Wang, 2018, p.106*). به‌عنوان‌نمونه، در پرونده آیو گروپ، دادگاه حکم داد که «...حتی با فرض دریافت منفعت مالی مستقیم از فعالیت‌های ادعایی نقض،

1. Viacom International, Inc. v. YouTube, Inc. (2012)
2. Capitol Records, LLC v. Vimeo, LLC (2016).

ازآنجاکه خوانده نه حق کنترل چنین فعالیت‌هایی را داشته و نه توانایی اعمال آن را دارا بوده است، همچنان واجد شرایط بهره‌مندی از حمایت مقرر در قانون محسوب می‌شود...».[1]

همچنین در پرونده ویاکام علیه یوتیوب، دادگاه پذیرفت که «...ممکن است اختلاف‌نظرهایی در خصوص تلقی درآمدهای تبلیغاتی که به‌صورت یکسان بر کل محتوای سکو اعمال می‌شود، صرف‌نظر از ناقض بودن یا نبودن محتوا، به‌عنوان منفعت مستقیم وجود داشته باشد...». بااین‌حال دادگاه با استناد به فقدان حق و توانایی یوتیوب در کنترل موارد نقض، حکم داد که این سکو همچنان مشمول حمایت دکترین «بندر امن» است.

۳.۱.۱. اقدام سریع در حذف یا مسدودسازی محتوای ناقض قانون پس از اطلاع

مطابق قانون *DMCA*، پس از دریافت اخطار معتبر مبنی بر نقض ادعایی، سرویس‌دهنده مکلف است بدون تأخیر نسبت به حذف محتوای موردنظر یا مسدودسازی دسترسی به آن اقدام نماید. در ایالات متحده، ارائه‌دهندگان خدمات، موظف‌اند تا نماینده‌ای را برای دریافت اخطاریه‌های مربوط به ادعاهای نقض کپی‌رایت به اداره کپی‌رایت معرفی کنند که مشخصات آن در وبگاه رسمی این اداره در دسترس عموم قرار دارد.

درصورتی‌که که اثر متعلق به دارنده کپی‌رایت از طریق سکو ارائه‌دهنده خدمات مورد نقض قرار گیرد، دارنده حق می‌تواند اخطاریه ادعای نقض (که معمولاً با عنوان "اخطار حذف" یاد می‌شود) را به نماینده معرفی‌شده ارسال نماید. مطابق با قوانین ایالات متحده، اخطار حذف زمانی از اعتبار قانونی برخوردار است که به‌صورت کتبی تنظیم شده و واجد عناصر زیر باشد (*U.S. Copyright Office, 2020, p.25*):

۱. امضای فیزیکی یا الکترونیکی شخص مجاز برای اقدام از جانب دارنده کپی‌رایت؛

۲. تعیین دقیق آثار مورد ادعای نقض‌شده؛

۳. شناسایی محتوای ادعایی ناقض و ارائه اطلاعات کافی برای یافتن آن توسط سرویس‌دهنده؛

٤. اطلاعات تماس شاکی؛

1. Io Group, Inc v. Veoh Internets, Inc. (2008)

۵. اظهارنامه‌ای مبنی اعتقاد با حسن‌نیت شاکی نسبت به غیرمجاز بودن استفاده مورد شکایت؛

٦. اظهارنامه‌ای مبنی بر صحت اطلاعات مندرج در اخطاریه و اختیار قانونی شاکی برای اقدام، تحت مجازات شهادت برای دروغ.

این پرسش مطرح می‌شود که درصورت فقدان هریک از عناصر یادشده، آیا اخطار حذف همچنان معتبر تلقی می‌شود یا خیر؟ در پاسخ باید گفت اخطارهایی که فاقد برخی از عناصر الزامی هستند، همچنان می‌توانند برای حذف محتوای ادعایی ناقض کافی باشند عناصری نظیر امضا، اظهار حسن‌نیت و اظهار صحت اطلاعات، همواره به‌عنوان اجزای مطلقاً ضروری اخطاریه تلقی نشده‌اند. درهمین‌راستا، در پرونده روسی علیه موشن پیکچرز، دادگاه مقرر داشت که نقص در برخی مفاد اخطار حذف، موجب بی‌اعتباری آن نخواهد شد.[1]

چنانچه سکو از وجود محتوای ناقض آگاه شود، به‌ویژه اگر از طریق شکایت دارنده کپی‌رایت یا دستور رسمی مراجع ذی‌صلاح باشد، باید فوراً نسبت به حذف یا مسدودسازی آن اقدام نماید. مفهوم «اقدام سریع» مندرج در بخش *512(c)* قانون، مفهومی نسبی است که باید به‌صورت موردی و با توجه به اوضاع و احوال هر پرونده تفسیر شود. این برداشت هم از تاریخچه تقنینی، هم از رویه قضائی و هم از ادبیات حقوقی استنباط می‌شود. در عمل، بازه زمانی یک تا چند روز پس از تحقق علم واقعی یا آگاهی عینی سکو، به‌عنوان معیار کلی اقدام سریع پذیرفته شده است *(Wilman, 2020, p.146)*. به‌عنوان‌نمونه، در پرونده شرکت اسکوئر رینگ دادگاه تصریح نمود که: «...تشخیص فوری بودن حذف محتوا ظرف ٤٨ ساعت، مستلزم بررسی مجموعه‌ای از عوامل موضوعی است...».[2]

اداره کپی‌رایت ایالات متحده نیز در گزارش سالانه ۲۰۲۰ خود در خصوص بخش *512(c)*، با اشاره به تنوع رویه دادگاه‌ها در تفسیر قید «سریع»، بر ضرورت انعطاف‌پذیری قضائی و توجه به شرایط خاص هر پرونده تأکید کرده است *(Smith, 2020, p.6)*.

۲.۱. ضمانت اجرای اخطار حذف اشتباه

1. Rossi v. Motion Picture Ass'n of America Inc. (2004)
2. Square Ring, Inc. v. UStream.com (2015)

پس از حذف یا غیرفعال‌سازی دسترسی به محتوای مورد اعتراض، سکو از هرگونه مسئولیت در قبال دعاوی احتمالی علیه کاربری که محتوا را بارگزاری کرده است، مصون می‌ماند. در این وضعیت، پرسش اساسی آن است که در صورت نادرست بودن اخطاریه حذف، چه تضمینی برای جبران حقوق تضییع‌شده کاربر وجود دارد. مطابق بخش *(f) 512* قانون، هر شخصی که عمداً و به‌طور اساسی در اخطار حذف ادعا کند که محتوا یا فعالیتی ناقض کپی‌رایت است، درحالی‌که چنین نباشد، مسئول جبران کلیه خسارت وارده ازجمله هزینه‌ها و حق‌الوکاله به طرفی خواهد بود که به نادرستی به نقض متهم شده است.

بر اساس این مقرره، کاربر منتشرکننده محتوا می‌تواند از طریق ارسال «اعتراض متقابل»، نسبت به اخطار حذف واکنش نشان دهد. در این‌راستا ارائه‌دهنده خدمات موظف است بدون تأخیر، حذف یا غیرفعال‌سازی محتوا را به کاربر اطلاع دهد. چنانچه کاربر با ارائه اعتراض متقابل به اخطار حذف اعتراض نماید، ارائه‌دهنده خدمات مکلف است، ظرف مدت ۱۰ تا ۱٤ روز کاری از زمان دریافت اعتراض، محتوای حذف‌شده را بازیابی کند، مگر آنکه دارنده کپی‌رایت در این بازه زمانی اقدام به طرح دعوا و اخذ دستور قضائی نماید.

مطابق بخش *(3)(g) 512*، اعتراض متقابل باید شامل عناصر زیر باشد:

۱. امضای فیزیکی یا الکترونیکی ارسال‌کننده؛

۲. شناسایی محتوای حذف‌شده و ذکر محل آن پیش از حذف؛

۳. اظهارنامه تحت مجازات شهادت دروغ مبنی بر اعتقاد صادقانه ارسال‌کننده به حذف اشتباه محتوا؛

٤. اطلاعات تماس ارسال‌کننده، به همراه پذیرش صلاحیت دادگاه فدرال ذی‌صلاح در ایالات متحده.

در خصوص معیار تشخیص «علم» و «اساسی بودن» اظهار خلاف واقع، پرونده گروه سیاست‌گذاری برخط علیه شرکت دایبولد اهمیت ویژه‌ای دارد. در این پرونده، دادگاه به این نتیجه رسید که خواهان عمداً و به طور اساسی در اخطار حذف خود اظهارات نادرستی ارائه کرده است، چراکه حتی در فرض شمول حمایت کپی‌رایت، محتوای مورد بحث

به‌وضوح مشمول استثنای استفاده غیرمنصفانه بودن است.[1] دادگاه همچنین مقرر داشت که در چهارچوب ماده ۵۱۲، «عمدی بودن» به این معناست که شخص یا عملاً از نادرستی ادعا آگاه بوده، یا با اعمال مراقبت متعارف می‌بایست از آن آگاه می‌بود، و «اساسی بودن» ناظر بر آن است که اظهار نادرست، بر واکنش ارائه‌دهنده خدمات نسبت به اخطار، تأثیر گذاشته باشد *(Wang, 2018, p.147)*.

۳.۱. چالش‌ها و انتقادات وارد بر دکترین «بندر امن» در حقوق ایالات متحده آمریکا

با وجود نقش مهم دکترین «بندر امن» مندرج در بخش ۵۱۲ قانون *DMCA* در توسعه اقتصاد دیجیتال و ایجاد اطمینان حقوقی برای ارائه‌دهندگان خدمات اینترنتی، این سازوکار با انتقادات متعددی روبه‌رو است. مهم‌ترین انتقاد، انتقال بار اصلی نظارت بر نقض حقوق مالکیت فکری به دارندگان حقوق است. در نظام «اخطار و حذف»، صاحبان آثار ناگزیر از پایش مستمر اینترنت و شناسایی موارد نقض هستند؛ امری که با توجه به حجم گستردهٔ محتوای کاربران، مستلزم صرف هزینه‌های مالی و فنی قابل‌توجهی بوده و برای اشخاص حقیقی و شرکت‌های کوچک غالباً دشوار می‌نماید *(Urban & Quitler, 2006, p.688)*.

چالش دیگر، تکرار نقض پس از حذف محتوا در قالب «چرخه اخطار و حذف» است؛ زیرا کاربران می‌توانند محتوا را مجدداً بارگذاری کرده یا با حساب‌های کاربری جدید به نقض ادامه دهند. این وضعیت نشان می‌دهد که سازوکار *DMCA* عمدتاً ماهیتی واکنشی دارد و کارکرد پیشگیرانهٔ آن محدود است *(U.S. Copyright Office, 2020, p.169)*.

از منظر تفسیری، معیارهای «آگاهی» و «حق و توانایی کنترل» نیز محل چالش هستند. رویهٔ قضائی ایالات متحده، ازجمله در پرونده ویاکام علیه یوتیوب، آگاهی کلی را کافی ندانسته و علم نسبت به موارد مشخص را ضروری دانسته است. این تفسیر، اگرچه امنیت حقوقی سکوها را تقویت کرده، از دید دارندگان حقوق به معنای کاهش مسئولیت‌پذیری ارائه‌دهندگان خدمات تلقی شده است.

---

1. Online Policy Group v. Diebold, Inc. (2004)

همچنین تفسیر شرط فقدان «منفعت مالی مستقیم» و توسعه مدل‌های کسب‌وکار مبتنی بر تبلیغات برخط، تعیین رابطه میان نقض حقوق و منافع اقتصادی سکوها را پیچیده کرده است. این دکترین از منظر آزادی بیان نیز مورد انتقاد قرار گرفته است؛ زیرا حذف سریع محتوا گاه به حذف آثار مشروع منجر می‌شود *(Urban et al. 2017. P.392)*.

درنهایت، تحولات فناورانه و استفاده از سامانه‌های خودکار شناسایی محتوا، مرز میان نظارت منفعل و فعال سکوها را مبهم ساخته و بحث‌هایی درباره ضرورت اصلاح چهارچوب مسئولیت مطرح کرده است.

۲. بررسی مسئولیت سکوهای میزبانی محتوا در اتحادیه اروپا

در اتحادیه اروپا، برخلاف ایالات متحده چهارچوب واحد و هماهنگ‌شده‌ای به‌عنوان مبنای عام مسئولیت مدنی سکوها وجود ندارد. تعیین حدود مسئولیت سکوهای میزبانی محتوا به قوانین داخلی کشورهای عضو واگذار شده است و این کشورها از مفاهیم متنوعی مانند «مسئولیت ثانویه»، «مسئولیت غیرمستقیم» و «مسئولیت مشترک در ارتکاب عمل زیان‌بار» استفاده می‌کنند *(Farano, 2012, p.22)*.

بااین‌حال، ارزیابی مسئولیت سکوهای میزبانی در اتحادیه اروپا عمدتاً تحت تأثیر دو سند بنیادین حقوقی قرار دارد که بیانگر تحول تدریجی رویکرد قانون‌گذار اروپایی در مواجهه با چالش‌های فزاینده فضای دیجیتال است.

۱.۲. دستورالعمل تجارت الکترونیک اتحادیه اروپا[1]

دستورالعمل تجارت الکترونیکی اتحادیه اروپا که با هدف تسهیل و تنظیم تجارت الکترونیک در داخل اتحادیه تصویب شد، با استقرار چهارچوب دکترین «بندر امن»، قواعد اولیه مسئولیت محدود میزبان‌ها را پایه‌گذاری نمود. این دستورالعمل به‌طور خاص به تبیین مسئولیت سکوهای اینترنتی و ارائه‌دهندگان خدمات برخط در قبال محتوای تولیدشده توسط کاربران پرداخته و نحوه تعامل آن‌ها با قواعد مسئولیت مدنی و حقوق مالکیت فکری

1. Directive on Electronic Commerce (2000)

را مشخص می‌سازد.

رویکرد حاکم بر این دستورالعمل ماهیتی انفعالی دارد؛ به این معنا که سکوهای میزبانی را صرفاً در صورتی مسئول شناخته می‌شوند که از محتوای غیرقانونی آگاه بوده و با وجود این آگاهی، در حذف یا مسدودسازی آن اقدام به موقع انجام ندهند. این نظام مبتنی بر سازوکار «اخطار و حذف» در بستر فضای دیجیتال اولیه طراحی شده و به همین دلیل، در پاسخگویی به پیچیدگی‌های عصر حاضر با محدودیت‌هایی مواجه است.

دستورالعمل تجارت الکترونیک و دکترین «بندر امن» در حقوق ایالات متحده، به‌ویژه از حیث عدم مسئولیت اولیه میزبان‌ها و لزوم تحقق آگاهی برای ایجاد مسئولیت، شباهت‌های قابل‌توجهی دارند. در هر دو نظام، سرویس‌دهندگان اینترنتی در قبال محتوای تولیدشده توسط کاربران خود مسئولیتی ندارند، مگر آنکه از نقض حقوق مالکیت فکری آگاه شوند و در واکنش به آن اقدامی انجام ندهند. به نظر می‌رسد ماده ١٤ دستورالعمل تجارت الکترونیک، به ویژه از ماده *512 (c)* قانون *DMCA* الهام گرفته شده باشد؛ هرچند در پیشنهاد اولیه کمیسیون اروپا اشاره‌ای به این موضوع نشده است؛ اما هم‌زمان تصویب دو مقرره و شباهت‌های مفهومی و اصطلاحی آن‌ها، این تأثیرپذیری را آشکار می‌سازد (*Wilman, 2020, p.17*).

مطابق ماده ١٤ دستورالعمل، ارائه‌دهنده خدمات میزبانی در قبال اطلاعات ذخیره‌شده به درخواست کاربر، مشروط به تحقق شرایط مقرر، مسئولیتی نخواهد داشت که در ادامه بررسی می‌شوند.

۱.۱.۲. عدم آگاهی از محتوای غیرقانونی

نخستین شرط معافیت از مسئولیت آن است که سرویس‌دهنده از فعالیت یا اطلاعات غیرقانونی علم واقعی نداشته و یا از اوضاع و احوالی که ماهیت غیرقانونی فعالیت یا اطلاعات را آشکار می‌سازد، آگاه نباشد.

دستورالعمل تعریف مشخصی از «علم واقعی» ارائه نمی‌دهد و تشخیص معیارها و مصادیق آن را به دادگاه واگذار کرده است. در خصوص آگاهی از نقض آشکار، این مفهوم را می‌توان معادل «تکلیف به دانستن» یا «وجود دلیل برای آگاهی» دانست که در حقوق مسئولیت مدنی برای سنجش آگاهی فرضی به‌کار می‌روند. در این زمینه دیوان دادگستری

اتحادیه اروپا، در پرونده لورل علیه ای‌بِی معیارهایی برای احراز آگاهی ارائه‌دهنده خدمات میزبانی از نقض موضوع ماده ۱٤ ارائه کرد. براساس این رأی، برای محروم شدن میزبان از معافیت مقرر، کافی است ثابت شود که وی از وقایع یا شرایطی آگاه بوده که یک فعال اقتصادی متعارف در وضعیت مشابه می‌بایست براساس آن‌ها، وجود نقض را تشخیص داده و مطابق ماده ۱٤ اقدام می‌کرد.[1]

۲.۱.۲. حذف سریع محتوا پس از آگاهی

شرط دوم آن است که سرویس‌دهنده، پس از تحصیل علم یا آگاهی نسبت به محتوای غیرقانونی، فوراً نسبت به حذف آن یا غیرفعال‌سازی دسترسی به اطلاعات موردنظر اقدام نماید. درواقع، سکو در ابتدا فاقد آگاهی عینی از ماهیت غیرقانونی محتوا بوده و پس از دستیابی به چنین آگاهی، برای بهره‌مندی از مصونیت مقرر در ماده ۱٤، ملزم به واکنش سریع است *(Wilman, 2020, p.39)*.

دیوان دادگستری اروپا در پرونده لورل علیه ای‌بِی که سابقاً گذشت، همچنین مشخص کرد که سکو می‌تواند به طرق گوناگونی از جمله اخطار ثبت‌شده توسط کاربران در خصوص محتوایی که به نظر آن‌ها ناقض حق است، و یا بررسی‌های خود سکو در راستای کشف محتوای ناقض، به علم حقیقی یا آگاهی مندرج در بند (ب) ماده ۱٤.۱ دست یابد.

بااین‌حال، در دستورالعمل، تعریف دقیقی از مفهوم «اقدام سریع» ارائه نکرده است. این ابهام، اگرچه امکان انعطاف‌پذیری در رسیدگی موردی را فراهم می‌کند؛ اما هم‌زمان موجب عدم قطعیت حقوقی قابل‌توجهی برای میزبان‌های اروپایی می‌شود. تعیین بازه‌های زمانی کوتاه ممکن است میزبان‌ها را به حذف بیش‌ازحد محتوا سوق دهد و اثر منفی بر آزادی بیان داشته باشد. در عمل، مقررات ملی کشورهای عضو اتحادیه اروپا رویکردهای متفاوتی اتخاذ کرده‌اند و بازه‌های زمانی متفاوتی بین دوازده ساعت تا سه روز را برای اقدام الزام‌آور دانسته‌اند (*Angelopoulos, 2016, p.88*).

1. L'Oréal v. eBay (2011)

۲.۲. قانون خدمات دیجیتال[1]

تحولات گسترده در شیوه تولید، توزیع و انتشار محتوا در بستر اینترنت و ظهور بازیگران جدید در حوزه خدمات دیجیتال، ناکارآمدی نسبی مقررات سنتی اتحادیه اروپا ازجمله دستورالعمل تجارت الکترونیک را آشکار ساخت. ازجمله این کاستی‌ها می‌توان به ابهام در مفهوم «آگاهی واقعی»، تفاوت‌های قابل توجه در طراحی و اجرای سازوکار «اخطار و حذف» و ناهمگونی سیستم‌های حقوق کشورهای عضو اشاره کرد. برخی کشورها مدل «اخطار و حذف»، برخی «اخطار و حذف ماندگار» و برخی «اخطار و اخطار» را پذیرفته‌اند و در مواردی نیز هیچ سازوکار مشخصی پیش‌بینی نشده است. این ناهمگونی‌ها منجر به عدم قطعیت حقوقی برای واسطه‌های اینترنتی در سطح اتحادیه شده است (*Madiega, 2020, pp.5-6*).

در واکنش به این وضعیت، قانون خدمات دیجیتال پا به عرصهٔ وجود گذاشت تا به‌عنوان نسل جدید قانون‌گذاری در حوزه مسئولیت سکوهای دیجیتال ایفای نقش کند. این قانون اگرچه اصل مسئولیت محدود میزبان‌ها را تغییر نداده و متن ماده ١٤ دستورالعمل تجارت الکترونیک را در ماده ٦ خود تکرار کرده است؛ اما با وضع مجموعه‌ای از الزامات رویه‌ای، ساختاری و نظارتی، سطح پاسخ‌گویی سکوها را به‌طور معناداری ارتقا داده است و چهارچوبی نظام‌مندتر برای ایفاء مسئولیت آن‌ها ترسیم شده است. مطالعات نشان می‌دهند که همچنان تفاوت‌های اساسی در اجرای دستورالعمل تجارت الکترونیک در سطح اتحادیه اروپا وجود دارد و رویه‌های قضائی ملی در زمینه نظام‌های مسئولیت، ناهماهنگ و پراکنده باقی مانده و پژوهشگران به تداوم ابهامات حقوقی در کاربرد قوانین ملی و وجود آراء متناقض میان کشورهای عضو و حتی درون کشورها اذعان دارند *(Madiega, 2020, p.4)*.

قانون خدمات دیجیتال با پذیرش تداوم ناهماهنگی در اجرای دستورالعمل تجارت الکترونیک و پراکندگی رویه‌های قضائی ملی، رویکردی سلسله مراتبی اتخاذ کرده و مسئولیت سکوها را متناسب با اندازه، میزان تأثیرگذاری و توانمندی‌های فنی آن‌ها تفکیک نموده است. این قانون علاوه بر پیش‌بینی سازوکارهای نظارتی پیشرفته برای سکوهای بسیار بزرگ،[2] با الزام به

1. Digital Services Act (2022)
2. Very Large Online Platforms (VLOPs)

شفافیت الگوریتمی، ایجاد سازوکارهای اعتراض و تقویت حقوق کاربران، چهارچوبی جامع‌تر برای حکمرانی فضای دیجیتال ارائه می‌دهد *(Van Hoboken et al, 2018, p.27)*.

۱.۲.۲. ایجاد سیستم گزارش‌دهی

مطابق ماده ۱۶ قانون خدمات دیجیتال، ارائه‌دهندگان خدمات میزبانی موظف‌اند نظام‌های ساده، برخط و کاربرپسندی را برای گزارش محتوای غیرقانونی ایجاد کنند. این نظام‌ها باید امکان ثبت گزارش‌های دقیق شامل دلایل حقوقی، محل مشخص محتوا ، اطلاعات تماس گزارش‌دهنده (جز در موارد خاص) و تأیید صحت اطلاعات را فراهم سازند. دریافت چنین گزارشی به منزله آگاهی رسمی سکو از محتوای غیرقانونی تلقی می‌شود. سکوها مکلف‌اند دریافت گزارش را فوراً تأیید کرده و در اسرع وقت، تصمیم نهایی خود را به همراه امکان اعتراض به اطلاع کاربران برسانند. بررسی گزارش‌ها باید به‌صورت عینی و به‌موقع انجام شود و درصورت استفاده از سیستم‌های خودکار، این موضوع باید به کاربران اطلاع داده شود.

بند اول ماده ۱۶ قانون خدمات دیجیتال تأکید می‌کند که سازوکارهای «اخطار و حذف» باید به‌سادگی قابل دسترس و کاربرپسند باشند. این سازوکارها باید به‌وضوح قابل شناسایی بوده، در مجاورت محتوای مربوطه قرار بگیرند و دست‌کم به همان میزان سازوکارهای گزارش محتوای مغایر با شرایط استفاده از خدمات میزبانی، ساده و قابل استفاده باشند. ازاین‌رو هرچند سازوکارهای گزارش نقض شرایط استفاده به‌طور مستقیم تحت شمول این مقرره قرار ندارند؛ اما می‌توانند به‌عنوان معیار مقایسه برای ارزیابی رعایت الزامات این ماده مورد استفاده قرار گیرند *(Wilman et al, 2024, p.136)*.

همچنین این بند تصریح می‌نماید که سازوکارهای «اخطار و حذف» باید امکان ارسال اطلاعیه‌ها را صرفاً از طریق وسایل الکترونیکی فراهم آورند. بدین‌ترتیب، ارائه‌دهندگان خدمات نمی‌توانند ارسال اطلاعیه‌ها را به شیوه‌های غیرالکترونیکی مانند مکاتبات کاغذی الزامی بکنند. بااین‌حال، این ماده در عین الزام به استفاده از ابزارهای الکترونیکی، امکان اتخاذ راهکارهای متنوع و متناسب را نیز به رسمیت می‌شناسد. این رویکرد که در راستای حفظ بی‌طرفی فناوری و تسهیل نوآوری اتخاذ شده، با توجه به تنوع گسترده در ماهیت خدمات، امکانات فنی ارائه‌دهندگان و انواع محتوای غیرقانونی مشمول مقرره، به تضمین

اصل تناسب کمک می‌کند. باوجوداین، دامنه اختیار ارائه‌دهندگان خدمات به‌واسطه الزامات مقرر در خصوص سهولت دسترسی و کاربرپسند بودن سازوکارها، محدود می‌گردد.

۲.۲.۲. اقدام داوطلبانه

یکی از نوآوری‌های قانون خدمات دیجیتال، شناسایی «اقدام داوطلبانه» است. مطابق ماده ۷، ارائه‌دهندگان خدمات واسطه صرفاً به این دلیل که با حسن‌نیت و با رعایت تدابیر لازم، به بررسی‌های داوطلبانه در خصوص محتوای غیرقانونی پرداخته یا اقدامات لازم برای شناسایی، کشف، حذف یا مسدودسازی دسترسی به این محتوا را انجام دهند، یا اقدامات ضروری برای انطباق با مقررات اتحادیه اروپا و قوانین ملی همسو با حقوق اتحادیه را اتخاذ بکنند، از شمول معافیت‌های مسئولیت محروم نخواهند شد.

این مقرره به زبان ساده بیان می‌کند که «عملکرد مطلوب نباید مجازات شود» و به‌عبارت دقیق‌تر، نباید با تهدید به از دست دادن معافیت از مسئولیت، از اتخاذ چنین اقداماتی جلوگیری کرد. در جریان تدوین قانون خدمات دیجیتال، ذینفعان هشدار داده بودند که ترس از محروم شدن از مزایای معافیت، به این دلیل که اقدامات آن‌ها ممکن است «بیش‌ازحد فعالانه» تلقی شود، می‌تواند به عاملی بازدارنده در برابر مقابله مؤثر با محتوای غیرقانونی تبدیل گردد. اقدامات پیشین که برای رفع این نگرانی‌ها اتخاذ شده بودند، ظاهراً نتوانسته بودند اطمینان حقوقی کافی ایجاد بکنند *(Wilman, 2022, p.6)*.

هر اقدام داوطلبانه که ارائه‌دهندگان خدمات واسطه برای مقابله با محتوای غیرقانونی انجام می‌دهند، لزوماً «مفید» نیست و بعضاً می‌تواند مخرب باشد؛ به‌عنوان‌مثال، در شرایطی که یک اقدام داوطلبانه منجر به حذف بیش از حد شود ـ یعنی حذف ناعادلانه اطلاعاتی که محتوای غیرقانونی محسوب نمی‌شوند ـ این اقدامات تأثیر منفی بر آزادی بیان خواهند گذاشت. به‌منظور جلوگیری از این مشکل، سکوها در صورت تحقق دو شرط، مشمول این ماده می‌شوند: حسن‌نیت و رعایت مراقبت لازم.

شرط حسن‌نیت ناظر بر قصد و هدف واقعی اقدامات است و تضمین می‌کند که اقدامات

انجام‌شده نه‌تنها در ظاهر، بلکه در عمل نیز با هدف مقابله با محتوای غیرقانونی صورت گرفته باشند؛ برای‌نمونه، اگر اقدامی تحت عنوان مقابله با محتوای غیرقانونی انجام شود؛ اما درواقع اهدافی نظیر تبلیغات یا سانسور غیرضروری را دنبال کند، شرط حسن‌نیت محقق نخواهد شد. همچنین، اتکاء به تفسیری غیرمنطقی از الزامات قانونی می‌تواند به نقض این شرط منجر بشود.

شرط رعایت مراقبت لازم به شیوه اجرای اقدامات مربوط است. همان‌گونه که در بازنگری[1] ۲٦ این قانون آمده است، این شرط مستلزم رفتار عینی، غیرتبعیض‌آمیز و متناسب، با لحاظ حقوق و منافع مشروع تمام طرف‌های ذی‌نفع بوده و ایجاب می‌کند تضمین‌های لازم برای جلوگیری از حذف غیرضروری محتوا پیش‌بینی شود. تعیین دقیق مصادیق این شرط به اوضاع و احوال هر پرونده بستگی دارد و اگرچه این امر تا حدودی موجب عدم قطعیت می‌شود؛ اما با توجه به تنوع گسترده خدمات مشمول مقرره و هدف قانون‌گذار در حفظ بی‌طرفی فناورانه و آینده‌نگری، ارائه قواعد جزئی‌تر دشوار بوده و واگذاری تصمیم‌گیری به دادگاه‌ها به‌صورت موردی، رویکردی موجه به نظر می‌رسد (*Wilman, 2024, p.82-83*).

۳.۲. چالش‌ها و انتقادات وارد بر دکترین «بندر امن» در حقوق اتحادیه اروپا

با وجود تثبیت نظام مسئولیت محدود ارائه‌دهندگان خدمات میزبانی در ماده ١٤ دستورالعمل تجارت الکترونیک و توسعه آن در قانون خدمات دیجیتال، این سازوکار در سطح اتحادیه اروپا با چالش‌های قابل‌توجهی مواجه بوده است. مهم‌ترین انتقاد، عدم هماهنگی در اجرای مقررات میان کشورهای عضو است. واگذاری اجرای دستورالعمل به قوانین ملی، به شکل‌گیری رویه‌های متفاوت در خصوص معیارهای آگاهی، سازوکار اخطار و حذف و حدود مسئولیت سکوها انجامیده و پیش‌بینی‌پذیری حقوقی را در بازار واحد دیجیتال کاهش داده است (*Madiega, 2020, p.8*).

از دیگر چالش‌ها، ابهام در مفاهیم «آگاهی واقعی» و «اوضاع و احوال آشکارکننده فعالیت

1. Recital

غیرقانونی» است. دیوان دادگستری اتحادیه اروپا در پرونده لورل علیه ای‌بِی معیار «فعال اقتصادی متعارف» را برای تشخیص آگاهی مطرح کرد؛ اما انعطاف‌پذیری این معیار به تفاسیر متفاوت در سیستم‌های حقوقی ملی انجامیده و امنیت حقوقی فعالان اقتصادی را تحت تأثیر قرار داده است *(Angelopoulos, 2016, p.85)*.

سازوکار «اخطار و حذف» نیز به‌دلیل انتقال بار نظارت بر نقض به دارندگان حقوق، با انتقاد مواجه شده است. این وضعیت، به‌ویژه برای صاحبان حقوق کوچک، هزینه‌های نظارتی قابل‌توجهی ایجاد می‌کند. افزون‌براین، نبود تعریف دقیق از مفهوم «اقدام سریع» به ایجاد استانداردهای زمانی متفاوت در کشورهای عضو منجر شده است؛ امری که از یک‌سو می‌تواند به حذف پیشگیرانه و گسترده محتوا و تهدید آزادی بیان بینجامد و از سوی‌دیگر ممکن است اثربخشی حمایت از حقوق مالکیت فکری را کاهش دهد (*Angelopoulos, 2016, p.90*).

درنهایت، اگرچه قانون خدمات دیجیتال با هدف رفع ناهماهنگی‌ها و افزایش شفافیت تصویب شد، پیچیدگی الزامات نظارتی و هزینه‌های انطباق، نگرانی‌هایی در خصوص محدود شدن رقابت و ورود بازیگران جدید به بازار ایجاد کرده است. همچنین ابهام در حدود «اقدامات داوطلبانه» و معیار حسن‌نیت می‌تواند به عدم قطعیت حقوقی و حذف بیش از حد محتوا منجر شود. ازاین‌رو، موفقیت نظام «بندر امن» در اتحادیه اروپا تا حد زیادی به نحوه تفسیر و اجرای مقررات توسط دادگاه‌ها و نهادهای نظارتی وابسته است.

۳. بررسی مسئولیت سکوهای میزبانی در ایران

با وجود آنکه طی سال‌های اخیر در سیستم‌های حقوقی پیشرو مانند ایالات متحده و اتحادیه اروپا، دکترین «بندر امن» به‌عنوان چهارچوبی بنیادین برای تحدید مسئولیت سکوهای میزبانی نهادینه شده است، در حقوق ایران چنین نهادی با این عنوان و گستره، به‌صراحت تعریف و تنظیم نشده است. برخی پژوهشگران مسئولیت‌هایی نظیر حفظ حریم خصوصی، مقابله با اطلاعات نادرست و نظارت بر حقوق محتوای دیجیتال را بر عهده سکوهای میزبانی دانسته و بر این‌اساس استدلال کرده‌اند که ازآنجاکه این سکوها به جمع‌آوری و پردازش داده‌های حساس می‌پردازند، باید مسئولیت گسترده‌تری در زمینه

حفظ حریم خصوصی، بررسی محتوای بارگزاری شده، نظارت بر الگوریتم‌ها و ارائه گزارش‌های شفاف برعهده داشته باشند *(کریم‌میان، ۱٤۰٤، ص. ۷۸)*. این دیدگاه مبتنی بر مقدماتی است که نه‌تنها با نحوه عملکرد و ویژگی‌های ذاتی سکوهای میزبانی انطباق ندارد بلکه می‌تواند به‌عنوان مانع جدی در مسیر توسعه این حوزه در سیستم حقوقی ایران عمل بکند. این مطلب به‌وضوح تفاوت دیدگاه حاکم بر پژوهش حاضر، با دیدگاه جاری در میان حقوقدانان و حتی قوانین حاکم را نمایان می‌سازد.

تحولات فنی و گسترش روزافزون استفاده از سکوهای داخلی، ضرورت تبیین جایگاه دکترین «بندر امن» در سیستم حقوقی ایران را بیش از پیش نمایان می‌سازد؛ زیرا نخست آنکه برخلاف ایالات متحده و اتحادیه اروپا، چهارچوب قانونی مشخصی در این زمینه در حقوق ایران وجود ندارد و دوم آنکه مقررات موجود صرفاً از منظر مسئولیت کیفری به این موضوع پرداخته‌اند؛ رویکردی که با منطق حاکم بر دکترین «بندر امن» فاصله قابل‌توجهی دارد.

۱.۳. مسئولیت کیفری ارائه‌دهندگان خدمات اینترنتی

قانون جرائم رایانه‌ای مصوب ۱۳۸۸، مندرج در فصل سی‌ام قانون مجازات اسلامی، در ماده ۲۱ مقرر می‌دارد: «ارائه‌دهندگان خدمات دسترسی موظفند طبق ضوابط فنی و فهرست مقرر از سوی کارگروه تعیین مصادیق موضوع ماده ذیل محتوای مجرمانه که در چهارچوب قانون تنظیم شده است اعم از محتوای ناشی از جرائم رایانه ای و محتوایی که برای ارتکاب جرائم رایانه‌ای به‌کار می رود را پالایش کنند...». براین‌اساس، سکوهای ارائه‌دهنده خدمات دسترسی اصولاً مسئولیتی در قبال محتوای منتشرشده توسط کاربران ندارند؛ زیرا وظیفه اصلی آن‌ها صرفاً فراهم‌سازی امکان دسترسی به اینترنت یا فضای مجازی است. مسئولیت کیفری این دسته از سکوها عمدتاً ناظر بر جلوگیری از فعالیت‌های مجرمانه است، نه نظارت بر محتوای کاربران؛ بنابراین، حتی در صورت آگاهی از وجود محتوای مجرمانه، ارائه‌دهنده خدمات دسترسی به‌طور مستقیم مسئول حذف آن نخواهد بود، مگر آنکه در نشر یا تسهیل ارتکاب جرم، ایفای نقش کرده باشد.

در همین راستا ماده ۲۳ قانون جرائم رایانه‌ای تصریح می‌کند که «ارائه‌دهندگان خدمات میزبانی موظفند به محض دریافت دستور کارگروه تعیین مصادیق مذکور در مادهٔ فوق یا مقام قضائی رسیدگی‌کننده به پرونده مبنی بر وجود محتوای مجرمانه در سامانه‌های رایانه‌ای خود از ادامهٔ دسترسی به آن ممانعت به عمل آورند...». این دو ماده، تنها مقرراتی هستند که مسئولیت سکوها را مورد بررسی قرار داده است. بر اساس این مقررات، سکوهای میزبانی تنها پس از اطلاع از وجود محتوای مجرمانه، مکلف به حذف یا مسدودسازی آن هستند و در صورت عدم رعایت این تکلیف، ممکن است با مسئولیت کیفری مواجه شوند. درنتیجه، مدیران سکوهای میزبانی اصولاً مسئولیت نظارت و پالایش مستمر محتوای بارگذاری‌شده توسط کاربران را برعهده ندارند و مسئولیت محتویات منتشرشده، در اصل متوجه کاربران منتشرکننده است. مسئولیت میزبان صرفاً در مواردی تحقق می‌یابد که با ترک فعل، از اجرای دستور مقام قضائی یا کارگروه تعیین مصادیق خودداری کرده باشد.

تحلیل این مقررات نشان می‌دهد که نمی‌توان آنها را مصداقی از دکترین «بندر امن» یا مصونیت محدود واسطه‌ها تلقی کرد. نخست آنکه این مواد صرفاً به مسئولیت کیفری ارائه‌دهندگان خدمات پرداخته و هیچ‌گونه قاعده‌ای در خصوص تحدید مسئولیت مدنی سکوهای میزبانی ارائه نمی‌دهند. دوم آنکه الزام به گزارش‌دهی و مسدودسازی محتوا در این مقررات، نه بر مبنای پذیرش دکترین «بندر امن»، بلکه بر اساس اصل قانونی بودن جرم و مجازات استوار است؛ به این معنا که قصور در انجام این تکالیف، خود می‌تواند موجب مسئولیت کیفری سکوها شود. بنابراین، تمرکز قانون‌گذار در این مواد بر ایجاد سازوکارهای کنترلی و اعمال ضمانت‌اجراهای کیفری است، نه بر طراحی نظام حمایتی برای تحدید مسئولیت سکوها.

در همین چهارچوب، برخی پژوهش‌ها نشان می‌دهند که این مقررات، نقش ارائه‌دهندگان خدمات دسترسی و میزبانی را عمدتاً در قالب مجریان فرایند پالایش و فیلترینگ محتوا تعریف کرده‌اند *(حاجی ده‌آبادی و همکاران، ۱۴۰۱،ص ۷۹)*. درواقع، قانونگذار از طریق سلب دسترسی و میزبانی، تلاش کرده تا کنترل و نظارت کامل‌تری بر فضای مجازی اعمال کند.

هرچند فیلترینگ به‌عنوان یکی از اقدامات پیشگیرانه می‌تواند قابل توجیه باشد؛ اما اجرای این تدابیر باید به گونه‌ای صورت گیرد که منجر به نقض حقوق بنیادین کاربران نشود *(نجفی ابرندآبادی و رضوانی، ۱۳۹٤، ص. ۵۵۹)*.

فقدان چهارچوب قانونی مشخص جهت تعیین حدود و ثغور مسئولیت سکوهای میزبانی، مشابه آنچه در قالب دکترین «بندر امن» در سایر سیستم‌های حقوقی پذیرفته شده است، به‌طور محسوسی زمینه‌ساز تشتّت در رویه قضائی می‌شود. نمونه بارز این وضعیت را می‌توان در آراء متفاوت صادرشده در مراحل مختلف رسیدگی به پرونده شکایت سازمان صدا و سیمای جمهوری اسلامی ایران علیه سکوی «آپارات» مشاهده کرد؛ جایی که برداشت‌های متفاوت قضات از حدود مسئولیت سکوی میزبانی، به نتایج کاملاً متعارض انجامیده است. در این پرونده، ابتدا دادگاه کیفری یک با استناد به نظر هیئت منصفه و به جهت عدم کفایت دلیل، حکم برائت صادر نمود؛ لیکن در پی فرجام‌خواهی، پرونده جهت رسیدگی مجدد به دادگاه کیفری دو ارجاع و این مرجع حکم به محکومیت سکو صادر کرد که در مرحله تجدیدنظر نیز تأیید شد. درنهایت با طرح درخواست اعمال ماده ٤٧٧ قانون آیین دادرسی کیفری و پذیرش آن، پرونده در دیوان عالی کشور مورد بازبینی قرار گرفت و رأی قطعی به نفع آپارات صادر گردید؛ فرایندی که طی حدود یک دهه رسیدگی، خود گویای تحول تدریجی نگرش قضائی نسبت به مسئولیت سکوهای میزبانی است. بروز چنین مواردی به روشنی ضرورت بازاندیشی در نظام مسئولیت سکوهای میزبانی را در حقوق ایران برجسته می‌سازد.

۲.۳. تفکیک مسئولیت سکوی دسترسی و سکوی میزبانی در قانون مجازات اسلامی

از میان انواع متنوع سکوهای فعال در فضای مجازی که در بخش مقدمه به آن‌ها اشاره شد، مهمترین سکوهای اینترنتی که در قانون مجازات اسلامی مورد توجه قانون‌گذار قرار گرفته‌اند، در دو دسته سکوهای دسترسی و سکوهای میزبانی قابل تفکیک هستند:

۱. سکوی دسترسی: این سکوها، همانند ارائه‌دهندگان خدمات میزبانی، وظیفه فراهم‌سازی امکان دسترسی کاربران به شبکه اینترنت یا فضای مجازی را برعهده دارند. در

آیین‌نامه قانون جمع‌آوری و استنادپذیری ادله الکترونیکی مصوب ۱۳۹۳، ارائه‌دهندگان خدمات دسترسی چنین تعریف شده‌اند: «اشخاصی هستند که امکان ارتباط کاربران با شبکه‌های رایانه‌ای یا مخابراتی و ارتباطی داخلی یا بین‌المللی یا هر شبکه مستقل دیگر را فراهم می‌آورند؛ از قبیل تأمین‌کنندگان، توزیع‌کنندگان، عرضه‌کنندگان خدمات دسترسی به شبکه‌های رایانه‌ای یا مخابرات». در معنای عام، ارائه‌دهندگان خدمات اینترنتی به شرکت‌هایی اطلاق می‌شود که نه‌تنها امکان دسترسی کاربران به اینترنت را فراهم می‌آورند، بلکه پس از اتصال به اینترنت، خدمات برخط متنوعی همچون رایانامه، جستجوی اینترنتی و سایر خدمات پایه را نیز در اختیار کاربران قرار می‌دهند *(ابهری و میری، ۱۳۹۰، ص. ۲)*.

۲. سکوی میزبانی: سکوهای میزبانی با فراهم‌سازی فضای ذخیره‌سازی داده‌ها و محتوای برخط، به کاربران اجازه می‌دهند محتوای خود را بارگذاری کنند؛ مانند سرورهای ارائه‌دهنده خدمات میزبانی وب. در آیین‌نامه قانون جمع‌آوری و استنادپذیری ادله الکترونیکی، ارائه‌دهندگان خدمات میزبانی این‌گونه تعریف شده‌اند: «اشخاصی هستند که امکان دسترسی کاربران به فضای ایجاد شده توسط سامانه‌های رایانه‌ای، مخابراتی و ارتباطی تحت تصرف یا کنترل خود را به کاربران واگذار می‌کنند تا رأساً یا توسط کاربر متقاضی، داده‌های رایانه‌ای را جهت نگهداری، انتشار، توزیع یا ارائه در شبکه‌های داخلی یا بین‌المللی یا هر منظور دیگر ذخیره یا پردازش کنند».

۳.۳. امکان‌سنجی اجرای دکترین «بندر امن» در ایران

با توجه به بررسی‌های پیشین درباره مبانی نظری و تطبیقی دکترین «بندر امن» اکنون می‌توان به این پرسش پرداخت که آیا اجرای چنین چهارچوبی در ایران امکان‌پذیر است و در صورت پاسخ مثبت، چه الزامات و پیش‌شرط‌هایی باید مورد توجه قرار گیرد؟

نخست، باید تأکید کرد که صرف اقتباس از مدل‌های خارجی، بدون لحاظ بستر نهادی، حقوقی و فنی ایران، نمی‌تواند منجر به تحقق مؤثر این دکترین بشود. ایران به‌عنوان کشوری درحال‌توسعه، با ظرفیت‌های محدود نظارتی، قضائی و فناورانه، نیازمند طراحی چهارچوبی بومی‌سازی‌شده و واقع‌بینانه است.

در گام نخست، قواعد مربوط به مسئولیت سکوها باید به‌صورت ساده، روشن و قابل

تفسیر تدوین شوند تا از قابلیت اجرای عملی برخوردار باشند. پیچیدگی بیش‌ازحد در مقررات مسئولیت، نه‌تنها به سردرگمی سکوها و نهادهای ناظر می‌انجامد بلکه احتمال اجرای سلیقه‌ای و سوءاستفاده از مقررات را نیز افزایش می‌دهد *(OECD, 2011, p.14)*. معافیت از مسئولیت نیز باید بر پایه معیارهایی مشخص و قابل اثبات، از جمله «عدم آگاهی واقعی از محتوای غیرقانونی» و «اقدام مؤثر پس از اطلاع»، تعریف شود.

علاوه‌براین، رعایت استانداردهای منعطفی همچون «متعارف بودن» در واکنش به محتوای غیرقانونی بالقوه، یا در مقابل، تجویز اقدامات مشخص و معین برای سکوها، از اهمیت بالایی برخوردار است. در عمل، غالباً هم سکوها و هم کاربران، رویکرد دوم را ترجیح می‌دهند؛ زیرا این شیوه موجب افزایش قابلیت پیش‌بینی و کاهش دامنه صلاحدید سکوها می‌شود (*Van Hoboken & Keller, 2019, p.6*). بااین‌حال، مقرراتی که به‌درستی تنظیم نشده باشند، ممکن است به حذف بیش از حد محتوا بینجامد. ازاین‌رو، سازوکارهای اخطار و حذف باید به‌گونه‌ای طراحی شوند که ضمن صیانت از منافع دارندگان حقوق، از حقوق کاربران در برابر حذف‌های خودسرانه نیز محافظت کنند. پیش‌بینی امکان اعتراض، بررسی مجدد و بازگردانی محتوا در صورت اشتباه، در این راستا ضرروی است.

از سوی‌دیگر، نقش فناوری‌های نوین، به‌ویژه سامانه‌های مبتنی بر هوش مصنوعی، در تسهیل اجرای مؤثر دکترین «بندر امن» نباید نادیده گرفته شود. استفاده از ابزارهای نیمه‌خودکار برای شناسایی اولیه محتوای غیرقانونی می‌تواند سرعت و کارایی فرایند «اخطار و حذف» را افزایش داده و نیاز به مداخله نیروی انسانی را کاهش دهد *(Cambridge Consultants, 2023, p.46)*. بااین‌حال، مطابق با رهنمودهای بین‌المللی، این ابزارها نباید جایگزین کامل تشخیص انسانی شوند. حفظ توازن میان نظارت ماشینی و داوری انسانی، تضمین‌کننده رعایت حریم خصوصی، جلوگیری از حذف بیش‌ازحد محتوا و پاسداری از آزادی بیان در فضای دیجیتال است.

یکی دیگر از الزامات کلیدی اجرای موفق دکترین «بندر امن»، طراحی سازوکارهای حل‌وفصل اختلافات با مشارکت واقعی ذی‌نفعان است. مشارکت کاربران، نهادهای تخصصی، بخش خصوصی و جامعه دانشگاهیان در فرایند تدوین مقررات و نظارت بر

اجرا، علاوه بر افزایش مشروعیت تصمیمات، به ارتقای کیفیت و کارآمدی سیاست‌ها و بازسازی اعتماد عمومی کمک می‌کند (*Tworek et al., 2020, p.2*). درهمین‌راستا، ایجاد نهادهای مستقل و تخصصی برای رسیدگی به اختلافات ناشی از حذف محتوا یا تعیین حدود مسئولیت سکوها، می‌تواند مانع از اعمال سلیقه فردی یا تأثیرپذیری از فشارهای بیرونی شود. این نهادها باید دارای اختیارات مشخص، رویه‌های شفاف و امکان دسترسی آسان برای طرفین باشند و تصمیمات آن‌ها نیز قابلیت بازبینی قضائی باشد. چنین ساختاری، علاوه بر تضمین بی‌طرفی و پاسخ‌گویی، اعتماد عمومی به نظام تنظیم‌گری فضای مجازی را تقویت خواهد کرد.

افزون‌براین، حمایت از سکوهای داخلی و نوپا باید به‌عنوان بخشی از سیاست تنظیم‌گری مورد توجه قرار گیرد. اجرای یک‌دست و سخت‌گیرانه مقررات، بدون توجه به تفاوت در مقیاس و ظرفیت سکوها می‌تواند به انحصار سکوهای بزرگ و تضعیف رقابت سالم منجر شود. ازاین‌رو، اعمال قواعد متناسب با نوع فعالیت و اندازه سکوها، به‌ویژه از طریق استانداردهای طبقه‌بندی‌شده، ضروری به‌نظر می‌رسد.

درنهایت، سیاست‌گذاری در این حوزه باید در تعامل مستمر با تجربیات بین‌المللی و در چهارچوب همکاری‌های فنی، آموزشی و مقررات‌گذاری با نهادهای تخصصی منطقه‌ای و جهانی انجام گیرد. چنین همکاری‌هایی می‌تواند در انتقال دانش، تدوین استانداردها و ارتقای ظرفیت نهادی نقش مؤثری ایفا کند.

در پایان، با وجود آنکه دکترین «بندر امن» خالی از ایراد و چالش نیست و در نظام‌های حقوقی پیشرو نیز با نقدها و محدودیت‌هایی مواجه بوده است، با لحاظ خلأها و کاستی‌های موجود در چهارچوب حقوقی ایران در زمینه تنظیم مسئولیت سکوها، بهره‌گیری از این رویکرد می‌تواند به‌عنوان نقطه آغازین مناسبی برای سامان‌دهی این حوزه تلقی شود؛ مشروط بر آنکه اجرای آن با رویکردی تدریجی، اصلاح‌پذیر و مبتنی بر بومی‌سازی مقررات در پرتو تحولات فناورانه و مقتضیات نهادی کشور همراه باشد. به‌بیان‌دیگر، کارآمدی این دکترین در نظام حقوقی ایران نه در پذیرش مطلق آن، بلکه در انطباق سنجیده و ارتقای تدریجی آن متناسب با نیازهای داخلی قابل تحقق خواهد بود؛ چنان‌که حضرت

سعدی نیز در بیان حکمت عملی این مسیر می‌فرماید:

به راه بادیه رفتن، به از نشستن باطل که گر مراد نیابم، به قدر وسع بکوشم

نتیجه‌گیری

با توجه به ماهیت فرامرزی فضای مجازی، رویکرد قانون‌گذار ایران ناگزیر باید به استانداردهای بین‌المللی نزدیک باشد. در این‌راستا، مطالعه دقیق رویه‌ها، قوانین و آرای قضائی سیستم‌های حقوقی پیشرفته، مسیر مطمئنی برای تفسیر و اعمال قواعد داخلی در چهارچوبی هماهنگ با استانداردهای جهانی فراهم می‌آورد.

مطالعه تطبیقی سیستم‌های حقوقی ایالات متحده و اتحادیه اروپا نشان می‌دهد که دکترین «بندر امن» به‌عنوان یک نهاد حقوقی شناخته‌شده، با تعیین معیارهای روشن برای مسئولیت سکوها، امکان رشد سکوهای مبتنی بر مشارکت کاربران را بدون تحمیل مسئولیت‌های نامتعارف فراهم کرده است. این دکترین، ضمن حفظ آزادی‌های مشروع کاربران، مسئولیت ارائه‌دهندگان خدمات اینترنتی را به موارد آگاهانه و همراه با سوءنیت محدود می‌سازد.

یافته‌های این پژوهش نشان می‌دهد که قوانین موجود در ایران در مواجهه با مسائل نوظهور، به‌ویژه در زمینه مسئولیت سکوهای میزبانی محتوا، از کارآمدی لازم برخوردار نیستند. ازاین‌رو ضرورت تدوین قوانین تخصصی و بازنگری جامع در مقررات فعلی بیش از پیش احساس می‌شود. ایجاد چهارچوبی منسجم و کارآمد، ضمن کاهش نگرانی‌های اجتماعی و پیشگیری از جرایم رایانه‌ای و نقض حقوق مالکیت فکری، می‌تواند امنیت حقوقی سکوها را تقویت کرده و زمینه افزایش سرمایه‌گذاری در این حوزه را فراهم آورد.

به‌عنوان ماحصل نهایی این پژوهش، باید تأکید نمود که در فرایند تقنین، اقتباس چشم‌بسته از مدل‌های خارجی، بدون توجه به بستر نهادی، حقوقی و فنی ایران، نمی‌تواند اثربخش باشد. ایران به‌عنوان کشوری درحال‌توسعه، نیازمند طراحی چهارچوبی بومی‌سازی‌شده و واقع‌بینانه است که در عمل نیز از قابلیت اجرا برخوردار باشد.

در این‌راستا، رعایت مجموعه‌ای از ملاحظات اساسی ضروری است؛ ازجمله آنکه: یکم، قواعد مربوط به مسئولیت سکوها باید به‌صورت ساده، شفاف و قابل تفسیر تدوین شوند.

دوم، معافیت از مسئولیت بر مبنای معیارهای مشخص و اثبات‌پذیر، همچون عدم آگاهی واقعی از محتوای غیرقانونی و اقدام مؤثر و به‌موقع پس از اطلاع، تعریف گردد. سوم، استانداردهای منعطفی نظیر «متعارف بودن» در واکنش به محتوای غیرقانونی بالقوه، یا درمقابل، اقدامات مشخص و معین برای سکوها، به‌طوردقیق ترسیم شده و از تفسیر موسع ممانعت به‌عمل آید تا از حذف خودسرانه و بی‌محابای محتوا محافظت شود. چهار، امکان اعتراض، بررسی مجدد و بازگردانی محتوا درصورت اشتباه در تصمیم‌گیری پیش‌بینی شود. پنج، نقش فناوری‌های نوین، به‌ویژه سامانه‌های مبتنی بر هوش مصنوعی، در تسهیل اجرای مؤثر دکترین «بندر امن» ملحوظ نظر قرار گیرد. شش، استفاده از ابزارهای نیمه‌خودکار برای شناسایی اولیه محتوای غیرقانونی، ضمن افزایش سرعت و کارایی فرایند «اخطار و حذف»، احتمال بروز خطای انسانی را کاهش می‌دهد. هفت، سازوکار حل‌وفصل اختلافات با مشارکت واقعی ذی‌نفعان و با حداقل زمان ممکن طراحی گردد. هشت، حمایت از سکوهای داخلی و نوپا به‌عنوان یک سیاست حمایتی در دستور کار قرار گیرد تا از انحصارگرایی سکوهای بزرگ و تضعیف رقابت سالم جلوگیری شود.

درنهایت، سیاست‌گذاری در این حوزه باید در تعامل مستمر با تجربیات بین‌المللی و در چهارچوب همکاری‌های فنی، آموزشی و مقررات‌گذاری با نهادهای تخصصی منطقه‌ای و جهانی صورت گیرد تا ضمن انتقال دانش و ارتقای ظرفیت نهادهای داخلی، به طراحی هوشمندانه سازوکارهای اجرایی و توسعه پایدار زیست‌بوم دیجیتال کشور کمک کند.

منابع

ابهری، حمید و میری، حمید (۱۳۹۰). مطالعه تطبیقی مبانی مسئولیت مدنی ارائه‌کنندگان خدمات اینترنتی. پژوهش‌های حقوق تطبیقی. ۳(۷۳)، ۲۰-۱.

حاجی ده‌آبادی، محمدعلی و سلیمی قلعه، احسان و دهقانی، پرویز (۱٤۰۱). پالایش محتوا در سنجه حق‌های بنیادین و رهیافت‌های جرم‌شناختی؛ نقد وضع موجود و درآمدی بر وضعیت مطلوب. دوفصلنامه علمی حقوق فناوری‌های نوین. ۳(٦)، ۷۷-۹٤.
https://doi.org/10.22133/mtlj.2022.363418.1125

رمضانیان سیاهکلرودی، عباس؛ دیانی، عبدالرسول و زرکلام، ستار (۱۳۹۹). مسئولیت مدنی واسطه‌های ارائه خدمات اینترنتی با تأکید بر نقض مالکیت فکری در فضای سایبر. دوفصلنامه علمی مطالعات حقوق بشر اسلامی. ۹(۱)، ۲۷۷-۲۹۷.

کریم‌میان، زهره (۱٤۰٤). چهارچوبی برای مسئولیت پلتفرم‌های آنلاین مبادله‌ای متناسب با ماهیت آن‌ها. فصلنامه سیاست علم و فناوری. ۱۸(۱)، ۸۲-٦۹.

https://doi.org/10.22034/jstp.2025.11801.1829

نجفی ابرندآبادی، علی حسین، رضوانی، سودابه، (۱۳۹٤)، سلب آزادی پیشگیری محور با تأکید بر ماده ۱۵۰ قانون مجازات اسلامی ۱۳۹۲. فصلنامه پژوهش حقوق کیفری. ٤(۱۲)، ٤۲-۹.

https://doi.org/10.22054/jclr.2015.178029

Angelopoulos, C. (2016). *European intermediary liability in copyright: A tort-based analysis*. The Netherlans: Wolters Kluwer.

Batura, O. (2020). *Study on redefining 'hosting' under article 14 of the e Commerce Directive*. Rotterdam: Rotterdam.

Cambridge Consultants. (2023). *Use of AI in online content moderation*. United Kingdom: Ofcom.

Capitol Records, LLC v. Vimeo, LLC, 826 F.3d 87 (2d Cir. 2016).

Farano, B. (2012). *Internet intermediaries' liability for copyright and trademark infringement: Reconciling the EU and US Approaches*. TTLF Working Papers, No. 14, Stanford-Vienna Transatlantic Technology Law Forum.

Gellert, R. M. & Wolters, P. T. J. (2021). *The revision of the European framework for the liability and responsibilities of hosting service providers*. Permanent Representation of the Netherlands to the European Union.

Human Rights Council. (2016). *Resolution adopted by the Human Rights Council on 1 July 2016: The promotion, protection and enjoyment of human rights on the Internet* (A/HRC/32/L.20). United Nations.

Io Group, Inc. v. Veoh Networks, Inc., 586 F. Supp. 2d 1132 (N.D. Cal. 2008).

Krokida, Z. (2022). *Internet service provider liability for copyright and trade mark infringement: Towards an EU co-regulatory framework*. United Kingdom: Hart Publishing.

L'Oréal v. eBay, C-324/09 (Court of Justice of European Union. 2011)

Madiega, T. (2020). *Reform of the EU liability regime for online intermediaries: Background on the forthcoming digital services act*. Brussels: European Union.

OECD. (2011). *The role of Internet intermedies in advancing public policy objectives*.

Paris: OECD Publishing.
Online Policy Group v. Diebold, Inc., 337 F. Supp. 2d 1195 (N.D. Cal. 2004).
Religious Technology Center v Netcom On-Line Communication Services, Inc., 907 F. Supp. 1361 (N.D. Cal. 1995).
Rossi v. Motion Picture Ass'n of America Inc., 391 F.3d 1000 (9th Cir. 2004).
Smith, C.Y (2020). Creative destruction: Copyright's fair use doctrine and the moral right of integrity. *Pepperdine Law Review* (Vol. 47). 601-664.
Square Ring, Inc. v. UStream.com, 2015 WL 307840 (D. Del. 2015).
Tworek, H.; Ó Fathaigh, R.; Bruggeman, L. & Tenove, C. (2020). *Dispute resolution and content moderation: Fair, accountable, independent, transparent, and effective*. Transatlantic Working Group on Content Moderation Online and Freedom of Expression working paper.
U.S. Copyright Office. (2020). *Section 512 of title 17: A report of the Register of Copyrights*. Washington, D.C.: U.S. Copyright Office.
Urban, J.M., & Quitler, L. (2006). Efficient Process or "Chilling Effects"? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act. *Santa Clara High Tech Law Journal* (Vol. 22). 621-693.
Urban, J.M., Karaganis, J., & Schofield, B.L. (2017). Notice and Takedown: Online Service Provider and Rightsholder Accounts of Everyday Practice. *Journal of Copyright Society of the USA* (Vol.64). 371-410.
Van Hoboken, J., & Keller, D. (2019). *Design principles for intermediary liability laws*. Institute for Information Law (IViR) & Stanford Center for Internet and Society.
Van Hoboken, J.; Quintais, J.; Poort, J. & Van Eijk, N. (2018). *Hosting intermediary services and illegal content online: An analysis of the scope of Article 14 ECD in light of developments in the online service landscape*. Luxembourg: Publications Office of the European Union.
Viacom International, Inc. v. YouTube, Inc., 676 F.3d (2d Cir. 2012).
Wang, J. (2018). *Notice-and-takedown procedures in the US, the EU, and China. In Regulating Hosting ISPs' Responsibilities for Copyright Infringement: The Freedom to Operate in the US, EU, and China*. Singapore: Springer Publishing.
Ward, A. M. (2012). *The "Viacom v YouTube" Litigation and Section 512 (c) DMCA: When the Safe Harbour Becomes a Permanent Mooring. In Google and the Law: Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models*. The Netherlands: TMC Asser Press.
Wilman, F. (2020). *The responsibility of online intermediaries for illegal user content in the EU and the US*. Edward Elgar Publishing.
Wilman, F. (2022). *The Digital Services Act (DSA) – An Overview*. Available at SSRN 4304586.
Wilman, F.; Kalėda, S.L, & Loewenthal, P-J. (2024). *The EU Digital Services Act: A Commentary*. United Kingdom: Oxford Publishing.