Insights of Intellectual Property Law in Islamic Countries
Online ISSN: 3060-5997
https://diplic.qom.ac.ir

The Capacity of Human Rights Governance in Digital Space in Response to Crimes Committed on Digital Platforms, with a Study of the Intellectual Property Framework of the Malaysian Legal System

Peyman Namamian [1]

1. Associate Professor of Criminal Law and Criminology, Faculty of Administrative Sciences and Economics, Arak University, Arak, Iran (Corresponding author), Email: p-namamian@araku.ac.ir

Abstract

Received: 18/02/2026
Revised: 07/05/2026
Accepted: 01/06/2026
Published online: 22/06/2026

The digital environment, notwithstanding its considerable benefits for communication and information dissemination, has generated a range of novel human-rights challenges. Manifestations of these challenges, most notably privacy intrusions, constraints on freedom of expression, and algorithmic discrimination demonstrate the structure for legal regimes to adapt promptly and effectively to the complex realities of cyberspace. Security based approaches frequently restrict fundamental freedoms rather than preserve them. It is essential to develop calibrated and proportionate legal mechanisms that protect citizens' rights online. Such mechanisms must enable robust enforcement against cybercrime while simultaneously preserving a safe, open, and dynamic digital environment. A comprehensive regulatory approach that foregrounds both preventive and protective measures is necessary to ensure that technological tools do not become instruments for the erosion of fundamental rights. Striking a sustainable balance between public security and human dignity should inform future policy development in this area. The rise of new information technologies and the expansion of digital platforms have also created significant intellectual-property challenges, particularly in jurisdictions such as that of Malaysia. The widespread online copyright infringement and trademark misuse indicates that existing legal frameworks are increasingly inadequate. Legislative and regulatory reform is therefore required to secure the rights of creators and right-holders in the digital sphere while preserving reasonable public access to knowledge and information.

Keywords: Digital Crimes, Human Rights Governance of Digital Space, Freedom of Expression and Privacy, Rights of Digital Creators, Malaysian Law.

How To Cite: Namamian, P. (2026). The Capacity of Human Rights Governance in Digital Space in Response to Crimes Committed on Digital Platforms, with a Study of the Intellectual Property Framework of the Malaysian Legal System, *Insights of Intellectual Property Law in Islamic Countries*, 2(2), 108-131. https://www.doi.org/10.22091/diplic.2026.15789.1046

Published by: University of Qom **© The Author(s)** **Article type: Research**

آموزه‌های حقوق مالکیت فکری کشورهای اسلامی
https://diplic.qom.ac.ir
شاپا الکترونیکی: ۳۰۶۰-۵۹۹۷

ظرفیت حکمرانی حقوق بشر فضای دیجیتال در پاسخ به جرائم ارتکابی در سکوهای دیجیتالی با مطالعه چارچوب حمایت نظام حقوقی مالزی از پدید آورندگان آثار دیجیتالی

پیمان نمامیان[1]

۱. دانشیار حقوق کیفری و جرم شناسی، دانشکده علوم اداری و اقتصاد، دانشگاه اراک، اراک، ایران (نویسنده مسئول)، رایانامه: p-namamian@araku.ac.ir

چکیده

فضای دیجیتال، با تمام مزایایی که در تسهیل ارتباطات به ارمغان آورده است، بستری برای بروز چالش‌های نوین حقوق بشری نیز گردیده است. مسائلی چون نقض حریم خصوصی، محدودیت‌های اعمال شده بر آزادی بیان و تبعیض‌های ناشی از الگوریتم‌ها، ضرورت انطباق سریع و مؤثر قوانین با واقعیت‌های پیچیده فضای دیجیتالی را گوشزد می‌کنند. رویکردهای صرفاً امنیتی، گاه به جای پاسداری از حقوق، به محدودیت آزادی‌های اساسی منجر می‌شوند. در این میان، تدوین سازوکارهای هوشمند و متعادل برای صیانت از حقوق شهروندی در فضای مجازی، امری حیاتی است. این سازوکارها باید قادر باشند ضمن مقابله مؤثر با جرائم دیجیتالی، فضایی امن، آزاد و پویا را برای کاربران تضمین نمایند. اتخاذ رویکردی جامع که بر جنبه‌های پیشگیرانه و حفاظتی تأکید دارد، اساس پیشگیری از تبدیل فناوری به ابزاری برای تضییع حقوق اساسی است. دستیابی به توازنی پایدار میان امنیت عمومی و کرامت انسانی، سنگ بنای سیاست‌گذاری‌های آتی در این حوزه خواهد بود. ظهور فناوری‌های نوین اطلاعاتی و گسترش سکوهای دیجیتال، چالش‌های حقوقی تازه‌ای را در حوزه مالکیت فکری، به ویژه در کشورهایی چون مالزی پدید آورده است. رواج گسترده نقض حقوق مؤلف و سوءاستفاده از علائم تجاری در فضای دیجیتالی، نیاز مبرم به بازنگری و اصلاح قوانین موجود را آشکار می‌سازد. هدف نهایی، صیانت مؤثر از حقوق پدیدآورندگان آثار و حقوق مالکیت فکری در فضای دیجیتالی، ضمن حفظ تعادل با دسترسی عمومی به دانش و اطلاعات است.

واژگان کلیدی: جرائم دیجیتالی، حکمرانی حقوق بشر فضای دیجیتال، آزادی بیان و حریم خصوصی، حقوق پدیدآورندگان فضای دیجیتالی، حقوق مالزی.

تاریخ دریافت: ۱۴۰۴/۱۱/۲۹
تاریخ اصلاح: ۱۴۰۵/۰۲/۱۷
تاریخ پذیرش: ۱۴۰۵/۰۳/۱۱
تاریخ انتشار برخط: ۱۴۰۵/۰۴/۰۱

استناد: نمامیان، پیمان (۱۴۰۵). ظرفیت حکمرانی حقوق بشر فضای دیجیتال در پاسخ به جرائم ارتکابی در سکوهای دیجیتالی با مطالعه چارچوب حمایت نظام حقوقی مالزی از پدید آورندگان آثار دیجیتالی، آموزه‌های حقوق مالکیت فکری کشورهای اسلامی، ۲(۲)، ۱۳۱-۱۰۸.
https://www.doi.org/ 10.22091/diplic.2026.15789.1046

ناشر: دانشگاه قم
© **نویسندگان**
نوع مقاله: پژوهشی

مقدمه

فناوری‌های دیجیتال به سرعت در حال تحول شرایط زندگی انسان‌ها هستند. امروزه تقریباً همه زمینه‌های روابط اجتماعی، اعم از در سطح داخلی و بین‌المللی، در حال دیجیتال شدن و استفاده از فناوری‌های جدید هستند. شورای امنیت سازمان ملل متحد در قطعنامه‌های ۲۴۱۹ (۲۰۱۸)، ۲۴۶۲ (۲۰۱۹) و ۲۴۹۰ (۲۰۱۹) به این نکته اشاره کرده است که فعالیت‌های دیجیتال افراد و نهادهای غیردولتی می‌تواند تهدیدی برای صلح و امنیت جهانی به‌حساب آید. این تهدیدات می‌تواند شامل حملات دیجیتالی به زیرساخت‌های حیاتی، اختلال در دسترسی به سامانه‌های پرداخت برخط، انسداد دسترسی به اینترنت و حساب‌های کاربری شبکه‌های اجتماعی نظیر توییتر و اینستاگرام باشد. ازاین‌رو، استفاده از فناوری‌های نوین ارتباطات و اطلاعات توسط افراد و سازمان‌های غیردولتی ممکن است به تهدیدی جدی برای امنیت جهانی تبدیل شود.[۱]

فناوری‌های دیجیتال امکانات جدیدی را برای حمایت از حقوق بشر فراهم کرده‌اند و بر تمامی ابعاد آن، ازجمله حقوق مدنی، سیاسی، فرهنگی، اقتصادی و اجتماعی، تأثیرگذارند. این فناوری‌ها به‌طور عمده روش‌های دسترسی به اطلاعات، به اشتراک‌گذاری آن، شکل‌دهی به نظرات عمومی، تبادل اندیشه‌ها و سازماندهی فعالیت‌های اجتماعی را تغییر داده‌اند. با این حال، این ابزارها تنها به تقویت آزادی‌ها کمک نکرده‌اند، بلکه در مواردی برای سرکوب، تحدید و نقض حقوق بشری نیز سوءاستفاده می‌شوند. استفاده نادرست از فناوری‌های دیجیتال به‌ویژه بر اقشار حاشیه‌ای و آسیب‌پذیر تأثیرات منفی داشته و می‌تواند موجب تشدید نابرابری و تبعیض، اعم از فضای حقیقی و واقعی، گردد.[۲]

در عصر دیجیتال تضمین حقوق بشر با چالش‌های نوینی نظیر حفظ حریم خصوصی، امنیت داده‌ها و مدیریت توازن میان آزادی بیان و ضرورت‌های امنیتی مواجه است. دسترسی آزاد به اطلاعات و تقویت دموکراسی، در کنار خطراتی همچون نفرت‌پراکنی و جرائم دیجیتالی، نیازمند چارچوب‌های قانونی کارآمد است. با وجود تلاش‌های برخی کشورها برای وضع مقررات حفاظتی، همچنان فقدان یک سند هنجاری جامع و هم‌راستایی بین‌المللی در مقررات، اجرای عدالت را با مانع روبه‌رو کرده است. اگرچه اسناد بین‌المللی بنیادین و کنوانسیون‌های منطقه‌ای موجود، بستری برای صیانت از آزادی‌های فردی فراهم آورده‌اند، اما

---

۱. تهدیدهای امنیت دیجیتال می‌تواند شامل ویروس‌های رایانه‌ای، هرزنامه، سرقت هویت، نقض داده‌ها، حمله‌های انکار سرویس و جرائم دیجیتالی باشد؛ مهاجمان می‌توانند از هکرها گرفته تا فعالان، مجرمان کوچک، کسب و کارها و دولت‌های ملی را شامل شود.

2. . https://www.ohchr.org/en/topic/digital-space-and-human-rights

پیشرفت‌های سریع فناوری، خلأهای جدی ایجاد کرده است. بر این اساس، تدوین قوانین هماهنگ جهانی، توسعه زیرساخت‌های قضائی و افزایش آگاهی عمومی، راهکارهای ضروری برای حفاظت از کرامت انسانی در فضای مجازی و انطباق نظام‌های حقوقی فعلی با اقتضائات زیست‌بوم دیجیتال به شمار می‌روند.

تجاوز به حقوق خالقان آثار و اشاعه غیرقانونی محتوا در بسترهای دیجیتال، تقابلی اساسی میان حقوق مالکیت فکری و دسترسی همگانی به اطلاعات و فرهنگ پدید آورده و بر چالش‌های موجود در فضای دیجیتال افزوده است. کشورهای اسلامی با استناد به مبانی فقهی «لاضرر» و «حق‌الناس»، رویکردی متعادل را اتخاذ کرده‌اند؛ رویکردی که ضمن صیانت از حقوق مادی و معنوی پدیدآورندگان در گستره فضای دیجیتالی، دسترسی عادلانه به میراث علمی و هنری را نیز تضمین می‌نماید. این توازن که با هدف ارتقاء عدالت فرهنگی و حمایت از نوآوری صورت می‌گیرد، در سطح بین‌المللی مستلزم اتخاذ راهبردهای جامع و هم‌راستا با هنجارهای جهانی و ارزش‌های بومی است (ر.ک: شاکری، ۱۴۰۳: ۲۴۸-۲۴۷). در این راستا، در این میان، تجربه مالزی به‌عنوان یک الگوی مطالعاتی موفق، نشان می‌دهد که تلفیق موازین حقوق بشری با آموزه‌های اسلامی می‌تواند راهکاری کارآمد برای مدیریت پیچیدگی‌های حوزه مالکیت فکری و مقابله با جرائم دیجیتالی در عصر دیجیتال باشد.[1]

این پژوهش به تحلیل و بررسی تأثیر اصول و موازین حقوق بشری در فضای دیجیتال و چالش‌های ناشی از گسترش فناوری‌های نوین اختصاص دارد. با توجه به رشد روزافزون سکوهای دیجیتال، فضای برخط به بستری نوین برای ارتکاب جرائم دیجیتال تبدیل شده است که شامل مسائلی همچون نقض حریم خصوصی، تهدید آزادی بیان و تبعیض دیجیتال است. در این راستا، پرسش اصلی پژوهش این است که «آیا اصول حقوق بشری که در گذشته و بر اساس شرایط فیزیکی و جغرافیایی جوامع تدوین شده‌اند، قادر به تأمین و حفاظت مؤثر از حقوق فردی در قبال تهدیدات فضای دیجیتال هستند؟» ازاین‌رو، هدف تحقیق تحلیل ظرفیت موازین حقوق بشری در انطباق با چالش‌های حقوقی فضای دیجیتال و بررسی ضرورت تدوین رویکردهای نوین برای حمایت از حقوق فردی در این فضا است. افزون بر این، پژوهش حاضر به بررسی موضوع حکمرانی دیجیتال و ضرورت ایجاد ساختاری مؤثر برای برقراری تعادل میان آزادی‌های فردی و امنیت عمومی می‌پردازد و بر این اساس الگوهای نوین حکمرانی حقوق بشر در فضای دیجیتال را مورد مداقه و سنجش قرار خواهد

1. Cyber Security Malaysia (2020). Cybersecurity Incidents and Trends in Malaysia. Vol.
1. https://www.cybersecurity.my/data/content_files/46/2222.pdf

داد. در این زمینه، نحوه هماهنگی میان حقوق بشر، فناوری و حاکمیت مورد بررسی قرار خواهد گرفت. این تحقیق از روش تحلیلی‌توصیفی بهره خواهد برد تا ضمن بررسی چارچوب‌های حقوق بشری موجود، قابلیت آن‌ها را در مواجهه با چالش‌های دیجیتال ارزیابی کرده و الگوهای نوآورانه برای حکمرانی حقوق بشری در فضای برخط پیشنهاد نماید. افزون بر این، پژوهش بر لزوم تطبیق اصول حقوق بشری با تحولات فضای دیجیتال و ایجاد رویکردهای نوین برای مقابله با نقض حقوق بشر در دنیای برخط تأکید دارد. پژوهش به‌ویژه به ضرورت تدوین قوانین بین‌المللی و همکاری‌های جهانی برای ایجاد تعادل میان حفظ آزادی‌های فردی و تأمین امنیت عمومی در فضای مجازی اشاره می‌کند. در ضمن، هدف اصلی این پژوهش ارائه راه‌حل‌های عملی برای بهبود حکمرانی حقوق بشر در دنیای دیجیتال است.

۱. پیشینه و تحولات رفتاری

در اوایل دهه ۱۹۸۰، با آغاز عصر رایانه، سازمان‌های مجری قانون نگرانی‌های فزاینده‌ای را نسبت به کمبود قوانین کیفری برای مقابله با جرائم رایانه‌ای نوظهور تجربه کردند. البته جرائم دیجیتال از دهه ۱۹۶۰ تا به امروز تحولات بسیاری داشته‌اند. در اوایل توسعه سامانه‌های اطلاعاتی، این جرائم عمدتاً توسط برخی از کارکنان سامانه‌ها صورت می‌گرفت و حملات فیزیکی به سامانه‌های رایانه‌ای در دوره ۱۹۶۰ تا ۱۹۸۰ شایع بود. همچنین، از سال ۱۹۸۰ به بعد، نرم‌افزارهای مخرب (ویروس‌ها و تروجان‌ها) به‌طور خاص علیه رایانه‌های شخصی آغاز به ظهور کردند (Jarrett and Bailie, 2011: 21).

در اوایل دهه ۱۹۹۰، اینترنت به یک عامل اساسی در رشد جرائم دیجیتال تبدیل شد. مجرمان با بهره‌گیری از روش‌های غیرمجاز و به‌طور معمول با هدف دستیابی به منافع مالی، به سامانه‌های آسیب‌پذیر نفوذ می‌کردند. به‌عنوان مثال، کلاهبرداری با کارت‌های اعتباری در میانه دهه ۱۹۹۰ به‌طور چشمگیری افزایش یافت. با پایان قرن بیستم و آغاز قرن بیست‌ویکم، این نوع کلاهبرداری‌ها تحت عنوان سرقت هویت قرار گرفت، جایی که مجرمان هویت افراد دیگر را برای انجام فعالیت‌های غیرقانونی می‌دزدیدند. تا سال ۲۰۰۸، سرقت هویت به سریع‌ترین نوع کلاهبرداری تبدیل شد. در سال‌های اخیر، جرائم مرتبط با تلفن‌های همراه نیز روندی رو به رشد داشته است (Kabay, 2008: 78). به‌علاوه، امروزه شاهد ظهور انواع جدیدی از فعالیت‌های مجرمانه هستیم که می‌توان آن‌ها را در قالب چهار نوع جرم مختلف دسته‌بندی کرد: الف. رایانه به‌عنوان هدف جرم، مانند زمانی که خود دستگاه رایانه به سرقت می‌رود؛ ب. رایانه به‌عنوان موضوع جرم، به این معنا که رایانه محیط وقوع جرم است؛ ج. استفاده از رایانه به‌عنوان ابزاری برای ارتکاب جرم، مانند نفوذ

به سامانه‌های دیگر برای انجام اقدامات غیرقانونی؛ د. استفاده از نمادهای رایانه‌ای برای انجام فعالیت‌های غیرقانونی (Casey, 2011: 186).

از زمان ظهور جرائم دیجیتال، این جرائم به سه نسل عمده تقسیم شده‌اند. نسل اول که در دهه‌های ۱۹۶۰ تا اوایل ۱۹۸۰ میلادی شکل گرفت، بر اساس استفاده از خود رایانه به‌عنوان ابزار جرم تعریف می‌شد و انواع جرائم آن محدود به تخلفات ساده بود. نسل دوم در دهه ۱۹۸۰ تا اوایل ۱۹۹۰ میلادی ظهور کرد و تمرکز آن بر داده‌ها و اطلاعات بود که تحت عنوان «جرائم مرتبط با داده‌ها» شناخته می‌شود. نسل سوم نیز از اواخر دهه ۱۹۹۰ به بعد به وجود آمد و به «جرائم مجازی» معروف است، جایی که با ترکیب رایانه‌ها و فناوری‌های پیشرفته مخابراتی و شبکه‌های ارتباطی، فضای مناسبی برای ارتکاب جرائم پیچیده فراهم شد. درحالی‌که در ابتدا، جرائم دیجیتال محدود و به تعداد کمی از تخلفات اختصاص داشت، امروزه فضای مجازی محل وقوع پنج دسته اصلی از جرائم است که هرکدام شامل ده‌ها نوع مختلف از فعالیت‌های غیرقانونی بوده و مجموعاً بیش از دویست نوع جرم را شامل می‌شود (شیرزاد، ۱۳۸۸: ۳۹).

در دهه گذشته شاهد افزایش جهانی در تعداد حقوق حاکم بر اینترنت و حوزه دیجیتال بودیم. با توسعه و گسترش سریع اینترنت در آغاز این قرن، قانون‌گذاران در سراسر جهان در قبال خلأ قانونی که با مقررات قانونی موجود قابل پر کردن نبود، لازم بود حوزه دیجیتال را با حقوق و مقررات ملی خاص تنظیم کنند. به‌عنوان مثال، اخیراً «قانون اجرای شبکه»[1] در آلمان و «قانون مبارزه با نفرت در اینترنت»[2] در فرانسه به تصویب رسید که هر دو وظیفه بحث‌برانگیز سکوهای برخط برای حذف محتوای غیرقانونی خاص را تدوین می‌کنند. در عین حال، اتحادیه اروپا در حال کار بر روی یک قانون خدمات دیجیتال پس از تصویب «مقررات عمومی حفاظت از داده‌ها»[3] است و از سال ۲۰۱۸ اجرا شده است.[4]

1. Netzwerkdurchsetzungsgesetz of 1 September 2017 (BGBl.I p. 3352), which was changed by Article 274 of the Decree of 19 June 2020 (BGBl.I p. 1328).
2. Assemblée nationale, proposition de loi visant à lutter contre les contenus haineux sur internet, loi n° 2020–766 de 24 juin 2020.
3. European Commission, 'The Digital Services Act package,' available at: https://dig ital-strategy.ec.europa.eu/.

٤. لازم به ذکر است اتحادیه اروپا سند بین‌المللی «مقررات عمومی حفاظت از داده‌ها» را به‌عنوان جایگزینی جامع برای «قانون حفاظت از دادهٔ اتحادیهٔ اروپا» در آوریل سال ۲۰۱۶ تنظیم کرد که در ۲۵ می ۲۰۱۸ از سوی پارلمان اروپا تصویب و لازم‌الاجرا شد (قناد و شریف، ۱۴۰۰: ۱).

۲. چالش‌های حقوقی در حکمرانی و الزامات همکاری‌های بین‌المللی

رشد سریع فناوری اطلاعات و ارتباطات منجر به تغییرات چشمگیر در حوزه‌های سیاسی، امنیتی، اقتصادی و اجتماعی جوامع گردیده است. در این چارچوب که به‌عنوان فضای مجازی شناخته می‌شود، تهدیدهای نوینی نظیر جنگ مجازی (عسکری، ۱۴۰۱: ۲۴۵-۲۴۰)، جنگ‌های اطلاعاتی، جرائم دیجیتال،[۱] حملات هکری و سرقت اطلاعات محرمانه نهادهای امنیتی و اطلاعاتی پدید آمده است که امنیت ملی کشورها را به شکل جدی تهدید می‌نماید.

فضای بی‌مرز دیجیتال، جهانی موازی با جهان فیزیکی را به وجود آورده است که در واقع کنترل و ادارهٔ حقوقی آن از حیطهٔ اعمال قدرت یک حاکمیت برنمی‌آید. بنابراین، برای حکمرانی بر این فضا و مقابله با جرائم روزافزون و پیچیدهٔ ارتکابی در فضای دیجیتال همکاری و معاضدت جامعهٔ بین‌المللی برای قاعده‌مندی نیاز است، به‌گونه‌ای که هیچ مجرمی بدون مجازات نماند و این مهم به دست نمی‌آید، مگر با تدوین مقررات هماهنگ و متحدالشکل؛ زیرا جرائم ارتکابی در فضای دیجیتال مرزهای جغرافیایی و سنتی را پشت سر می‌گذارند و به سبب ویژگی‌هایی که دارند، می‌توان برخی از این‌گونه جرائم را در زمرهٔ آن دسته جرائمی به شمار آورد که برای مقابله با آن‌ها اعمال صلاحیت جهانی ضرورت دارد (جلالی و توسلی‌اردکانی، ۱۳۹۸: ۱۳۵۱).

توسعه فناوری‌های دیجیتال همه جنبه‌های زندگی بشر و حقوق بین‌الملل ازجمله دامنه، موضوعات، ابزار و روش‌های تحریم‌های بین‌المللی و یک‌جانبه را تغییر داده و همچنان در حال تغییر است. فهرست زیر نمونه‌هایی را ارائه می‌دهد اما کامل نیست: پاسخ به حملات مسلحانه و تهدیدات علیه صلح و امنیت بین‌المللی. استفاده از ابزارهای دیجیتال برای تأمین مالی تروریسم؛ فعالیت‌های دیجیتال مخرب، ازجمله حملات به زیرساخت‌های حیاتی که به سطح یک حمله مسلحانه نمی‌رسند. انسداد تجارت برخط کشورهای هدف، شرکت‌ها و افراد و همچنین سایر اتباع. پیشگیری از دسترسی به سامانه عامل‌های برخط عمومی، انسداد تجارت با نرم‌افزار یا تجهیزات ارتباطی اطلاعاتی، انسداد حساب‌های رسانه‌های اجتماعی، فهرست ارزهای دیجیتال (Douhan, 2022: 129).

---

۱. جرائم دیجیتال از جمله جرائمی است که مولود جامعه فناور و مدرن بوده و به همین دلیل، ابهامات زیادی در باب ماهیّت و پیشینه این‌گونه جرائم از یک سو و ویژگی‌های این جرائم و مرتکبان آن‌ها از سوی دیگر وجود دارد. با عنایت به این ابهامات و نیز تفاوت‌های موجود بین جرائم دیجیتال و سایر جرائم، پیشگیری و مقابله با جرائم دیجیتال اقدامات تهاجمی خاصّی را می‌طلبد (موسوی و دیگران، ۱۴۰۱: ۳۲۳).

جرائم دیجیتال در دهه اخیر به یک واقعیت شناخته شده تبدیل شده‌اند. افراد روزانه به دستگاه‌های رایانه‌ای و موبایل وابسته‌اند و از این فناوری‌ها برای ارتباط با دیگران و انجام فعالیت‌های روزمره استفاده می‌کنند. این فعالیت‌ها حجم زیادی از داده‌ها و اطلاعات را تولید یا منتقل می‌کنند. جرم دیجیتال زمانی رخ می‌دهد که فعالیت غیرقانونی بر روی داده‌ها یا اطلاعات در سامانه‌های رایانه‌ای یا شبکه‌ها صورت گیرد (ملکوتی و خلیل‌زاده، ۱۴۰۱: ۸۳-۸۱). در ابتدا این جرائم بیشتر درزمینهٔ مالی بودند، اما اکنون به اشکال مختلفی مانند سرقت یا آسیب به سامانه‌های اطلاعاتی توسعه یافته‌اند (Kondo, Katseng, Zvidzayi, 2018: 121). با ظهور اینترنت و شبکه‌ها، میزان جرائم دیجیتال به‌طور چشمگیری افزایش یافته و این شبکه‌ها نقش مهمی در گسترش این نوع جرم ایفا می‌کنند.

با ظهور اینترنت بخش قابل توجهی از نگرانی‌های امنیت بین‌المللی به فضای دیجیتال معطوف شده است. این فضا با ساختار فنی پیچیده خود چالش‌های بزرگی را برای دولت‌ها به‌ویژه در مواجهه با شرکت‌های فناوری که به‌عنوان بازیگران اصلی شناخته می‌شوند، ایجاد کرده است. یکی از بزرگ‌ترین تهدیدات این فضا برای تمام کشورها اعم از کشورهای پیشرفته و کشورهای درحال‌توسعه، این است که ضعف فناورانه در یک کشور می‌تواند زمینه‌ساز تهدیدات جدی علیه سایر کشورها شود. این مسئله به این دلیل است که سوءاستفاده از زیرساخت‌های اینترنتی کشورهایی که امکان نظارت، پیشگیری مؤثر و حکمرانی در فضای دیجیتال را ندارند، به یک روش رایج برای اقدامات خرابکارانه و حتی جنگ‌های مجازی علیه کشورهای دیگر تبدیل شده است.[1]

۳. حکمرانی حقوق بشر و مسئولیت‌های دولت‌ها

در عصر دیجیتال، دولت‌ها مسئولیت‌های حیاتی در تنظیم و نظارت بر سکوهای برخط و تأمین حقوق بشر دارند. با پیشرفت سریع فناوری‌های دیجیتال و تأثیرات آن‌ها بر جامعه، دولت‌ها موظف به تصویب و اجرای قوانین و مقررات مؤثری هستند که امنیت ملی، حقوق فردی و بازار دیجیتال را حفاظت کنند. مقررات عمومی حفاظت از داده‌ها[2] در اتحادیه اروپا، ازجمله این مقررات هستند که با هدف پیشگیری از نقض حریم خصوصی و تأمین فضای امن برای کاربران وضع می‌شوند.

1. https://unstudies.ir/iauns-forum.
2. General Data Protection Regulation (GDPR), https://gdpr-info.eu.

یکی از مسئولیت‌های اصلی دولت‌ها، وضع قوانین و مقرراتی است که فعالیت‌های شرکت‌های مالک سکوها را تنظیم کند. این قوانین باید در حوزه‌های مختلفی مانند حفاظت از داده‌ها، نظارت بر محتوای برخط و احترام به حقوق بشر تدوین شوند. دولت‌ها می‌توانند قوانینی برای حفاظت از حریم خصوصی کاربران وضع کرده و از سوءاستفاده از داده‌ها پیشگیری کنند. علاوه‌بر این، نظارت بر محتوای برخط و پیشگیری از انتشار اطلاعات نادرست و افراطی نیز ازجمله وظایف دولت‌ها به شمار می‌آید. با این حال، لازم است که این نظارت‌ها به‌طور متوازن و با رعایت اصول حقوق بشر صورت گیرد تا از سانسورهای غیرضروری پرهیز شده و آزادی بیان حفظ گردد.

حکمرانی حقوق بشر در فضای دیجیتال با چالش‌هایی مانند تضاد بین امنیت و آزادی‌های فردی روبه‌روست. نظارت بر فضای دیجیتال برای مقابله با جرائم دیجیتالی ممکن است به نقض حریم خصوصی منجر شود. نبود نظارت هماهنگ و مؤثر در سطح جهانی، منجر به عملکرد پراکنده و غیر یکپارچه سکوها می‌شود که این می‌تواند حقوق بشر را در مقیاس جهانی تهدید کند. جرائم دیجیتال علاوه‌بر تهدید امنیت افراد، می‌تواند به نقض آزادی‌های اساسی نیز منجر شود. ازاین‌رو، ضروری است که سازوکارهایی برای تقویت امنیت دیجیتال و حفظ حریم خصوصی ایجاد گردد. این سازوکارها باید تضمین کننده دسترسی، یکپارچگی و محرمانگی اطلاعات باشند تا افراد بتوانند از حقوق خود بهره‌برداری کنند. در دنیای دیجیتال، امنیت دیجیتالی و حقوق بشر به‌طور متقابل به هم وابسته‌اند. پیشرفت‌های سریع در فناوری‌هایی مانند هوش مصنوعی و داده‌های کلان، چالش‌های جدیدی را برای حقوق بشر در فضای دیجیتال به وجود آورده است که نیازمند تصویب قوانین جدید و همکاری مؤثر بین دولت‌ها و نهادهای بین‌المللی است.

در سال ۲۰۱۶، «ائتلاف آزادی برخط»[1] بیانیه‌ای را در مورد رویکرد مبتنی بر حقوق بشر به امنیت دیجیتالی تصویب کرد که تأیید می‌کند که حقوق بشر و امنیت دیجیتالی مکمل، وابسته به یکدیگر و تقویت کننده یکدیگر هستند و سیاست‌ها و اقدامات امنیت دیجیتالی باید دارای قواعد و موازینی باشند.[2] علاوه‌بر این، قرار دادن حقوق بشر به‌عنوان مخالف امنیت دیجیتالی نه‌تنها گمراه کننده است، بلکه امنیت و امنیت عمومی و همچنین آزادی را تضعیف می‌کند. هم حقوق بشر و هم امنیت دیجیتالی باید با هم دنبال شوند تا به‌طور مؤثر

1. Freedom Online Coalition; https://freedomonlinecoalition.com/
2. https://freeandsecure.online/resources/foc-statement-support-cybersecurity-human-rights-recommendations/ - This statement endorses the work of the FOC Working Group 1 on an Internet Free and Secure, Details on the WG can be found here: https://freedomonlinecoalition.com/working-groups/working-group-1/

آزادی و امنیت را ارتقا دهند، به خطر می‌افتد. از سال ۲۰۱۶، چالش‌های جدیدی درزمینهٔ امنیت دیجیتال به وجود آمده است. در پی این تحولات، بسیاری از سیاست‌ها، قوانین و شیوه‌های ملی جدید تدوین و تصویب شده‌اند. با این حال، توصیه‌های ائتلاف آزادی برخط در خصوص حقوق بشر و امنیت دیجیتال، به ویژه با توجه به تمرکز مداوم بر امنیت دیجیتال در سطح سازمان ملل متحد، همچنان از اهمیت بالایی برخوردارند. هدف این بیانیه تأکید مجدد بر تعهدات سال ۲۰۱۶ است و در عین حال، رویکردی مبتنی بر حقوق بشر را برای تقویت امنیت دیجیتال، ارتقای ثبات در حکمرانی فضای دیجیتال و ترویج فناوری‌های نوظهور و قابل اعتماد ارائه می‌دهد. این بیانیه همچنین به تضمین حفاظت از تمامی کاربران برخط می‌پردازد و حاوی توصیه‌هایی برای شیوه‌های ملی در حوزه امنیت دیجیتال و فرآیندهای بین‌المللی مرتبط است. این توصیه‌ها بر اساس راهکارهایی است که توسط گروه کاری چندجانبه ائتلاف آزادی برخط تدوین شده‌اند.

در سطح بین‌المللی، نقش سازمان‌های بین‌دولتی، نظیر سازمان ملل متحد، به‌طور فزاینده‌ای در تشکیل بحث‌ها در مورد رفتار مسئولانه دولت در فضای دیجیتال از طریق گروه کارشناسان دولتی سازمان ملل متحد[1] درزمینهٔ ارتقای رفتار مسئولانه دولت در حکمرانی فضای دیجیتال در زمینه امنیت بین‌المللی و کارگروه باز سازمان ملل متحد[2] درزمینهٔ تحولات، اطلاعات، مخابرات و امنیت بین‌المللی و نیز در سطوح منطقه‌ای توسط سازمان‌هایی ازجمله اتحادیه آفریقا، اتحادیه اروپا، سازمان کشورهای آمریکایی، سازمان امنیت و همکاری در اروپا، شورای اروپا و مجمع منطقه‌ای انجمن کشورهای جنوب شرق آسیا[3] قابل ملاحظه و اثرگذار است.

در هر حال، آینده حقوق بشر در حکمرانی فضای دیجیتالی به تحول قانون و تفسیر آن توسط نهادهای حاکمیتی ملی و بین‌المللی بستگی دارد. البته برخی اذعان می‌دارند که ما با وضعیتی روبه‌رو هستیم که در آن فناوری در حال اجرای قانون است.[4] لازم به ذکر است، در ۲۲ می ۲۰۲۰، شورای امنیت سازمان ملل متحد در بحث خود در مورد امنیت دیجیتالی بر لزوم به رسمیت شناختن جرائم دیجیتالی به‌عنوان یکی از موضوعات

1. United Nations Group of Governmental Experts (UNGGE)
2. United Nations Open-ended Working Group (OEWG)
3 . Regional Forum of the Association of Southeast Asian Nations (ARF)
4.°http://eprints.lse.ac.uk/3707/1/Introduction%E2%80%93Human_Rights_and_Equity_in_Cyberspace_%28LSERO%29.pdf

حقوق بشر تأکید کرد. روند اقدام به تفصیل این است که اقداماتی مانند قطع اینترنت توسط دولت و هک کردن دستگاه‌های مخالفان می‌تواند منجر به نقض جدی حقوق بشر شود.[1]

۴. نقش دولت‌ها و سکوها و بخش خصوصی در تضمین حقوق بشر و امنیت برخط

در عصر دیجیتال فناوری‌های نوظهور مانند اینترنت و سامانه‌های نظارت برخط، علاوه‌بر ارائه مزایای فراوان، ممکن است به ابزاری برای نقض حقوق بشر تبدیل شوند. تهدیداتی نظیر نقض حریم خصوصی، سانسور اطلاعات و حملات دیجیتالی، به‌ویژه در فضای برخط، ازجمله چالش‌های جدی محسوب می‌شوند. به همین دلیل، قرارداد جهانی دیجیتال باید تدابیر لازم را برای حفاظت از حقوق بشر در فضای مجازی اتخاذ کرده و از نقض آن پیشگیری کند. با گسترش استفاده از اینترنت، چالش‌هایی چون سوءاستفاده از داده‌ها، هک اطلاعات و تحدید خدمات برخط توسط دولت‌ها، تهدیدات جدیدی را به وجود آورده‌اند که می‌توانند به نقض حقوق بشر منتهی شوند. ازاین‌رو، دولت‌ها و سکوها و بخش خصوصی باید مسئولیت‌های خود را در راستای حفظ حقوق بشر و امنیت برخط به‌طور جدی بر عهده گیرند.

دولت‌ها باید قوانینی بین‌المللی برای حفظ حقوق بشر در فضای دیجیتال تدوین و اجرا کنند، درحالی‌که سکوهای دیجیتال و بخش خصوصی نیز باید اقداماتی مؤثر برای مقابله با جرائم دیجیتال، حفاظت از داده‌های کاربران و پیشگیری از سوءاستفاده‌های برخط انجام دهند. هم‌افزایی میان دولت‌ها و سکوها و بخش خصوصی می‌تواند ضامن امنیت برخط و رعایت حقوق بشر در فضای دیجیتال باشد.

۴-۱. مسئولیت‌های دولت‌ها در قبال نقض حقوق بشر و استفاده غیرقانونی از فناوری‌ها

پس از جنگ‌های جهانی اول و دوم که به از دست دادن شمار زیادی از جان‌ها انجامید، تلاش‌هایی برای کاهش آثار و رنج‌های ناشی از جنگ‌ها آغاز شد و مقررات بین‌المللی حقوق بشر و حقوق بشردوستانه وضع گردید تا حداقل‌هایی برای حفظ امنیت و کرامت انسان‌ها مشخص شود. اهمیت این مقررات زمانی برجسته می‌شود که ضمانت‌های اجرایی مؤثر برای آن‌ها فراهم باشد، زیرا بدون این ضمانت‌ها، حتی بهترین قوانین نیز قادر به اجرای واقعی نخواهند بود. مسئله ضمانت اجرای حقوق بین‌الملل یکی از موضوعات پیچیده در حوزه‌های داخلی و بین‌المللی است و در حقوق بشر و حقوق بشردوستانه به‌ویژه از حساسیت بالایی برخوردار است، چراکه هدف نهایی این حقوق، حفاظت از کرامت و حقوق اساسی انسان‌هاست (ساکی، ۱۳۸۷:

1. “It's Time to Treat Cybersecurity as a Human Rights Issue”, Human Rights Watch, 26 May 2020.

۱۰۱). با رشد فضای دیجیتال نیاز است که اجرای این حقوق با تحولات فناوری هماهنگ شود؛ اما متأسفانه در بسیاری از موارد، فناوری‌ها به جای آنکه به حمایت از حقوق بشر بپردازند، به ابزارهایی برای نظارت و تبعیض علیه گروه‌های آسیب‌پذیر تبدیل می‌شوند (خاف‌خانی، ۱۳۸۶: ۴۹-۴۸).

قرارداد جهانی دیجیتال باید نقش اساسی در تأثیرگذاری بر ذینفعان برای رعایت تعهدات و مسئولیت‌های خود درزمینهٔ به رسمیت شناختن، حفاظت و ارتقای حقوق بشر در محیط‌های دیجیتال ایفا کند. این تعهدات باید نه‌تنها در سطح فردی بلکه در سطح جمعی نیز به اجرا در آید. پیمان دیجیتال باید اینترنت را به‌عنوان یک ابزار اساسی برای تحقق همه حقوق بشر به رسمیت بشناسد و دسترسی معنادار به آن را ارتقا دهد؛ امری که تنها زمانی ممکن است که افراد بتوانند به‌طور آزاد و ایمن از اینترنت استفاده کنند. این پیمان باید اقدامات پیشگیرانه‌ای برای کاهش شکاف‌های دیجیتال جنسیتی ترغیب کند و مفاهیم مشترکی را ترویج دهد که می‌تواند به سوی چارچوب‌های مبتنی بر حقوق بشر و تمرکز بر رفع تمامی اشکال خشونت‌های مبتنی بر جنسیت، ازجمله از طریق تسهیل استفاده از فناوری، هدایت شود. علاوه‌بر این، قرارداد باید چارچوب‌هایی را تقویت کند که شامل تعادلی مناسب از حقوق و معیارهای قانونی برای پاسخگویی ضروری به خشونت‌های برخط باشد، به‌طوری‌که این اقدامات هیچ‌یک از حقوق بنیادین دیگر را نقض نکند.[1]

حقوق بشر در فضای دیجیتال زمینه جدیدی از نگرانی جهانی است. با ظهور اینترنت و محبوبیتی که در سال‌های اخیر به دست آورده است، نظارت بر فضای دیجیتال به‌واسطه حکمرانی دولت‌ها و حفظ حقوق بشر افرادی که از آن استفاده می‌کنند، ضروری است. اینترنت دسته جدیدی از مجرمان یعنی مجرمان دیجیتال را به وجود آورده است. مجرمان دیجیتال به زندگی خصوصی افراد نفوذ می‌کنند و از این طریق حقوق بشر کاربران اینترنت را نقض می‌کنند. اینترنت یک رسانه قوی برای بیان ایده‌های ما است و بنابراین باید بدون هیچ محدودیتی باشد. این بستری را برای ما فراهم می‌کند تا از حق آزادی بیان و اطلاعات استفاده کنیم. در زمانی که اینترنت به وجود آمد و فناوری هنوز در حال رشد بود، هیچ کس هرگز فکر نمی‌کرد که بتواند تا این حد بر حقوق اساسی آن‌ها تأثیر بگذارد (ضیایی، ۱۳۹۶: ۷۹). بنابراین، در عصر دیجیتال، استفاده نادرست از فناوری اطلاعات و ارتباطات می‌تواند در رابطه با فعالیت‌های دولت و بخش خصوصی رخ دهد.

---

[1] . Derechos Digitales statement to the Global Digital Compact Thematic Deep-Dive session on human rights online, Published on 12 May 2023, https://www.apc.org/en/pubs/derechos-digitales-statement-global-digital-compact-thematic-deep-dive-session-human-rights.

بیشتر اصول حقوق بشر معطوف به شناسایی و پیشگیری از سوءاستفاده از سوی سازمان‌های دولتی است، اگرچه اخیراً گسترش حمایت از حریم خصوصی از بخش عمومی به بخش خصوصی قابل ملاحظه است.

زمانی که دولت‌ها در حملات دیجیتال مشارکت می‌کنند، حقوق بشر به خطر می‌افتد؛ مانند زمانی که روسیه در سال‌های ۲۰۱۶ در کریمه و ۲۰۱۸ در «اینگوشتیا» اینترنت را قطع کرد، یا وقتی دولتی گوشی یک مخالف یا خبرنگار را هک می‌کند، همان‌طور که عربستان سعودی و امارات متحده عربی بارها این اقدام را انجام داده‌اند. فناوری‌های مرتبط با نقض حقوق بشر شامل اینترنت، روش‌های تحلیل دی‌ان‌ای، شناسایی بیومتریک، دوربین‌های مداربسته، تلفن‌های همراه، دستگاه‌های شنود، پایگاه‌های داده شبکه‌ای و شبکه‌های عصبی برای تحلیل داده‌ها، سامانه‌های تشخیص صدا و سایر فناوری‌ها می‌شود.[1] در ماه مه ۲۰۲۰، شورای امنیت سازمان ملل متحد درباره امنیت دیجیتال و ضرورت شناسایی حملات دیجیتال به‌عنوان یکی از ابعاد حقوق بشر بحث کرد. اقدامات خاصی مانند قطع اینترنت توسط دولت‌ها یا هک کردن دستگاه‌های مخالفان می‌تواند به نقض جدی حقوق بشر منجر شود. این نگرانی‌ها توسط حداقل دوازده کشور ازجمله استونی، بلژیک، هلند، اکوادور، ژاپن و سوئیس تأیید شد.[2]

۲-۴. نقش سکوها و دولت‌ها و بخش خصوصی در پیشگیری از نقض حقوق و تضمین امنیت برخط

سکوها به‌عنوان ابزارهای ارتباطی نوین، امکانات گسترده‌ای را برای کاربران فراهم می‌کنند، اما هم‌زمان با چالش‌ها و جرائم متنوعی مانند خشونت برخط، آزار و اذیت، انتشار اطلاعات غلط و نقض حریم خصوصی روبه‌رو هستند که ممکن است آثار منفی بر حقوق بشر بگذارند.[3] این چالش‌ها به‌طور عمده در دو بخش اصلی قابل تحلیل هستند: اول، حقوق بشر و دوم، توانایی‌های اجرایی سکوها. از جنبه حقوق بشر، مفاهیمی نظیر آزادی بیان و حق حریم خصوصی در فضای دیجیتال با چالش‌های جدیدی مواجه شده است. سکوها که معمولاً نهادهای خصوصی به شمار می‌روند، ممکن است در نظارت و واکنش به محتوای مجرمانه با مشکلاتی مواجه شوند. از سوی دیگر، در بعد اجرایی، مسائلی چون تضاد میان قوانین ملی و بین‌المللی و

1. http://www.cybercrimejournal.com/smithijccjuly2007.pdf.
2. Human Rights Watch. Retrieved 26 May 2020.
۳. ناشناس بودن کاربران در فضای مجازی، به‌ویژه در سکوهایی نظیر توییتر و تلگرام، روند پیگیری و برخورد با جرائم را پیچیده و دشوار می‌سازد. علاوه بر این، سکوهای دیجیتال ممکن است استانداردهای متفاوتی برای مدیریت محتوای کاربران در کشورهای مختلف اعمال کنند که این مسئله می‌تواند منجر به نقض حقوق بشر گردد.

ضرورت حفظ تعادل میان حفاظت از حریم خصوصی و مقابله با محتوای مضر، مسائلی پیچیده و چالش‌برانگیز ازنظر حقوقی و اخلاقی ایجاد می‌کنند.[۱]

پیشگیری از نقض حقوق بشر در عصر دیجیتال مسئولیتی مشترک میان قانون‌گذاران و جامعه بین‌المللی، به‌ویژه سازمان ملل متحد، است. این نهادها باید اطمینان حاصل کنند که مقررات جدید در این حوزه با اسناد هنجاری بین‌المللی و قوانین محلی هم‌راستا بوده و رعایت حقوق بشر در فضای دیجیتال تضمین گردد. از سوی دیگر، بخش خصوصی نیز می‌تواند با طراحی و توسعه فناوری‌های جدید به‌گونه‌ای که از نقض حقوق بشر پیشگیری کرده یا آن را به حداقل برساند، نقش مؤثری در پیشگیری از سوءاستفاده‌ها ایفا کند. به این ترتیب، حمایت از حقوق بشر در دنیای دیجیتال بهترین نتیجه را از تعامل میان نوآوری‌های تکنولوژیکی و اصلاحات سیاستی به دست می‌آورد. برای مثال، توسعه دهندگان سخت‌افزار و نرم‌افزار می‌توانند متقاعد شوند که در فرآیند طراحی و تولید محصولات جدید، راه‌حل‌های فناورانه‌ای برای رفع چالش‌های مربوط به حقوق بشر در نظر بگیرند.

جرائم دیجیتال به‌طور فزاینده‌ای حقوق بشر را درزمینه‌های مختلفی همچون آزادی بیان، حق حریم خصوصی، آزادی عقیده و جریان آزاد اطلاعات نقض می‌کنند. دولت‌ها سیاست‌های مختلفی را برای محافظت از رایانه‌های مرتبط با جرائم دیجیتال ایجاد کرده‌اند، اما بسیاری از این سیاست‌ها به دلیل گستردگی بیش‌ازحد و تعاریف مبهم، فاقد کنترل‌های لازم و سازوکارهای پاسخگویی دموکراتیک هستند که می‌تواند منجر به نقض حقوق بشر و سرکوب نوآوری گردد.[۲] این وضعیت گاهی اوقات به‌گونه‌ای است که دولت‌ها امنیت را به‌عنوان محافظت از خود در برابر بی‌ثباتی سیاسی تعریف کرده و برای حفظ خود اقدامات نامتناسبی اتخاذ می‌کنند که خود تبدیل به منبع ناامنی می‌شود. نمونه‌ای از این موارد جاسوسی از عمر عبدالعزیز، مخالف سعودی است که توسط دولت عربستان سعودی با استفاده از نرم‌افزارهای جاسوسی صورت گرفت.

---

۱. برای مقابله با این مشکلات، سکوها می‌توانند از ابزارهای فنی پیشرفته، همچون هوش مصنوعی، برای شناسایی و حذف محتواهای مجرمانه بهره‌برداری نمایند. علاوه بر این، تقویت مقررات حقوق بشری، آموزش فرهنگ دیجیتال و نظارت بین‌المللی می‌تواند به کاهش نقض‌های حقوق بشری و ارتکاب جرائم دیجیتالی کمک کند. درنهایت، ایجاد همکاری میان سکوها و دولت‌ها و سازمان‌های حقوق بشری برای تدوین و اجرای چارچوبی منسجم و مؤثر ضروری به نظر می‌رسد.

۲. جرائم دیجیتال ناقض حقوق بشر نظیر حق حریم خصوصی، حق رازداری، حق رهایی از هرگونه باج‌گیری و شکنجه است. هکرها معمولاً داده‌های محرمانه کاربر یا هر شرکتی را قفل می‌کنند و برای باز کردن آن‌ها باج می‌خواهند، همچنین داده‌ها را سرقت کرده و از آنها سوءاستفاده می‌کنند.

این اقدام باعث به خطر افتادن محرمانه بودن ارتباطات او با جمال خاشقجی در ماه‌های منتهی به قتل خاشقجی شد.[۱]

در این زمینه، پس از معرفی فناوری‌های جدید، باید ارزیابی دقیقی از پتانسیل آن‌ها برای نقض حقوق بشر و تهدید موازین بین‌المللی و ملی انجام شود. دولت‌ها باید الزامات گزارش‌دهی بر اساس موازین بین‌المللی را جدی گرفته و افراد و سازمان‌ها را تشویق کنند تا هرگونه نقض حقوق بشر را فوراً گزارش دهند. در بازار سرمایه‌داری، جایی که شهرت شرکت‌ها اهمیت زیادی دارد، ارتباط با فناوری‌های نقض کننده حقوق بشر می‌تواند به‌عنوان یک عامل بازدارنده قوی عمل کند و به راهی مؤثر برای پیشگیری از پیشرفت‌های مضر در عصر دیجیتال تبدیل شود.[۲] با این حال، قواعد و مقررات حقوق بین‌الملل بشر هنوز تمام ابعاد جرائم دیجیتال را پوشش نمی‌دهند. از سوی دیگر، به دلیل عدم اجماع جامعه جهانی و ابهامات موجود در نحوه اجرای برخی از این اصول، می‌توان با توسعه تدریجی قواعد قراردادی و عرفیِ فعلی، این ابهامات را حل‌وفصل کرد (محمودی و انصاری‌مهیاری، ۱۴۰۱: ۱۹).

با گسترش فضای دیجیتال، تضمین و اعمال مؤثر حقوق بشر درزمینهٔ اطلاعات و تعاملات برخط به یک ضرورت جدی تبدیل شده است. در این راستا، نیاز به تدوین استانداردهای بین‌المللی نوین برای حفاظت از این حقوق در دنیای دیجیتال، به‌ویژه حقوق بشر دیجیتال و منشور جهانی حقوق دیجیتال، بیش‌ازپیش احساس می‌شود. این منشور باید به‌طور شفاف حقوقی مانند دسترسی آزاد به اطلاعات، حفاظت از داده‌های شخصی و آزادی بیان را تعریف کرده و روش‌های اجرایی آن‌ها را تبیین نماید. علاوه‌بر این، تدوین چارچوب‌های بین‌المللی برای نظارت بر رعایت این حقوق توسط دولت‌ها و شرکت‌های فناوری امری ضروری است. یکی از چالش‌های اساسی در این حوزه، تضاد میان حقوق حریم خصوصی و نیازهای امنیتی، به‌ویژه درزمینهٔ داده‌کاوی و مدیریت اطلاعات توسط شرکت‌های فناوری است. برای مواجهه با این چالش‌ها، تقویت قوانین و ارتقای آگاهی عمومی درزمینهٔ حقوق دیجیتال اهمیت فراوانی دارد. علاوه‌بر این، ایجاد ساختارهای بین‌المللی جامع برای حمایت از حقوق بشر دیجیتال در فضای برخط امری اجتناب‌ناپذیر به نظر می‌رسد. این ساختار باید شامل شفافیت در استانداردهای سکوها، تعیین صلاحیت قضائی روشن و حفظ تعادل میان حریم

1.°https://www.legalserviceindia.com/legal/article-4724-cyber-security-and-cyber-crime-infringes-human-rights-html.

2. Dominik Brodowski, Cybercrime, human rights and digital politics, in: Research Handbook on Human Rights and Digital Technology Edited by Ben Wagner, Matthias C. Kettemann and Kilian Vieth, Elgaronline from Edward Elgar Publishing, 2019, p. 47.

خصوصی و مسئولیت‌پذیری باشد. همچنین، تقویت سازوکارهای شکایت و جبران خسارت می‌تواند در بهبود وضعیت حقوق بشر در فضای مجازی مؤثر واقع شود.

۵. چالش‌ها و تخلفات ناشی از فناوری‌های نوین و پاسخ‌های حقوقی به آن‌ها

در دهه‌های اخیر با گسترش جرائم دیجیتال و تلاش‌های قانونی برای مقابله با آن‌ها، شاهد بسیاری از موارد سوءاستفاده از فناوری اطلاعات و ارتباطات بوده‌ایم که می‌توان آن‌ها را به‌عنوان نقض حقوق بشر تلقی کرد. در این میان، برخی از موارد به‌طور خاص شناسایی شده‌اند یا به‌عنوان تخلفات بالقوه مطرح گردیده‌اند.

الف. حریم خصوصی: مجرمان دیجیتالی برای سرقت داده‌ها به دستگاه‌های الکترونیکی افراد حمله می‌کنند تا از اطلاعات به دست آمده برای مقاصد خود استفاده کنند. این اقدامات نقض آشکار حق حفظ حریم خصوصی[1] محسوب می‌شود (Agarwal and Ladha, 2022: 9). یکی از نگرانی‌های اصلی در خصوص حریم خصوصی، به‌ویژه در مورد کارت‌های شناسایی بیومتریک، ترس از جمع‌آوری اطلاعات بدون رضایت یا آگاهی افراد است، یا جمع‌آوری داده‌ها بدون تعریف دقیق هدف استفاده از آن‌ها. این اطلاعات ممکن است برای مقاصد دیگری غیر از هدف اولیه جمع‌آوری، مورد استفاده قرار گیرند. علاوه‌بر رعایت اصول و قوانین حریم خصوصی، ممکن است اقدامات اضافی برای تقویت حفاظت از حریم خصوصی در دنیای دیجیتال ضروری باشد. این اقدامات شامل الزام به استفاده از سطوح مشخص رمزگذاری برای ضبط، ذخیره‌سازی و انتقال داده‌ها، محدود کردن دسترسی به پایگاه‌های داده تحت نظارت دقیق ناظران مستقل، پیشگیری از بازسازی یا نگهداری نمونه‌های بیومتریک اصلی از اطلاعات رمزگذاری شده و پیشگیری از مقایسه داده‌های بیومتریک که مستقیماً از افراد به دست نیامده، می‌شود. برخی از این موارد ممکن است نیازمند اصلاحات در قانون حفظ حریم خصوصی ۱۹۸۸ (مشترک‌المنافع) باشد (Smith, 2007: 171).

ب. تعقیب و محاکمات کیفری: قانون جرائم رایانه‌ای دامنه اختیارات تحقیقاتی سازمان‌های مجری قانون را به‌طور قابل توجهی گسترش می‌دهد تا با مشکلاتی مانند پنهان‌سازی شواهد الکترونیکی از طریق رمزگذاری مقابله کنند. کشورهایی که تحت منشور حقوق بشر محدود نشده‌اند، راه‌حل ساده‌ای برای مقابله با چالش رمزگذاری ارائه داده‌اند: آن‌ها به‌طور مستقیم از افراد می‌خواهند که کلیدهای رمزگذاری خود را

---

۱. حریم خصوصی عمومی شامل آزادی اطلاعات و بیان در اینترنت از یک طرف و امنیت و حریم خصوصی در فضای مجازی از طرف دیگر است.

افشا کنند یا با اتهامات جنایی مواجه شوند. در ماده ۶ کنوانسیون رم ممکن است مانعی برای چنین افشای اجباری وجود داشته باشد، هرچند کمیسیون اروپایی حقوق بشر دامنه این ماده را تنها به اظهارات شفاهی محدود کرده است. با این حال، رویه‌های اروپایی در مورد رمزگشایی اجباری باید به‌طور دقیق تدوین شوند تا در برابر نظارت قضائی مقاومت کنند (Smith, Grabosky, & Urbas, 2004: 42). کنوانسیون شورای اروپا[1] در مورد جرائم دیجیتال (۲۰۰۱) شامل مقررات مختلفی است که برای حفاظت از هنجارها و حقوق بشر در تحقیقات جرائم دیجیتال طراحی شده‌اند، ازجمله الزامات نظارت قضائی یا نظارت مستقل، رعایت تناسب و احترام به حقوق اشخاص ثالث، به‌ویژه در ارتباط با قدرت مقرراتی که اجازه جستجو، ضبط و نظارت را می‌دهد. برخی از مدافعان حریم خصوصی این مقررات را به‌عنوان ناکافی مورد انتقاد قرار داده‌اند (Taylor, 2001: 30).

ج. تبعیض: نقض احتمالی قوانین ضد تبعیض در دنیای دیجیتال ممکن است زمانی رخ دهد که افرادی که به ارتکاب فعالیت‌های غیرقانونی برخط متهم می‌شوند، ادعا کنند که رفتارشان ناشی از اختلال یا شرایط خاصی است. برای نمونه، در یک پرونده مدنی در کانادا، یک استاد دانشگاه به دلیل استفاده از تجهیزات کارفرمایی برای دانلود محتوای هرزه‌نگاری کودکان از دانشگاه اخراج شد.[2]. همچنین اتحادیه کارکنان خدمات عمومی به دلیل اعتراف به ارتکاب جرم، این فرد را به دو سال حبس تعلیقی محکوم کرد. چنین پرونده‌هایی می‌توانند سؤالات پیچیده‌ای در خصوص تداخل میان حقوق فردی و قوانین حاکم بر فضای دیجیتال مطرح کنند، به‌ویژه زمانی که افراد به دلیل شرایط خاص خود از تبعیض یا مجازات‌های ناعادلانه شکایت می‌کنند (Smith, Grabosky & Urbas, 2004: 75).

---

۱. لازم به ذکر است، توسعه و تکامل فضای دیجیتالی سبب ایجاد اشکال مختلفی از جرائم دیجیتالی شده است. ازاین‌رو در دهه‌های اخیر کشورها در قبال جرائم دیجیتال در جهت تدوین معاهدات بین‌المللی گام برداشته‌اند. یکی از این معاهدات بین‌المللی، معاهده جرائم دیجیتالی شورای اروپا (کنوانسیون بوداپست) در سال ۲۰۰۱ بوده که به‌عنوان نخستین معاهده در این زمینه نگاشته شده است. این معاهده شامل اصول سیاست نمادین ازجمله اطمینان بخشیدن به مردم در جهت خنثی کردن سلاح‌های جاسوسی دیجیتالی، آموزش عمومی درباره جرائم دیجیتالی و بازدارندگی ارتکاب فعالیت‌های مجرمانه در فضای دیجیتالی، است (کتانچی و پورقهرمانی، ۱۳۹۸: ۳۱).

۲. فضای دیجیتال به‌عنوان بخشی جدایی‌ناپذیر از زندگی کودکان، زمینه‌ساز دسترسی آنان به حقوق اساسی مانند آموزش، آزادی بیان، تفریح و مشارکت در فعالیت‌های جمعی است. با این وجود، گسترش جرائم پیچیده، کمبود آگاهی و نارسایی‌های قانونی، سلامت روانی و اخلاقی کودکان را به‌طور جدی تهدید می‌کند. یافته‌های پژوهش نشان می‌دهد که خشونت علیه کودکان در فضای دیجیتال به صورت گسترده رخ می‌دهد و مستندات بین‌المللی بر ضرورت اتخاذ تدابیر حمایتی از سوی دولت‌ها تأکید دارند. این تدابیر شامل تقویت همکاری‌های بین‌المللی، تصویب قوانین حمایتی، بهره‌گیری از فناوری‌های فیلترینگ و ارتقای سواد رسانه‌ای است تا حکمرانی فضای دیجیتال به محیطی امن و مناسب برای کودکان تبدیل گردد (بذرپاچ، ۱۴۰۱: ۲۹۷).

د. آزادی بیان و اندیشه: در دنیای دیجیتال تخلفات می‌توانند از سوی سازمان‌ها، شرکت‌ها یا افراد مختلف رخ دهند. نظارت بر ارتباطات ایمیل و تلفن همراه توسط سازمان‌ها ممکن است به نقض آزادی بیان منجر شود، درحالی‌که از سوی دیگر، انتشار هرزنامه‌ها، مطالب نژادپرستانه یا حملات دیجیتالی می‌تواند حقوق دیگران را زیر پا بگذارد. محدودیت‌های قانونی در خصوص محتوای برخط، نظیر انسداد مطالب توهین‌آمیز یا زشت، ممکن است با نقض آزادی بیان تضاد داشته باشد.[۱] با این حال، این حقوق در موارد خاصی محدود می‌شوند تا از حقوق افراد دیگر، امنیت ملی، نظم عمومی، سلامت عمومی و اخلاقیات حفاظت شود. فضای اینترنت به‌ویژه محیطی است که در آن برقراری تعادل میان این حقوق دشوار است. مسئله «نژادپرستی دیجیتال» نیز از سوی شورای اروپا مورد توجه قرار گرفته و در سال ۲۰۰۱، کنوانسیون شورای اروپا درزمینهٔ جرائم دیجیتال به همراه پروتکل الحاقی در مورد جرم‌انگاری تبلیغات نژادپرستانه و بیگانه‌هراسی از طریق اینترنت به تصویب رسید. در خصوص مجازات‌های تحقیرآمیز، ماده ۷ میثاق بین‌المللی حقوق مدنی و سیاسی تصریح می‌کند که هیچ فردی نباید مورد شکنجه یا رفتار تحقیرآمیز قرار گیرد. با این حال، مجازات اعدام هنوز در برخی کشورها برای جرائم خاص، ازجمله جرائم رایانه‌ای، اعمال می‌شود (Smith, Grabosky, & Urbas, 2004: 79).

هـ. کیفرهای تحقیرآمیز: ماده ۷ میثاق بین‌المللی حقوق مدنی و سیاسی تصریح می‌کند که «هیچ فردی نباید تحت شکنجه یا رفتار یا مجازات ظالمانه، غیرانسانی یا تحقیرآمیز قرار گیرد.» با این حال، مجازات اعدام هنوز در برخی کشورها اجرا می‌شود و در موارد نادر، مانند چین، حتی برای جرائم مرتبط با فضای مجازی یا رایانه‌ای نیز مجازات اعدام صادر شده است. این موضوع نشان دهنده تضاد میان اصول حقوق بشر و برخی قوانین ملی است که ممکن است به شدت حقوق فردی را نقض کنند.[۲]

---

۱. استفاده ابزاری از اینترنت مشمول همان مسئولیت‌ها و مجازات‌های قانونی است که برای رفتارهای مشابه در قانون تعیین شده است. اسناد بین‌المللی بر حفظ حریم خصوصی تأکید داشته و نحوه اجرای آن بر عهده قوانین داخلی کشورها گذاشته شده که این موضوع از اصول اساسی حاکم بر فضای اینترنت به شمار می‌رود. دولت‌ها موظف‌اند در چارچوب منافع ملی، حداقل امکانات دسترسی به اینترنت را فراهم کنند و تنها در شرایط خاص و استثنایی مجاز به قطع این ارتباط هستند. علاوه‌بر این، به منظور تضمین حقوق برابر، دولت‌ها باید خدمات اینترنتی ویژه‌ای را برای معلولان و افراد دارای محدودیت فراهم آورند تا امکان بهره‌مندی آنان از خدمات و فعالیت‌های اینترنتی فراهم گردد. درنهایت، امنیت ملی همواره مهم‌ترین دغدغه دولت‌ها در تدوین و اجرای مقررات مربوط به استفاده از اینترنت محسوب می‌شود (ایازی، شریفی‌طرازکوهی، پاکزاد و ساعدی‌بناب، ۱۴۰۰: ۲۵).

2. See: People's Daily Online 2000.

٦. مطالعه موردی: چارچوب حمایتی نظام حقوقی مالزی

استقرار نظام حقوق بشر دیجیتال در جوامع اسلامی با چالش‌های ساختاری در حوزه هم‌گراییِ قواعد فقهی با الزامات بین‌المللیِ مالکیت فکری مواجه است. در این گذار، مالزی به واسطه نظام حقوقی دوگانه (تلفیق نظام کامن‌لا و قواعد شرعی)، الگویی کارآمد از توازن میان اقتضائات فناوری و تعهدات دینی و اخلاقی ارائه داده است که می‌تواند به‌عنوان یک الگوی عملیاتی برای بازنگری در سیاست‌گذاری‌های حقوقیِ سایر کشورهای اسلامی مورد مداقه قرار گیرد.

هرچند مالزی به تمامی اسناد بنیادین حقوق بشر (ازجمله میثاق بین‌المللی حقوق مدنی و سیاسی) نپیوسته است، اما از طریق «اصول عامه» مندرج در قانون اساسی فدرال، مبانی مزبور را در نظام تقنینی خود درونی‌سازی کرده است. اصل دهم قانون اساسی، ضمن تضمین حق آزادی بیان، به مقنن اجازه می‌دهد به استناد «نظم عمومی» و «اخلاق اسلامی»، محدودیت‌های مقتضی را اعمال نماید. در ساحت تقنین دیجیتال، «قانون جرائم رایانه‌ای، مصوب ۱۹۹۷»،[۱] «قانون ارتباطات و چندرسانه‌ای، مصوب ۱۹۹۸»،[۲] «قانون (اصلاحیه) کمیسیون ارتباطات و چندرسانه‌ای مالزی، مصوب ۲۰۲۴»[۳] و «قانون امنیت سایبری، مصوب ۲۰۲۴»،[٤] ارکان اصلی مقابله با بزهکاری دیجیتالی (شامل سرقت داده، نقض حریم خصوصی و تعرض به مالکیت فکری) را تشکیل می‌دهند (Redzuan Mohamad, et al, 2024: 169). در عین حال، افزایش بسیار قابل توجهی در استفاده از اینترنت در سال ۲۰۲۰ مشاهده می‌شود به علت همه‌گیری کووید-۱۹ که کشور را تحت تأثیر قرار داد و اولین مورد در مالزی در ۲۵ ژانویه ۲۰۲۰ شامل شهروندان چینی که در ۲۳ ژانویه ۲۰۲۰ به مالزی آمدند گزارش شد. لازم به ذکر است مطابق گزارش سال ۲۰۲۳، امنیت دیجیتال مالزی در سال ۲۰۲۲، ۴۷۴۱ مورد تهدید دیجیتال بوده است، درحالی‌که تا فوریه ۲۰۲۳، موارد گزارش شده ۴۵۶

1. Computer Crimes Act 1997; Date of Royal Assent 18 June 1997 Date of publication in the Gazette 30 June 1997 PREVIOUS REPRINT, http://www.commonlii.org/my/legis/consol_act/cca1997185.
2. Communications and Multimedia Act 1998 (CMA); Communications and Multimedia Act 1998; date of Royal assent 3 september 1998 date of publication in the Gazette 5 october 1998, https://www.vertic.org/media/National%20Legislation/Malaysia/MY_Communications_and_Multimedia_Act.pdf.
3. Malaysian Communications and Multimedia Commission (Amendment) Act 2024
4. The Cyber Security Act 2024; https://www.rajahtannasia.com/media/7831/2024_03_2024-dr-8-bi.pdf.

مورد کلاهبرداری بود.[1] ازاین‌رو، برای پیشگیری از گسترش همه‌گیری از جدی‌تر شدن، دولت اولین فرمان کنترل حرکت[2] را در ۱۸ مارس ۲۰۲۰ اجرا کرد و پس از آن مرحله دوم فرمان کنترل حرکت، دستور کنترل حرکت مشروط،[3] فرمان کنترل جنبش توان‌بخشی را اجرا کرد. در عین حال، اذعان می‌گردد پنج نوع جرائم دیجیتالی در مالزی وجود دارد. فیشینگ، هک، کلاهبرداری، سرقت هویت و آزار و اذیت یا قلدری دیجیتالی است (نمامیان، ۱۴۰۳: ۱۲۲).

از منظر فقهی، حقوق مالکیت فکری پدیدآورندگان آثار دیجیتالی در مالزی به مثابه «حقِ مالیِ غیرمادی» شناخته شده و تحت شمول قاعده فقهی «لاضرر و لاضرار» قرار دارد. وفق این امر هرگونه انتفاع غیرمجاز از آثار متعلق به غیر، مصداق غصب منافع و نقض حقوق‌الناس محسوب می‌گردد. اگرچه صلاحیت اختصاصی دادگاه‌های شرعی در دعاوی مالکیت فکری محدود است، اما این نهادها در تفسیر ماهیت جرائم دیجیتال و تبیین تعارض محتوای تولیدی با موازین اخلاقی، دارای نقش هدایت‌گر هستند؛ به ویژه هنگامی که نقض مالکیت فکری با عوارض سوءاجتماعی همراه باشد.

در پاسخ به چالش‌های نوظهور در بسترهای تجارت الکترونیک دولت مالزی با تصویب «قانون اصلاحیه حق مؤلف ۲۰۲۲»،[4] دایره جرم‌انگاری را توسعه داده است. در این فرآیند، «کمیسیون ارتباطات و چندرسانه‌ای مالزی»[5] مکلف است در راستای اعمال محدودیت‌ها، اصل «تناسب» را رعایت نماید تا توازن میان صیانت از حقوق صاحبان اثر و آزادی‌های قانونی کاربران مخدوش نگردد. این رویکرد، نمادی از کاربست موازین حقوق بشری در حکمرانی دیجیتال با هدف پیشگیری از مداخلات خودسرانه است (Sidi Ahmed, 2019: 162).

با این همه، تجربه مالزی نشان می‌دهد که موازین حقوق بشری در فضای دیجیتالی برای حمایت از آثار دیجیتالی پدید آورندگان، نه در مواجهه با شریعت، بلکه در پرتو یک نظام اخلاقی‌فقهیِ همسو با تعهدات جهانی قابل تحقق است. مالزی با تلفیق قواعد مدرن و ارزش‌های دینی، الگویی از «عدالت دیجیتال» را ارائه کرده که ضمن صیانت از حقوق خالقان اثر، کرامت انسانی را بر سوداگری اقتصادی ارجح می‌داند. این

1. https://www.nst.com.my.
2. Movement Control Order (MCO).
3. Conditional Movement Control Order (CMCO).
4. Copyright (Amendment) Act 2022 ('The Amendment Act').
5. Malaysian Communications and Multimedia Commission.

الگوی ترکیبی، الگوی راهبردیِ مؤثری برای همسان‌سازی قانون‌گذاری دیجیتال در کشورهای اسلامی فراهم می‌آورد.

نتیجه‌گیری

جرائم دیجیتال به دلیل ویژگی‌های خاص خود، مانند شکنندگی شواهد دیجیتال، چالش‌های پیچیده‌تری نسبت به جرائم سنتی ایجاد می‌کنند. این نوع جرائم به راحتی می‌توانند تغییر کرده یا آسیب ببینند که همین امر فرایند اثبات و پیگیری آن‌ها را دشوارتر می‌سازد. از آنجا که جرائم دیجیتال به‌طور جهانی و در بسیاری از حوزه‌ها تأثیرگذار هستند، مقابله با آن‌ها نیازمند همکاری‌های بین‌المللی و اتخاذ تدابیر خاص در سطح جهانی است. فناوری‌های نوین، مانند سامانه‌های احراز هویت بیومتریک، می‌توانند به‌طور مؤثری از حقوق بشر و اطلاعات هویتی افراد محافظت کنند؛ با این حال، برای پیشگیری از نقض احتمالی حقوق بشر، ضروری است که در مراحل اولیه توسعه این فناوری‌ها، پیشگیری از مشکلات آینده مد نظر قرار گیرد.

با افزایش تعداد کاربران اینترنت و پیچیدگی‌های روزافزون جرائم دیجیتال، تدوین هنجارهای حقوقی و مقررات جهانی برای مقابله با این تهدیدات از اهمیت ویژه‌ای برخوردار است. هرچند کنوانسیون بوداپست برخی از ابعاد جرائم دیجیتال را پوشش داده است، اما به دلیل ماهیت منطقه‌ای آن، نمی‌تواند به‌طور کامل به‌عنوان یک سند بین‌المللی جامع عمل کند. ازاین‌رو، ایجاد یک کنوانسیون جهانی که به شفافیت در درک و مقابله با جرائم دیجیتال کمک کند و استانداردهای یکسانی برای مسائل فرامرزی تدوین کند، ضروری است. بنابراین، دولت‌ها باید سیاست‌های خود را به‌گونه‌ای تنظیم کنند که حقوق اساسی بشر، ازجمله حریم خصوصی و آزادی‌های فردی، در فضای دیجیتال تهدید نشود و از این حقوق به‌طور مؤثری محافظت گردد.

برای تقویت حکمرانی حقوق بشر در فضای دیجیتال و مقابله با جرائم برخط، اقدامات مختلفی درزمینهٔ اصلاح قوانین، نظارت دقیق، آموزش کاربران و بهره‌گیری از فناوری‌های نوین مطرح شده است. نخستین گام اساسی، روزآمدسازی مقررات حقوق بشری به‌گونه‌ای است که با چالش‌های دیجیتال نظیر نقض حریم خصوصی و سانسور برخط هماهنگ شود. این قوانین باید به اندازه کافی منعطف باشند تا بتوانند با پیشرفت‌های فناوری هم‌راستا شوند. همکاری‌های بین‌المللی در مبارزه با جرائم فرامرزی نیز بسیار ضروری است تا یک چارچوب حقوقی متحد برای مقابله با تهدیدات برخط شکل گیرد. نظارت شفاف و پیوسته بر سکوهای دیجیتال، به‌ویژه شبکه‌های اجتماعی، برای اطمینان از رعایت حقوق کاربران و پیشگیری از سوءاستفاده‌ها الزامی است. به‌علاوه، حفظ آزادی بیان و دسترسی آزاد به اطلاعات باید با تأمین امنیت

عمومی به‌طور متعادل صورت گیرد. آموزش کاربران درزمینهٔ حقوق دیجیتال و امنیت برخط نیز به‌منظور مقابله با تهدیدات دیجیتالی و محافظت از هویت افراد امری حیاتی است. استفاده از فناوری‌های امن مانند رمزنگاری داده‌ها و احراز هویت بیومتریک می‌تواند از حقوق کاربران در برابر نقض‌های احتمالی حفاظت کند. درنهایت، وضع مقررات دقیق برای شرکت‌های فناوری و تقویت ابزارهای قضائی برای تعقیب جرائم دیجیتالی ضروری به نظر می‌رسد.

در نظام حقوقی مالزی، انطباق هنجارهای بین‌المللی با موازین دینی، از طریق نظام حقوقی دوگانه (کامن‌لا و شریعت) و اصول حقوق بشر مندرج در قانون اساسی فدرال، صورت پذیرفته است. قوانین مربوط به جرائم دیجیتالی، با استناد به مبانی فقهی ازجمله قاعده «لاضرر»، حقوق مالکیت فکری را به مثابه حقی شرعی و قابل استناد، شناسایی و حمایت می‌نمایند. این کشور با اتخاذ رویکرد «حکمرانی چند بازیگر» و اعمال اصل «تناسب» در محدودسازی ارائه دهندگان خدمات دیجیتال، تعادلی میان تضمین آزادی بیان، صیانت از حقوق کاربران و برقراری امنیت دیجیتالی ایجاد کرده است. نهادهایی نظیر دادگاه‌های شرعی و کمیسیون حقوق بشر مالزی در تفسیر جنبه‌های اخلاقی جرائم نوظهور دیجیتال و مدیریت چالش‌های کلان‌داده، نقشی کلیدی ایفا می‌کنند. به هر روی، انطباق موفقیت‌آمیز شریعت با قواعد حقوق مدرن در مالزی، مدلی راهبردی و عدالت‌محور را متجلی ساخته که ضمن تسهیل پیشرفت فناوری، پاسداری هم‌زمان از کرامت انسانی و حقوق پدید آورندگان اثر در فضای دیجیتالی را تضمین می‌نماید.

فهرست منابع

ایازی، رضا؛ شریفی‌طرازکوهی، حسین؛ پاکزاد، بتول و ساعدی‌بناب، بهزاد (۱۴۰۰). «ماهیت حقوق بشری آزادی بیان در بستر اینترنت و تکالیف دولت‌ها در این خصوص»، **مطالعات حقوق بشر اسلامی**، شماره ۲۰.

بذرپاچ، حمید (۱۴۰۱). «نقش دولت در امنیت اخلاقی اطفال در فضای سایبر در پرتو اسناد بین‌المللی»، **سیاست جهانی**، شماره ۲.

جلالی، محمود و توسلی اردکانی، سعیده (۱۳۹۸). «ضرورت ایجاد نظام هماهنگ حقوقی بین‌المللی در مقابله با جرائم در فضای مجازی»، **مطالعات حقوق عمومی**، شماره ۴.

خاف‌خانی، مهدی (۱۳۸۶). «فرصت‌های دیجیتالی در فضای سایبر و مسئله حقوق بشر»، **دانشنامه حقوق و سیاست**، شماره ۷.

ساکی، محمدرضا (۱۳۸۷). « ضمانت اجرای کیفری جرائم علیه حقوق بشر و حقوق بشر دوستانه»، **دیدگاه‌های حقوق قضایی**، شماره ۴۴.

شاکری، زهرا (۱۴۰۳). «برخی مؤلفه‌های مؤثر بر تحول نظام مالکیت فکری؛ گسترش یا تحدید قلمرو حقوق»، **تحقیق و توسعه در حقوق خصوصی**، شماره ۱.

شیرزاد، کامران (۱۳۸۸). **جرائم رایانه‌ای**، چاپ اول، تهران: نشر بهینه فراگیر.

ضیایی، سید یاسر (۱۳۹۶). «حمایت از حقوق بشر در فضای سایبر»، **پژوهش‌های حقوقی**، شماره ۳۱.

عسکری، پوریا (۱۴۰۱). **حقوق بشردوستانه در جنگ سایبری، در: دانشنامه رفتار سایبری**، به کوشش باقر شاملو، چاپ اول، تهران: بنیاد حقوقی میزان.

قناد، فاطمه و شریف، الهام (۱۴۰۰). «مطالعهٔ اجمالی حمایت از داده‌های شخصی در نظام حقوقی ایران و سند مقررات عمومی حفاظت از داده‌های اتحادیهٔ اروپا»، **حقوق فناوری‌های نوین**، شماره ۴.

کتانچی، الناز و پورقهرمانی، بابک (۱۳۹۸). «سیاست‌های نمادین معاهده جرائم سایبری شورای اروپا»، **مطالعات بین‌المللی**، شماره ۲.

محمودی، هادی و انصاری مهیاری، علیرضا (۱۴۰۱). «بررسی راه کارهای تقلیل حملات سایبری از منظر حقوق بین‌الملل بشردوستانه»، **مطالعات حقوقی فضای مجازی**، شماره ۳.

ملکوتی، رسول و خلیل‌زاده، مونا (۱۴۰۱). «راهکارهای حقوقی تأمین امنیت سایبری»، **مطالعات و تحقیقات وسایل ارتباط جمعی**، شماره ۱.

موسوی، سید جمال؛ روحانی مقدم، محمد و آقائی بجستانی، مریم (۱۴۰۱). «تدابیر پیشگیری از جرائم سایبری با تأکید بر اقدامات پلیسی با رویکردی فقهی»، **مطالعات فقه و حقوق اسلامی**، شماره ۲۶.

نمامیان، پیمان (۱۴۰۳). «ظرفیت نظام حقوقی مالزی در قبال ارتکاب جرائم دیجیتالی»، **آموزه‌های حقوق کیفری کشورهای اسلامی**، شماره ۴.

Reference

Alena Douhan (2022), "The Changing Nature of Sanctions in the Digital Age", in: Digital Transformations in Public International Law, Angelo Jr. Golia Matthias C. Kettemann Raffaela Kunz [Eds.], Published by Nomos, p. 129.

Kondo T, Katsenga NN, Zvidzayi T, Cybercrime and human rights: A case for the due process of internet criminals, Volume 6, Issue 2, 2018, p. 121.

Marshall Jarrett and Michael W. Bailie, Prosecuting Computer Crimes; Computer Crime and Intellectual Property Section Criminal Division, Published by Office of Legal Education Executive Office for United States Attorneys, 2011, p. 21.

M.E. Kabay, (2008), A Brief History of Computer Crime: An Introduction for Students. MSIA School of Graduate Studies, Norwich University.

Eoghan Casey (2011). Digital Evidence and Computer Crime (3rd Ed). Elsevier Inc publisher.

A Study on the Cyber-Crime and Cyber Criminals: A Global Problem, Volume: 03, June 2014, pp. 172-173.