



RESEARCH ARTICLE

Criminal Policy Imperatives in Addressing Platform-Based State Crimes

Hossein Javadi Hossein Abadi^{1*}, Azim Aghababaei Taghanaki²

1. Assistant Professor of Law, Faculty of Administrative Sciences and Economics, University of Isfahan, Isfahan, Iran

* Corresponding Author's Email: h.javadi@ase.ui.ac.ir

2. Ph.d. Student of Criminal Law and Criminology, Faculty of Law, Tarbiat Modares University, Tehran, Iran

Email: aghababaei.azim@modares.ac.ir

 <https://doi.org/10.22059/jppolicy.2026.109044>

Received: 1 June 2026

Accepted: 9 August 2026

ABSTRACT

Employing a descriptive-analytical approach, this article conceptualizes platform-based state crimes, delineates the structural and functional features of platforms that enable such offenses, and situates these dynamics within the broader landscape of digital state crime. The findings highlight several pressing criminal policy imperatives: the inadequacy and fragmentation of existing criminal policy frameworks; the amplification of state power through platform infrastructures; society's deep structural dependence on platforms and the resulting expansion of victimization; the multilayered and complex nature of platform-based state crimes; persistent ambiguities regarding state and platform responsibility for rights violations; the need for effective mechanisms of user redress; the imperative to safeguard digital human rights and prevent the consolidation of digital dictatorship; and the necessity of avoiding bias and discriminatory norm-setting in criminal policymaking. Collectively, these factors underscore the urgent need for coherent and robust criminal regulation in the domain of platform-based state crimes.

Keywords: State Crime; Platform-Based State Crime; Criminal Policy; Criminal Policymaking; Platforms.

Citation: Javadi Hossein Abadi, Hossein; Aghababaei Taghanaki, Azim (2026). Criminal Policy Imperatives in Addressing Platform-Based State Crimes. *Iranian Journal of Public Policy*, 12 (3), 180-195.

DOI: <https://doi.org/10.22059/jppolicy.2026.109044>

Published by University of Tehran



This Work Is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International \(CC BY-NC 4.0\)](https://creativecommons.org/licenses/by-nc/4.0/)



مقاله پژوهشی

ضرورت‌های سیاستگذاری جنایی در قبال جرایم حکومتی پلتفرمی

حسین جوادی حسین آبادی^{۱*}، عظیم آقابابائی طاقانکی^۲

۱. استادیار حقوق، دانشکده علوم اداری و اقتصاد، دانشگاه اصفهان، اصفهان، ایران

* رایانامه نویسنده مسئول: h.javadi@ase.ui.ac.ir

۲. دانشجوی دکتری حقوق کیفری و جرم‌شناسی، دانشکده حقوق، دانشگاه تربیت مدرس، تهران، ایران

رایانامه: aghababaei.azim@modares.ac.ir

doi <https://doi.org/10.22059/jppolicy.2026.109044>

تاریخ دریافت: ۱۱ خرداد ۱۴۰۵
تاریخ پذیرش: ۱۸ مرداد ۱۴۰۵

چکیده

مقاله پیش رو به روش توصیفی-تحلیلی ضمن شناسایی مفهوم جرایم حکومتی پلتفرمی و تبیین ویژگی‌های پلتفرم‌ها و جرایم ارتكابی در بستر آن‌ها، بر آن است که با پیوند این حوزه با جرایم حکومتی دیجیتال، به ضرورت‌های سیاستگذاری جنایی در این عرصه بپردازد. یافته‌های پژوهش نشان می‌دهد ناکارآمدی و عدم انسجام سیاست جنایی موجود، تشدید جرایم حکومتی به واسطه قدرت فوق‌العاده سکوها، وابستگی گسترده جامعه به پلتفرم‌ها و تعمیم بزه‌دیدگی، پیچیدگی ساختاری و چندلایه بودن جرایم حکومتی پلتفرمی، ابهام در مسئولیت پلتفرم‌ها و دولت در قبال نقض حقوق شهروندان، ضرورت ایجاد سازوکارهای جبران خسارت برای کاربران، لزوم رعایت حقوق بشر دیجیتال و جلوگیری از ایجاد دیکتاتوری دیجیتال و اجتناب از سوگیری در سیاست جنایی و هنجارگذاری تبعیض‌آمیز، از جمله ضرورت‌هایی است که هنجارگذاری جنایی در عرصه جرایم حکومتی پلتفرمی را اجتناب‌ناپذیر ساخته است.

واژگان کلیدی: جرم حکومتی، جرم حکومتی پلتفرمی، سیاست جنایی، سیاستگذاری جنایی، پلتفرم.

استناد: جوادی حسین آبادی، حسین؛ آقابابائی طاقانکی، عظیم (۱۴۰۵). ضرورت‌های سیاستگذاری جنایی در قبال جرایم حکومتی پلتفرمی. فصلنامه سیاستگذاری عمومی، ۱۲ (۳)، ۱۸۰-۱۹۵.

DOI: <https://doi.org/10.22059/jppolicy.2026.109044>



ناشر: دانشگاه تهران

مقدمه

ظهور و به کارگیری پلتفرم‌ها در بستر فناوری اطلاعات^۱ از شخصی‌ترین حوزه‌ها تا اجتماعی‌ترین وجوه زیست انسانی را متأثر ساخته است. پلتفرم‌ها یا سکوها، طیف گسترده‌ای از کنش‌های روزمره انسان را از خرید و فروش کالا و خدمات، جست‌وجوی اطلاعات برخط و برقراری ارتباطات اجتماعی گرفته تا سرگرمی، دسترسی به اخبار، حمل‌ونقل، اقامت، کارایی و جذب نیروی کار، دسترسی به برنامه‌های کاربردی و حتی کارکردهای سیاسی پشتیبانی می‌کنند و در نتیجه، نوعی وابستگی کارکردی در میان کاربران ایجاد کرده (West, 2019: 11)، در فرآیند نوآوری و خلق ارزش از اهمیت روزافزونی برخوردار شده‌اند (Sun et al, 2015: 1) در حال حاضر سکوها با ارائه طیف وسیعی از خدمات، از جمله تبادل اطلاعات، تبلیغات و تسهیل تجارت الکترونیک، نقش مثبتی برای کنشگران انسانی ایفا می‌کنند؛ همچنین سکوهای تجاری به واسطه قابلیت گردآوری و تحلیل کلان‌داده‌ها و نیز تمرکز منابع مالی و انسانی در درون خود، به سطحی از قدرت کم‌سابقه با ابعاد فراملی دست یافته‌اند (Davies et al, 2023: 253) و در پاره‌ای از موارد، این میزان از قدرت، از حدود اقتدار حاکمیت‌ها و دولت‌ها فراتر رفته است (O'Reilly, 201: 32). با این حال، هم‌زمان بستر نوینی را برای ارتکاب جرایم فراهم آورده‌اند (Hessam et al., 2021: 70). که فقدان سیاست‌های تنظیمی و کنترل‌گر (از جمله سیاست‌های جنایی) سبب تشدید این وضعیت‌های آسیب‌زا شده است. توضیح آنکه رفتارهای سکوها، با توجه به گستره کاربران و حجم حساب‌های فعال در این پلتفرم‌ها، در صورت عدم پایبندی به اصول اخلاقی و انسانی، می‌تواند زمینه‌ساز بهره‌برداری مجرمانه از آن‌ها گردد. در این چارچوب، اندیشه‌ها و کنش‌های جنایی نیز با اتکا به سکوها قادرند پیامدهای فاجعه‌بار و گسترده‌ای را رقم بزنند. یکی از جرایمی که ممکن است از طریق سکوها یا در بستر آن‌ها ارتکاب یابد، جرایم حکومتی است. ارتکاب این نوع بزه با استفاده قدرت فوق‌العاده سکوها، آثار به مراتب مخرب‌تری نسبت به سایر جرایم در فضای غیرپلتفرمی ایجاد خواهد کرد. مواجهه با این دسته از جرایم از طریق سازوکارهای سنتی حقوق کیفری، با دشواری‌های جدی مواجه بوده و در برخی موارد حتی ناممکن می‌نماید؛ از این‌رو، مداخله فعال سیاست‌گذاران جنایی در طراحی و اجرای خط‌مشی‌های ناظر بر پیشگیری، مقابله و کنترل جرایم ارتكابی در بستر سکوهای تجاری فناوری اطلاعات، امری ضروری تلقی می‌شود. نمونه‌های قابل توجهی از جرایم حکومتی وجود دارد که حکومت‌ها از طریق فضای مجازی جرایم ارتكابی خود را تسهیل نمودند. برای نمونه، رخداد‌های سال‌های ۲۰۱۶ و ۲۰۱۷ در کشور میانمار^۲ قابل ذکر است. در این کشور، یکی از عوامل مؤثر در وقوع کشتارهای جمعی مسلمانان، انتشار تبلیغات ضدانسانی علیه مسلمانان روهینگایا^۳ از طریق حساب‌های کاربری جعلی ایجاد شده توسط برخی اعضای ارتش تاتمادو^۴ و نیز اثرگذاری بر افکار عمومی و هدایت آن به سمت گرایش‌های خشونت‌آمیز علیه این گروه بوده است (Hamilton, 2022: 1351-1352). این الگوی کنش، از حیث کارکرد تبلیغی و اثرگذاری بر افکار عمومی، شباهت‌هایی با شیوه‌های پروپاگاندای تاریخی از جمله اقدامات رژیم نازی و نقش آدولف هیتلر در شکل‌گیری فضای ضدیهودی پیش از و در جریان هولوکاست^۵ دارد که در آن، زمینه‌های ذهنی و اجتماعی برای خشونت گسترده علیه یهودیان فراهم شد. با این حال، تفاوت اساسی در این است که سکوهای دیجیتال به دلیل ماهیت مبتنی بر دیده‌شدن، سرعت انتشار بالا و مقیاس‌پذیری گسترده، می‌توانند این گونه فرآیندهای اثرگذاری و بسیج افکار عمومی را با شتابی به مراتب بیشتر از الگوهای سنتی تاریخی پیش ببرند. در باب بیان اهمیت این موضوع باید دقت داشت که این حوزه در نقطه تلاقی سه عرصه حساس سیاست جنایی (با مرکزیت حقوق کیفری)، حکمرانی و فناوری‌های نوین قرار دارد و هرگونه غفلت نظری یا عملی در آن می‌تواند پیامدهای عمیقی برای حقوق بنیادین شهروندان و نظم عمومی به همراه داشته باشد. تحقق جرایم حکومتی در بستر پلتفرم‌های دیجیتال، به دلیل قدرت ساختاری این سکوها، آثار آن‌ها را چند برابر می‌کند. از سوی دیگر، «قدرت فوق‌العاده و فراملی سکوها» و نیز «وابستگی شدید جوامع به آن‌ها»

1. Information Technology (IT)

2. Myanmar

3. Rohingya

4. Tatmadaw

5. Holocaust

موجب شده است که خلأهای سیاست جنایی موجود، بیش از پیش آشکار گردد و ناکارآمدی ابزارهای سنتی حقوق کیفری در این عرصه نمایان شود. در چنین شرایطی، پرداختن به ضرورت‌های سیاست‌گذاری جنایی در این حوزه، نه تنها به توسعه ادبیات جرم‌شناسی در زمینه کمک می‌کند، بلکه می‌تواند مبنایی نظری برای اصلاح سیاست‌های کیفری، تضمین حقوق شهروندان و تحقق حکمرانی مطلوب در فضای سایبری فراهم آورد. این پژوهش زمینه‌ساز پژوهش‌های بعدی از جمله بایسته‌های سیاست‌گذاری جنایی، پیامدهای آن و همچنین ارائه مدل سیاست جنایی برای کنترل جرایم حکومتی پلتفرمی خواهد شد. براساس آنچه گفته شد مقاله پیش رو با طرح مفهوم جرایم حکومتی پلتفرمی با توجه به اهمیت روز افزون این فناوری و استفاده گسترده شهروندان از آن درصدد پاسخ به این پرسش است که چه ضرورت‌هایی سیاست‌گذاری جنایی در عرصه جرایم حکومتی پلتفرمی را اجتناب ناپذیر ساخته است؟ برای پاسخ به این پرسش لازم است ضمن فهم دقیق مفهوم پلتفرم و جرایم حکومتی پلتفرمی توضیح داد که چرا جرایم حکومتی پلتفرمی در حال حاضر آنچنان شیوع یافته است که اگر در عرصه سیاست‌گذاری جنایی به آن پرداخته نشود با نقض انواعی از حقوق شهروندان جرایم حکومتی پرشماری رخ خواهد داد. البته طبیعی است که به سادگی نمی‌توان حکومتی که خود از پلتفرم‌ها در جهت سلب حقوق شهروندان بهره جسته است را به سمت سیاست‌گذاری جنایی در این عرصه ترغیب نمود. چرا که «دولت قواعدی برای مجازات کردن خود وضع نمی‌کند و انگهی در حال حاضر با طرح اندیشه دولت قانونمند به جای دولت قانونی، قدرت دولت تابع حقوق و محدود می‌باشد. بنابراین حقوق می‌تواند قدرت دولت را محدود کند» (Shiri, 2021: 199). بنابراین با حرکت به سمت دولت حقوقی که مبتنی بر هنجارهای فرا قانونی است امکان سیاست‌گذاری جنایی در عرصه جرایم حکومتی و به صورت ویژه جرایم حکومتی پلتفرمی پدید می‌آید. چراکه این رفتارهای زیانبار دولت در این عرصه می‌تواند بر خلاف موازین شرعی، انسانی، طبیعی و اجتماعی تلقی شود و با مبانی حقوق در تعارض قرار گیرد. در نتیجه اگر سیاستگذار را به این مهم واقف کنیم که اثرات ارتکاب جرم حکومتی در بلندمدت دامن حاکمیت را فرا خواهد گرفت و استمرار قدرت را با چالش مواجه می‌سازد، به هنجارگذاری جنایی در عرصه جرایم حکومتی پلتفرمی رغبت خواهد کرد.

پلتفرم‌ها و لزوم سیاست‌گذاری جنایی افتراقی

پلتفرم^۱ به معنای «سکو» است. در فرهنگ لغت آکسفورد، «پلتفرم» به عنوان سطحی برجسته تعریف شده است که افراد یا اشیا می‌توانند بر روی آن قرار گیرند یا بایستند (Dictionary, 2008, p.335). به عقیده برخی، سکو مجموعه‌ای از نرم‌افزارها، سخت‌افزارها و برنامه‌های کاربردی را در بر می‌گیرد (Chappell, 2011, pp. 8-9) و فناوری همه منظوره‌ای است که گروهی از برنامه‌ها^۲ را به هم پیوند می‌دهد (Fichman, 2004, p.132). پلتفرم‌های فناوری اطلاعات، ماهیتی سایبری-شرکتی^۳ داشته (Moro Visconti, 2020, p.1; Volkov & Sidorenko, 2022, p.3) و در نتیجه، مفهوم محیط فیزیکی و اجتماع را از وضعیت عینی و ملموس آن به سمت بستر و فضای مجازی دگرگون ساخته‌اند. علی رغم تعاریف یاد شده به نظر می‌رسد هنوز در ادبیات علمی برداشت یکپارچه‌ای از این مفهوم شکل نگرفته است (Hamilton, 2022, p.1353). نیل به این هدف از طریق شناسایی کاربرد سکوها و همچنین ویژگی‌های آن میسر خواهد شد. یکی کارکردهای سکوها آن است که با کمک نرم‌افزارها امکان استفاده کاربران از خدمات خود را فراهم می‌سازد (Taudes et al., 2000, pp. 228-229) و بدین وسیله امکان تبادل مستمر و پرسرعت اطلاعات میان کاربران در بستر فضای مجازی را فراهم می‌کند (Rai et al., 2006, p. 227). این مفهوم دارای شش بُعد اساسی است. بُعد نخست، فناوری پایه یا بستر فناورانه^۴ است (Hagiu, 2014, p.71; Riemer & Richter, 2010, p.9; Tiwana et al., 2010, p.256) که زمینه توسعه افزونه‌ها را فراهم

1. Platforms

2. Applications

3. Cyber-corporate

4. Technological Base

می‌سازد. بعد دوم شامل استانداردها (Rai et al., 2006, p. 227)، قوانین و مقررات (Kraemer et al., 2010, p. 1) و ارتباط‌ها است (Lahiri et al., 2010, p. 81; Meyer & Seliger, 1998, p. 61; Tiwana et al., 2010, pp. 675-676). که ناظر بر قواعد و استانداردهای دسترسی به سکو از مکان‌ها و زمان‌های مختلف می‌باشد. بعد سوم به افزونه‌ها^۱ اختصاص دارد؛ اعم از برنامه‌های کاربردی (Bergvall-Kåreborn & Ceccagnoli et al., 2012, p. 263; Taudes et al., 2000, pp. 228-229)، مکمل‌ها (Jain et al., 2006, p. 184)، که در واقع نرم‌افزارهای متصل به سکو هستند و قابلیت‌های تجاری آن را فعال می‌کنند. بعد چهارم، تعامل‌پذیری یا قابلیت همکاری^۲ است که با مفاهیمی همچون تعامل^۳ (Tiwana et al., 2010, p. 268) توسعه^۴ (Anderson Jr et al., 2014, p. 156) اتصال^۵ (Riemer & Richter, 2010, p. 1) یا قابلیت اشتراک‌گذاری^۶ بیان می‌شود (Dhar & Sundararajan, 2007, p. 134). بعد پنجم، تراکنش‌پذیری^۷ (Sun et al., 2015, p. 5) است که شامل انواع تبادلات^۸، تعاملات^۹ و معاملات^{۱۰} می‌شود. و النهایه بعد ششم، حاکمیت^{۱۱} مربوط هست که به سیاست‌ها، ساختارها، فرایندها و سازوکارهای مدیریت سکو اشاره دارد (Sun et al., 2015, p. 7). فلذا سیستم مربوط به یک سکو یک سیستم پیچیده متشکل از اجزای بسیاری است. پیچیدگی‌های حکمرانی پلتفرم‌ها به‌گونه‌ای فزاینده با مفاهیم حقوقی و اقتصادی محدودی که بر آن استوار است در تعارض قرار می‌گیرد؛ از این رو، تحلیل ساختار لایه‌ای پلتفرم‌ها و تمرکز قدرت عمودی در میان آن‌ها، نقطه عزیمت ضروری برای هرگونه تنظیم‌گری مؤثر به شمار می‌رود (van Dijck, 2020, pp. 2802 & 2814). علاوه بر ابعاد پیش‌گفته، پلتفرم‌ها دارای ویژگی‌های منحصر به فردی هستند که سیاست‌گذاری جنایی افتراقی در خصوص آن‌ها را اجتناب‌ناپذیر ساخته است؛ ویژگی‌هایی از قبیل اتکای گسترده به الگوریتم‌ها و کلان‌داده‌ها که امکان دستکاری روان‌شناختی کاربران و جهت‌دهی به ادراک، ترجیحات و تصمیمات آنان را فراهم می‌آورد (Susser et al., 2019, p. 1)؛ ایجاد و تقویت وابستگی ساختاری و روزافزون کاربران به خدمات پلتفرمی به‌گونه‌ای که این سکوها به بخش جدایی‌ناپذیر زیست روزمره تبدیل شده‌اند (Perakslis & Quintana, 2023, p. 1)؛ مقیاس‌پذیری و سرعت انتشار بسیار بالا که امکان گسترش سریع محتوا، از جمله محتوای زیان‌بار یا مجرمانه، را در سطحی گسترده و حتی فراملی فراهم می‌سازد قابلیت ناشناس‌سازی و پنهان‌سازی هویت که شناسایی مرتکبان و انتساب رفتارهای مجرمانه را با چالش‌های جدی مواجه می‌کند (Hashmi et al., 2025, p. 255)؛ تمرکز بی‌سابقه قدرت اقتصادی، اطلاعاتی و ارتباطی در دست گردانندگان پلتفرم‌ها (Sun et al., 2015, p. 1) که در برخی موارد از قدرت دولت‌ها نیز فراتر می‌رود؛ و نیز پیچیدگی فنی و چندلایه بودن ساختار این سکوها به‌مثابه نظام‌هایی سایبری-شرکتی که از اجزای متنوع و درهم‌تنیده تشکیل شده‌اند (Moro Visconti, 2020, p. 1; Volkov & Sidorenko, 2022, p. 3). ویژگی‌های پیش‌گفته، کنش مجرمانه را در بستر خود از سطوح ساده به سطوح چندوجهی، پنهان، ترکیبی و پیچیده تغییر داده و مشکلاتی از قبیل ایجاد بزه‌دیدگی‌های جمعی، جرایم گسترده، عدم قابلیت شناسایی مرتکب، عدم قابلیت انتساب و مانند آن را رقم زده است. وانگهی، همه این چالش‌ها زمانی که مرتکب جرم، حکومت باشد به‌صورت قابل توجهی تشدید خواهد شد. لذا اگرچه پرداختن به جرایم ارتكابی توسط اشخاص عادی از طریق پلتفرم‌ها واجد اهمیت است و سیاست‌گذاری دقیقی را می‌طلبد، اما آنگاه که مرتکب جرم دولت باشد، آثار و پیامدهای

1. Add-ons
2. Plug-ins
3. Interoperability
4. Interoperate
5. Expend
6. Connect
7. Shareable
8. Transactionality
9. Exchanges
10. Interactions
11. Transactions
12. Governance

جرایم حکومتی پلتفرمی به مراتب گسترده‌تر و شدیدتر خواهد بود. از این رو، لازم است جرم حکومتی پلتفرمی مفهوم‌سازی شود و سیاست‌گذاری جنایی پیرامون آن تدوین شود.

جرم حکومتی پلتفرمی

جرم حکومتی پلتفرمی در بستر فناوری اطلاعات به آن دسته از رفتارهای مجرمانه یا ناقض حقوق بنیادین اطلاق می‌شود که در آن، نهادهای حکومتی به طور مستقیم یا غیرمستقیم با بهره‌گیری از زیرساخت‌ها و ظرفیت‌های سکوها دیجیتال، به ارتکاب، تسهیل یا حمایت از اعمال زیان‌بار علیه شهروندان مبادرت می‌ورزند. به دیگر سخن در جرایم حکومتی پلتفرمی حکومت‌ها یا نهادهای وابسته با استفاده از پلتفرم‌های دیجیتال مرتکب نقض حقوق شهروندان می‌شوند. برخی از گونه‌های جرایم حکومتی پلتفرمی عبارتند از نظارت فراگیر بدون مبنای قانونی، نقض حریم خصوصی، نقض حق دسترسی به اطلاعات، دستکاری اطلاعات، سانسور یا عملیات نفوذ، سوءاستفاده از داده‌های شهروندان، مهندسی افکار عمومی، استفاده از پلتفرم‌ها برای سرکوب سیاسی یا تبعیض و.... این مفهوم در نقطه تلاقی «جرایم حکومتی» و «بزهکاری پلتفرمی» شکل گرفته و ناظر بر وضعیتی است که در آن، قدرت حاکمیتی در بسترهای فناورانه، از طریق ابزارهایی چون داده‌کاوی، نظارت گسترده یا کنترل اطلاعات، به نقض آزادی‌ها و حقوق اساسی می‌انجامد. از این رو، جرم حکومتی پلتفرمی واجد ویژگی‌هایی همچون سازمان‌یافتگی، پیچیدگی فنی، مقیاس‌پذیری و آثار گسترده اجتماعی است که آن را از اشکال سنتی بزهکاری متمایز می‌سازد. همچنین جرایم حکومتی پلتفرمی از این جهت که نامرئی هستند و حکومت به عنوان عامل وقوع جرم می‌تواند متوسل به انواع پنهان‌کاری‌ها شود از جرایم سنتی خطرناک‌تر هستند. قدرتی که پلتفرم‌ها در اختیار حکومت‌ها قرار می‌دهند بدون آنکه در قبال اقدامات خود پاسخگو باشند زمینه سوء استفاده ساختاری حکومت از آن‌ها را فراهم نموده و باعث می‌شود بدون آنکه حکومت در معرض اعتراض و اغتشاش قرار گیرد جرایم حکومتی واقع شده و دولت به اهداف خویش برسد. در واقع حکومت‌ها در طول زمان آموختند که جرم حکومتی را نه به صورت علنی و قابل رویت بلکه به صورت پنهانی و استتار شده انجام دهند تا از تبعات آن در امان باشند. از منظر رویکردهای پست مدرن می‌توان گفت که حکومت‌ها با به خدمت گرفتن دانش در عصر جدید به سمت کنترل‌گری همه‌جانبه و انقیاد شهروندان حرکت نموده و بدون آنکه هزینه آن را بپردازند و مسئولیتی متوجه آنان باشد مجموعه از حقوق شهروندان را در لوای فعالیت‌های به ظاهر مشروع و قانونی نقض می‌کنند و در همان حال ندای پای‌بندی به حقوق بشر سر داده و خود را تابع آن نشان می‌دهند. البته استخدام دانش در نقض حقوق شهروندان منحصر به کشورهای توسعه یافته نیست. بلکه در گذر زمان در پرتو تعامل این کشورها با کشورهای در حال توسعه همان گونه یک بزهکار عادی در پرتو همنشین‌های افتراقی شیوه‌های ارتکاب جرم را می‌آموزد کشورهای در حال توسعه نیز از قدرتهای جهانی آموختند که چگونه بدون آنکه برای آن‌ها هزینه‌های چندانی داشته باشند حقوق شهروندان خویش را نقض کرده، انواعی از جرایم حکومتی را مرتکب شوند. جز آنکه کشورهای در حال توسعه در این میان گوی سبقت را از آموزگار خویش ربوده و چنان در این عرصه تاختند که هیچ چیز و هیچ کس را یارای مهار آن‌ها نیست. به تدریج با توسعه دانش‌های مبتنی بر فناوری ارتباطات و اطلاعات جریان پیش گفته شدت یافت و جرایم حکومتی از مدل‌های سنتی به سمت شیوه‌های نوین تغییر جهت داد. این تحول با تولد و گسترش فضای سایبر سرعت چشم‌گیری را تجربه نمود و به صورت پیوسته توسعه یافت تا عصر رایانه و نرم افزارهای سنتی به پایان خویش نزدیک و دوره پلتفرم‌ها آغاز گردد. به ترتیبی که در حال حاضر چنان پلتفرم‌ها با زندگی بشر آمیخته شده است که حیات بدون آن برای بسیاری ناممکن است. در چنین شرایطی حکومت‌ها که راه ورود حریم خصوصی شهروندان را بدون نیاز به دستور قضایی و موازین آیین دادرسی کیفری یافته‌اند! با ایجاد، حمایت و پشتیبانی از پلتفرم‌های حکومت ساخته مهمان شهروندانی شدند که خود آنان را به ضیافت کنترل‌گری گسترده دعوت کرده بودند و چه چیز برای حکومت شیرین‌تر از این رخداد مبارک! بدین سان حکومت‌ها با بزک کردن پلتفرم‌ها، ایجاد محتوای سرگرم‌کننده مانند فیلم، موسیقی و مانند آن، الزام به نصب برخی از آن‌ها برای انجام امور اداری، مسدودسازی سایر راه‌های اخذ خدمات

پیوندی ناگسستنی میان پلتفرم‌ها و زندگی شهروندان برقرار نموده و خود را تبدیل به ناظر دائمی زندگی آنان نمودند. البته در این مسیر از انواعی از فریب‌کاری‌ها استفاده نموده و لزوم استفاده از پلتفرم‌ها را به مصلحت شهروندان، صرفه جویی در وقت، سرعت در اخذ خدمت، کاهش هزینه و مانند آن مرتبط ساخته تا شهروندان نفهمند که همه این فناوری‌ها برای کنترل‌گری حکومت در عرصه حریم خصوصی متولد شده است. وانگهی در حال حاضر با نمایان شدن جرایم حکومتی پلتفرمی سیاستگذار را گزیری از انتخاب دو مسیر نیست. یکی استفاده از فنون خنثی‌سازی (انکار جرایم حکومتی پلتفرمی، انکار بزه دیدگان جرایم حکومتی پلتفرمی، عدم پذیرش مسئولیت ناشی از جرایم حکومتی پلتفرمی، توسل به ارزش‌های برتر برای استمرار رفتار مجرمانه) و دیگری پذیرش سیاستگذاری جنایی در این عرصه. هرچند حکومت‌ها غالباً شیوه نخست را بر می‌گزینند. ولی استفاده از این شیوه‌ها هر چند در کوتاه مدت موثر ولی در بلند مدت ناکارآمد است. لذا حکومت را گزیری انتخاب مسیر دوم و سیاستگذاری جنایی در عرصه جرایم حکومتی پلتفرمی نیست. برای نیل به این هدف نیازمند شرح توجیهات ضرورت سیاستگذاری جنایی در این عرصه هستیم.

توجیهات ضرورت سیاستگذاری جنایی در عرصه جرایم حکومتی پلتفرمی

تبیین توجیهات ناظر بر ضرورت سیاستگذاری جنایی در عرصه جرایم حکومتی پلتفرمی از اهمیت بنیادین برخوردار است؛ زیرا بدون درک دقیق زمینه‌ها و ملاحظات حاکم بر این حوزه، هرگونه مداخله تقنینی یا اجرایی با خطر ناکارآمدی یا حتی نقض حقوق بنیادین شهروندان مواجه خواهد بود.

ناکارآمدی و عدم انسجام سیاست جنایی موجود

ناکارآمدی و عدم انسجام سیاست جنایی موجود در ایران در مواجهه با «جرایم حکومتی پلتفرمی» را باید به صورت منسجم و در پیوند میان دو خلأ بنیادین تحلیل کرد: نخست، غفلت ساختاری از جرم حکومتی در سیاست جنایی، و دوم، ضعف جدی در تنظیم‌گری و کنترل بزه‌کاری پلتفرمی. این دو کاستی، در تعامل با یکدیگر، وضعیت کنونی را به مرحله‌ای رسانده‌اند که نظام عدالت کیفری عملاً فاقد ظرفیت لازم برای مواجهه مؤثر با این پدیده نوظهور است. در گام نخست، سیاست جنایی ایران اساساً بر مبنای الگوهای سنتی و فردمحور شکل گرفته و در آن، جرم به عنوان کنشی فردی و منفک از ساختار قدرت تصور شده است (Ardebili, 2015: 58). این در حالی است که جرایم حکومتی، بنا به ماهیت خود، در بستر ساختارهای قدرت و در چارچوب سازمان‌های رسمی رخ می‌دهند و واجد ویژگی‌هایی همچون سازمان‌یافتگی، پیچیدگی و پیوند با منافع سیاسی و اقتصادی هستند. بر همین اساس، در ادبیات جرم‌شناسی تأکید می‌شود که این دسته از جرایم را نمی‌توان با رویکردهای تک‌ساحتی تحلیل و کنترل کرد و نیازمند چارچوب‌های تلفیقی و چندسطحی هستند. با وجود این، در سیاست جنایی تقنینی و اجرایی ایران، نه تعریف روشنی از جرم حکومتی ارائه شده و نه سازوکار مشخصی برای پیشگیری، شناسایی و پاسخ‌دهی به آن پیش‌بینی گردیده است. نتیجه این غفلت، شکل‌گیری خلأیی است که در آن، رفتارهای زیان‌بار ناشی از سوءاستفاده از قدرت، یا اساساً خارج از دایره جرم‌انگاری قرار می‌گیرند یا در قالب عناوین کلی و غیرمتناسب مورد رسیدگی قرار می‌گیرند. این کاستی زمانی ابعاد جدی‌تری می‌یابد که به بستر پلتفرم‌های دیجیتال منتقل می‌شود. در این حوزه نیز سیاست جنایی ایران با نارسایی‌های عمیق مواجه است. از منظر تقنینی، یکی از مهم‌ترین مشکلات، «فقدان تعاریف روشن و مصادیق دقیق جرایم در بستر پلتفرم‌های دیجیتال» است که موجب می‌شود مراجع قضایی با تفسیرهای متفاوت و گاه متعارض از قوانین مواجه شوند و در نتیجه، آرای ناهمگون و متناقض صادر گردد. به ترتیبی که قوانین مجازات اسلامی، آیین دادرسی کیفری، قانون جرایم رایانه‌ای و ... نتوانسته‌اند در حال حاضر برای این معضل پاسخ مناسبی ارائه کنند. این وضعیت، نه تنها به عدم قطعیت حقوقی و تضعیف عدالت قضایی منجر می‌شود، بلکه امکان بهره‌برداری بزه‌کاران از خلأهای قانونی را نیز فراهم می‌سازد. در سطح قضایی و اجرایی نیز این ناکارآمدی به وضوح قابل مشاهده است. فقدان مبنای روشن در سیاستگذاری جنایی، موجب شده است که رسیدگی‌های قضایی در بسیاری موارد تابع برداشت‌های شخصی و سلیقه‌ای

باشد و «صدور آرای مختلف و حتی متضاد از سوی مراجع قضایی» به یک رویه نسبتاً رایج تبدیل شود. این امر، علاوه بر نقض اصل برابری در برابر قانون، به تضعیف اعتماد عمومی به نظام عدالت کیفری نیز منجر می‌شود. از سوی دیگر، نبود سازوکارهای پیشگیرانه مؤثر موجب شده است که سیاست جنایی در برابر تحولات سریع فناوری، همواره در وضعیت انفعالی قرار گیرد. عامل مهم دیگری که به عدم انسجام سیاست جنایی دامن زده، «تعدد مراجع سیاست‌گذار و فقدان هماهنگی میان آن‌ها» است. در چنین وضعیتی، هر یک از نهادها بدون وجود یک چارچوب کلان و منسجم، اقدام به وضع مقررات یا اتخاذ تصمیماتی می‌کنند که لزوماً با یکدیگر همخوانی ندارند. این چندپارگی نهادی، به‌ویژه در حوزه جرایم نوظهور پلتفرمی، موجب شده است که خطوط مشی واحد و منسجمی برای کنترل بزه‌ها شکل نگیرد. در نتیجه، نه تنها کارآمدی سیاست جنایی کاهش می‌یابد، بلکه امکان اعمال یک رویکرد جامع و هماهنگ در پیشگیری و مقابله با جرایم نیز از میان می‌رود. در نهایت، باید تأکید کرد که ترکیب این نارسایی‌ها یعنی فقدان توجه به جرایم حکومتی از یک سو و ضعف ساختاری در مواجهه با جرایم پلتفرمی از سوی دیگر منجر به شکل‌گیری یک وضعیت دوگانه از ناکارآمدی شده است. در چنین شرایطی، نه ابزارهای سنتی حقوق کیفری توانایی کنترل بزهکاری در بسترهای دیجیتال را دارند و نه سیاست‌های موجود قادرند به چالش‌های ناشی از پیوند قدرت حاکمیتی و فناوری‌های نوین پاسخ دهند. از این‌رو، بازنگری بنیادین در سیاست جنایی و حرکت به سوی طراحی چارچوبی منسجم، شفاف و متناسب با ماهیت جرایم حکومتی پلتفرمی، ضرورتی اجتناب‌ناپذیر به نظر می‌رسد.

تقویت شدت جرایم حکومتی با قدرت فوق‌العادهی سکوها

سکوه‌های تجاری فناوری اطلاعات در دهه‌های اخیر به موقعیتی کم‌نظیر در اقتصاد جهانی دست یافته‌اند؛ موقعیتی که نه تنها در سطح ملی، بلکه در عرصه فراملی نیز مولد قدرت بوده است. این سکوها با اتکا به ماهیت شبکه‌ای و داده‌محور خود، توان عبور از مرزهای جغرافیایی و حاکمیتی را داشته و با اتصال میلیون‌ها کاربر، سرمایه‌گذار و کسب‌وکار، زمینه‌ای فراهم می‌آورند که در پرتو آن، کارآمدی و اعمال مقررات کیفری سرزمینی با چالش‌های جدی مواجه می‌شود (Razmetaeva et al., 2021, p. 167) از این‌رو، پژوهشگران از مفاهیمی همچون «حاکمیت سکویی» (Gillespie, 2017, p. 254; Gorwa, 2019, p. 854) و حتی «دولت به‌مثابه سکو» (Bracken, 2015; Yakhchali et al., 2020: 204) سخن به میان آورده‌اند؛ مفاهیمی که بیانگر آن است که سکوها در برخی حوزه‌ها، به‌نحوی کارکردهای سنتی دولت‌ها را بازتولید یا حتی جایگزین کرده‌اند. با وجود آن که سکوه‌های تجاری فناوری اطلاعات در چارچوب بسترهای خود به نوعی مقررده‌گذاری مبادرت می‌ورزند و با توجه به گستره فراملی و جمعیت انبوه کاربران، از این حیث به سطحی از قدرت چشمگیر دست یافته‌اند (Bloch-Wehba, 2019, p. 27) با این حال، باید توجه داشت که قدرت و گستره فراملی سکوها عمدتاً ناشی از انباشت کلان‌داده‌هایی است که در اختیار دارند و نیز ظرفیت کم‌نظیر آن‌ها در تحلیل و بهره‌برداری از این داده‌ها. به‌عنوان نمونه، شرکت‌هایی نظیر Amazon، Google و Meta نه تنها خدمات متنوعی را به کاربران در کشورهای مختلف عرضه می‌کنند، بلکه در عمل، الگوهای مصرف، سازوکارهای تبلیغاتی و حتی جهت‌گیری‌های اقتصادی را در مقیاس جهانی تحت تأثیر قرار می‌دهند. این گستره نفوذ موجب شده است که بسیاری از دولت‌ها در فرآیند سیاست‌گذاری اقتصادی، ناگزیر از لحاظ‌کردن نقش و اثرگذاری این سکوها باشند؛ به‌گونه‌ای که تغییرات در تصمیمات و الگوریتم‌های آن‌ها می‌تواند آثار مستقیم و قابل‌توجهی بر بازارهای ملی بر جای گذارد. گسترش قدرت فراملی سکوها صرفاً به حوزه اقتصادی محدود نمی‌شود، بلکه پیامدهای سیاسی و حقوقی عمیقی را نیز به دنبال دارد. این پلتفرم‌ها قادرند جریان اطلاعات، نحوه شکل‌گیری افکار عمومی و حتی فرآیندهای انتخاباتی را متأثر سازند. تحول قدرت پلتفرم‌ها از یک نیروی اقتصادی صرف به بازیگر سیاسی-حقوقی، موجب شده است که نه تنها الگوهای رقابت بازاری، بلکه موازین نهادی ناظر بر آزادی بیان، مدیریت محتوا و نظارت بر داده‌های کاربران نیز به‌طور جدی در معرض تغییر قرار گیرند؛ این امر، شکاف‌های موجود در پاسخگویی را بیش از پیش آشکار می‌سازد (Sander, 2021, pp. 159 & 161 & 192). تلاقی قدرت فزاینده و فراملی سکوه‌های دیجیتال با ساختارهای حاکمیتی،

در صورتی که در مسیر ارتکاب یا تسهیل جرایم حکومتی قرار گیرد، به یکی از مخاطره‌آمیزترین اشکال بزهکاری در عصر دیجیتال تبدیل می‌شود. در چنین وضعیتی، ظرفیت‌های بی‌سابقه سکوها در گردآوری، تحلیل و کنترل کلان‌داده‌ها، این امکان را فراهم می‌آورد که مداخلات حکومتی در حوزه‌هایی چون نظارت، کنترل اطلاعات و هدایت افکار عمومی، با دقت، گستره و پنهان‌کاری بیشتری انجام شود. این امر، مرز میان تنظیم‌گری مشروع و مداخله مجرمانه را تیره ساخته و امکان پاسخ‌گویی و نظارت مؤثر را به شدت کاهش می‌دهد. افزون بر این، مقیاس‌پذیری و نفوذ گسترده این سکوها موجب می‌شود که آثار چنین جرایمی، نه محدود به یک قلمرو ملی، بلکه در سطحی وسیع و حتی فراملی بروز یابد. از این رو، هم‌افزایی میان قدرت سکویی و اقتدار حکومتی، در صورت فقدان سیاست‌گذاری جنایی کارآمد، می‌تواند به شکل‌گیری نوعی «بزهکاری ساختاری پنهان» منجر شود که کنترل و مهار آن به مراتب دشوارتر از اشکال سنتی جرم است.

وابستگی گسترده جامعه به سکوها و تعمیم بزه‌دیدگی

وابستگی فزاینده کاربران به خدمات سکوهای تجاری و اجتماعی را می‌توان از برجسته‌ترین پیامدهای گسترش فناوری‌های نوین تلقی کرد. این وابستگی در ابتدا در نتیجه عواملی نظیر سهولت دسترسی، سرعت ارائه خدمات، کاهش هزینه‌ها و جذابیت‌های تعاملی شکل گرفت، اما به تدریج به یک نیاز بنیادین و در مواردی به حالتی شبه‌اعتیادی تبدیل شده است. (Perakslis & Quintana, 2023, p. 1). امروزه، طیفی گسترده از فعالیت‌ها - از خرید کالا و خدمات، حمل‌ونقل، بانکداری و امور مالی تا ارتباطات اجتماعی و سرگرمی - به‌طور فزاینده‌ای در بستر پلتفرم‌ها متمرکز شده‌اند، به گونه‌ای که اختلال در دسترسی به این خدمات می‌تواند زندگی روزمره کاربران را با چالش‌های جدی مواجه سازد. از سوی دیگر، افزایش این وابستگی به فناوری اطلاعات، فضای سایبری و به‌ویژه سکوها، فرصت‌های نوینی برای ارتکاب جرایم سایبری فراهم آورده است (Drew, 2020, p.17). یافته‌های برخی تحقیقات میدانی، به‌ویژه در خصوص سکوهایی مانند تیک‌تاک، حاکی از شکل‌گیری نوعی «اعتیاد رفتاری»¹ در بستر سکویی است. (Yang et al., 2025, p. 2106) چنین وابستگی عمیقی موجب شده است که سکوهای تجاری فناوری اطلاعات به‌مثابه زیرساخت‌های حیاتی جامعه تلقی شوند؛ به نحوی که قطع یا محدودسازی آن‌ها می‌تواند پیامدهای گسترده اجتماعی، اقتصادی و حتی سیاسی در پی داشته باشد. از منظر سیاست جنایی، این سطح از وابستگی واجد کارکردی دوگانه است: از یک سو می‌تواند بستری برای ارتقای نظم اجتماعی، توسعه عدالت خدماتی، افزایش دسترسی عمومی و تسهیل تعاملات اجتماعی فراهم آورد؛ و از سوی دیگر، زمینه‌ساز تهدیداتی همچون سوءاستفاده‌های مجرمانه، نظارت پنهان، دستکاری‌های روان‌شناختی و حتی نفوذ ایدئولوژیک گردد. بدین ترتیب، هرچه میزان وابستگی جامعه به این سکوها افزایش یابد، به همان نسبت، آسیب‌پذیری آن در برابر اختلالات سیستمی، دستکاری اطلاعاتی و جرایم سازمان‌یافته نیز تشدید خواهد شد. تلاقی جرم حکومتی با بزهکاری پلتفرمی در بستری که کاربران وابستگی عمیقی به سکوها یافته‌اند، مخاطره‌ای مضاعف و ساختاری ایجاد می‌کند؛ زیرا در این وضعیت، ابزارهای حیاتی زندگی روزمره می‌توانند به مجرای اعمال قدرت و ارتکاب رفتارهای زیان‌بار تبدیل شوند. این هم‌پوشانی، امکان سوءاستفاده از داده‌های گسترده کاربران و هدایت یا دستکاری رفتار و ادراک آنان را در مقیاسی وسیع فراهم می‌سازد و در نتیجه، بزه‌دیدگی نه به صورت فردی، بلکه به صورت جمعی و نظام‌مند رخ می‌دهد. افزون بر این، وابستگی شدید کاربران به خدمات سکویی، قدرت مقاومت اجتماعی در برابر این مداخلات را کاهش داده و امکان تداوم و پنهان‌سازی چنین جرایمی را تقویت می‌کند. در نهایت، این وضعیت می‌تواند به تضعیف اعتماد عمومی، اختلال در نظم اجتماعی و شکل‌گیری نوعی کنترل نامرئی اما فراگیر بر زیست دیجیتال شهروندان بینجامد.

1. Behavioral Addiction

پیچیدگی ساختاری و چندلایه بودن جرایم حکومتی پلتفرمی

پیچیدگی ساختاری و چندلایه بودن جرایم حکومتی پلتفرمی از این واقعیت ناشی می‌شود که این جرایم در نقطه تلاقی سه نوع قدرت شکل می‌گیرند: قدرت حکومت، قدرت فناوری/پلتفرم و قدرت داده. از این رو، این جرایم نه تک‌لایه‌اند و نه با الگوهای سنتی جرم‌شناسی به‌طور کامل قابل تحلیل هستند. در لایه ساختاری، قدرت حکومتی در بستر دیجیتال به‌صورت بی‌مهابا اعمال می‌شود و در فضای سایبری، مرز میان «اقدام قانونی» و «سوءاستفاده حکومتی» قابل تشخیص نیست؛ به‌گونه‌ای که امکان انوعای از پنهان‌کاری‌ها و توجیه‌گری‌ها فراهم می‌شود. بررسی موردی پلتفرم‌های یکپارچه‌سازی و تحلیل داده در بخش عمومی نشان می‌دهد که نظارت دولت بر خود از طریق این پلتفرم‌ها نه تنها با چالش‌های نهادی جدی مواجه است، بلکه عوامل سیاسی نقش تعیین‌کننده‌ای در شکل‌گیری تنظیم‌گری عملی دارند و ابزارهای کنترل دموکراتیک، همچون تفکیک قوا و شفافیت عمومی، بیشترین اهمیت را در این عرصه دارا هستند (Ulbricht et al., 2024, pp. 1-2). از سوی دیگر، در لایه فناوری، پلتفرم‌ها ذاتاً متمرکز، مقیاس‌پذیر و داده‌محور هستند و همین ویژگی‌ها موجب می‌شود که حکومت‌ها بتوانند از زیرساخت‌های آن‌ها برای نظارت، کنترل و مداخله استفاده کنند. در این میان، علاوه بر پلتفرم‌های حکومتی، حتی پلتفرم‌های خصوصی نیز ممکن است ناخواسته به ابزاری برای ارتکاب جرایم حکومتی تبدیل شوند. در لایه داده، با توجه به انباشت گسترده داده‌ها در پلتفرم‌ها، امکان تحلیل و بهره‌برداری پیشرفته از آن‌ها فراهم می‌شود؛ به‌نحوی که حجم کلان داده‌های کاربران، تحلیل‌های پیش‌بینانه و قابلیت پروفایل‌سازی سیاسی را تسهیل می‌کند. کاربرد الگوریتم‌ها در نظارت دولتی با به چالش کشیدن مفروضات سنتی درباره مفهوم «کارگزاری» در حقوق بشر، روش‌های نوینی از نظارت را ایجاد کرده است که ضمانت‌های اطلاع‌رسانی و جبران خسارت، به‌مثابه دو ضمانت حیاتی در پرونده‌های نظارت مخفیانه، را در عمل ناکارآمد می‌سازند (Kosta, 2020, p. 212). این وضعیت در شرایطی رخ می‌دهد که چارچوب حقوقی مؤثر و روشنی برای تحدید رفتار دولت در این عرصه و جلوگیری از نقض حقوق شهروندان وجود ندارد. در چنین فضایی، نقض حریم خصوصی و سلب برخی حقوق بنیادین، غالباً در پوشش مفاهیمی همچون امنیت ملی، مبارزه با تروریسم، حفظ نظم عمومی و صیانت از ارزش‌های فرهنگی توجیه شده و جرایم حکومتی پلتفرمی به‌عنوان «اقدامی ضروری» جلوه داده می‌شوند. در واقع، در غیاب موازین حقوقی شفاف که حدود و اختیارات دولت را در حوزه پلتفرم‌ها تنظیم کند، عوامل و ملاحظات سیاسی نقش تعیین‌کننده‌ای در این زمینه ایفا می‌کنند. افزون بر این، جرایم حکومتی پلتفرمی واجد آثار نامتقارن بر گروه‌های اجتماعی هستند و تأثیر یکسانی بر همه افراد ندارند؛ به‌گونه‌ای که گروه‌های آسیب‌پذیر بیش از سایرین در معرض این نوع بزه‌دیدگی قرار می‌گیرند.

ابهام در مسئولیت پلتفرم‌ها و دولت در قبال نقض حقوق شهروندان

ابهام در مسئولیت دولت و پلتفرم‌ها در قبال نقض حقوق شهروندان یکی از بنیادی‌ترین چالش‌های حکمرانی دیجیتال در عصر پلتفرم‌هاست. مرز میان «اقدام حکومتی» و «اقدام پلتفرمی» به‌گونه‌ای درهم‌تنیده است که تشخیص فاعل نقض حق، تعیین مسئولیت و اعمال ضمانت‌اجرا با دشواری جدی مواجه می‌شود. دولت‌ها از یک‌سو با اتکا به قدرت حاکمیتی، از پلتفرم‌ها برای نظارت، کنترل محتوا، استخراج داده و مهندسی افکار عمومی استفاده می‌کنند؛ و پلتفرم‌ها از سوی دیگر، با استناد به ماهیت خصوصی خود، از پذیرش مسئولیت در برابر تصمیمات تبعیض‌آمیز یا ناقض حقوق کاربران می‌گریزند. شواهد نشان می‌دهد که دولت‌های اروپایی در حال استفاده از سازوکارهای الگوریتمی پلتفرم‌های دیجیتال برای اعمال محدودیت بر بیان آزاد و نظارت بر کنشگران مدنی هستند، در حالی که پلتفرم‌هایی که پیش‌تر از همکاری در شناسایی کاربران خودداری می‌کردند، اکنون همکاری خود با مراجع قانونی را گسترش داده‌اند؛ این تحول پیامدهای عمیقی برای حق حریم خصوصی و آزادی بیان دارد (Ó Fathaigh et al., 2021). این وضعیت، نوعی «منطقه خاکستری مسئولیت» ایجاد می‌کند که در آن، شهروندان نه به دولت

دسترسی مؤثر دارند و نه می‌توانند پلتفرم را به‌طور مستقل پاسخگو سازند. این ابهام ساختاری پیامدهای عمیقی برای عدالت کیفری و اعتماد عمومی دارد. هنگامی که مشخص نیست چه نهادی مسئول حذف خودسرانه محتوا، مسدودسازی حساب، افشای داده، تبعیض الگوریتمی یا دستکاری اطلاعات است، امکان مطالبه حق، جبران خسارت و اعمال نظارت مستقل عملاً از میان می‌رود. چنین وضعیتی نه تنها به تقویت «مصونیت عملی دولت-پلتفرم» می‌انجامد، بلکه زمینه را برای هنجارگذاری گزینشی و سوءگیری در سیاست جنایی فراهم می‌کند. رفع این ابهام مستلزم طراحی چارچوب‌هایی است که در آن، مرزهای مسئولیت دولت و پلتفرم به‌طور دقیق تعریف شود و سازوکارهای پاسخگویی پلتفرمی و ممیزی مستقل دیجیتال ایجاد گردد. تداوم این ابهام، به شکل‌گیری نوعی خلأ پاسخگویی نهادی منجر می‌شود؛ خلأیی که در آن، هیچ نهاد مشخصی مسئولیت نهایی حفاظت از حقوق شهروندان را بر عهده نمی‌گیرد. این خلأ به‌ویژه در حوزه‌هایی مانند تصمیم‌گیری الگوریتمی، رتبه‌بندی محتوا و مدیریت داده‌های حساس نمود می‌یابد؛ جایی که پلتفرم‌ها با استناد به پیچیدگی فنی و دولت‌ها با اتکا به ضرورت‌های امنیتی، از ارائه توضیح شفاف درباره مبانی تصمیمات خود خودداری می‌کنند. نتیجه آن است که شهروندان در برابر نقض حقوق خود با ساختاری مواجه‌اند که در آن، فاعل نقض حق نامرئی، فرآیند تصمیم‌گیری غیرقابل ردیابی و مسیر اعتراض نامعلوم است. این وضعیت نه تنها تحقق عدالت را تضعیف می‌کند، بلکه امکان جبران خسارت مؤثر و ارزیابی کارآمد سیاست‌های داده‌ای را نیز از میان می‌برد. در غیاب سازوکارهای روشن، شهروندان نمی‌توانند ثابت کنند که آسیب ناشی از اقدام دولت بوده یا پلتفرم؛ و همین امر، چرخه انتقال مسئولیت میان دو بازیگر را تقویت می‌کند. این چرخه، اعتماد عمومی را فرسوده و مشروعیت حکمرانی دیجیتال را به‌طور جدی تهدید می‌کند. افزون بر این، ابهام در مسئولیت‌پذیری می‌تواند به شکل‌گیری الگوی جدیدی از اقتدارگرایی دیجیتال منجر شود؛ الگویی که در آن، دولت و پلتفرم با تقسیم غیررسمی نقش‌ها، مسئولیت‌ها و اختیارات، نوعی «حاکمیت دوگانه غیرپاسخگو» ایجاد می‌کنند. در چنین ساختاری، دولت می‌تواند از پلتفرم‌ها برای اعمال کنترل غیرمستقیم بر جریان اطلاعات استفاده کند، در حالی که پلتفرم‌ها نیز با اتکا به حمایت یا سکوت دولت، از پاسخگویی در برابر تبعیض الگوریتمی، حذف گزینشی محتوا یا افشای داده‌های شخصی می‌گریزند. در نهایت، رفع این ابهام نیازمند طراحی چارچوب‌های دقیق مسئولیت مشترک، تعیین مرزهای روشن میان اقدام حکومتی و اقدام پلتفرمی، و ایجاد سازوکارهای الزام‌آور برای پاسخگویی الگوریتمی و جبران خسارت مؤثر است. تنها در چنین چارچوبی است که می‌توان از تبدیل قدرت دیجیتال به ابزار سلطه جلوگیری کرد و حکمرانی پلتفرمی را بر پایه شفافیت، مسئولیت‌پذیری و برابری حقوقی استوار ساخت.

ضرورت ایجاد سازوکارهای جبران خسارت برای کاربران

ایجاد سازوکارهای جبران خسارت برای کاربران در بستر جرایم حکومتی پلتفرمی یک ضرورت اجتناب ناپذیر است، در غیاب چنین سازوکاری، کاربر در برابر دولت و پلتفرم عملاً بی‌دفاع می‌ماند. هنگامی که اقداماتی مانند حذف خودسرانه محتوا، مسدودسازی حساب، افشای داده‌های شخصی، نظارت پنهان یا دستکاری الگوریتمی رخ می‌دهد، کاربر نه تنها از حق اعتراض مؤثر محروم است، بلکه هیچ مسیر واقعی برای احقاق حق ندارد. این وضعیت، اصل بنیادین حق بر جبران مؤثر را که در حقوق بین‌الملل به‌عنوان یکی از ارکان حقوق بشر شناخته می‌شود، نقض می‌کند. ضعف ساختاری مکانیزم‌های جبران خسارت در حوزه نقض حقوق اطلاعاتی آن قدر عمیق است که نه تنها از اثربخشی قوانین حمایتی می‌کاهد، بلکه عملاً حاکمیت نظارت عمومی توسط مراجع دولتی کم‌منبع را به تنها پاسخ باقی‌مانده تبدیل می‌کند و امکان کنترل مؤثر و مستقل نقض حقوق افراد را از میان می‌برد (Savelyev, 2020, p. 46-49). بنابراین سیاستگذاری جنایی باید سازوکارهایی ایجاد کند که کاربر بتواند بدون ترس، بدون پیچیدگی و بدون مواجهه با قدرت نامتقارن دولت، پلتفرم، خسارت‌های مادی و غیرمادی خود را مطالبه و دریافت کند. از سوی دیگر، وجود سازوکارهای جبران خسارت، نقش بازدارنده و تنظیم‌گرانه‌ای در برابر هم‌پوشانی خطرناک دولت و پلتفرم دارد. اگر پلتفرم‌ها بدانند که همکاری با دولت در اقدامات غیرقانونی مانند تحویل داده بدون حکم قضایی، سانسور سیاسی یا اعمال تبعیض

الگوریتمی می‌تواند منجر به مسئولیت مدنی و کفاری و الزام به جبران خسارت شود، انگیزه بیشتری برای مقاومت در برابر دستورات غیرقانونی خواهند داشت. این سازوکارها همچنین دولت را از «مصونیت عملی» خارج می‌کند. در نتیجه، جبران خسارت نه فقط یک ابزار حمایتی برای کاربران، بلکه یک رکن اساسی در مهار جرایم حکومتی پلتفرمی و تضمین حکمرانی مسئولانه در فضای دیجیتال نیز محسوب می‌شود.

لزوم رعایت حقوق بشر دیجیتال و جلوگیری از ایجاد دیکتاتوری دیجیتالی

در حال حاضر دیجیتالی‌شدن نه صرفاً یک «افزونه تکنیکی»، بلکه یک نیروی تحول‌ساختاری است که شیوه حکمرانی، کنترل و بقای رژیم‌های اقتدارگرا را دگرگون می‌سازد. همان‌گونه که شلومبرگر^۱ و همکاران (۲۰۲۴) توضیح می‌دهند حکومت‌ها در حال حاضر از طریق پلتفرم‌ها به دنبال نظارت و کنترل جمعیت، مدیریت اطلاعات و دستکاری افکار عمومی، بسیج سیاسی و کنترل مشارکت، مدیریت نخبگان و رقابت درون‌حکومتی، سازوکارهای مشروعیت‌سازی دیجیتال، سرکوب دیجیتال و بازآرایی رابطه دولت-جامعه هستند. نکته قابل توجه آنکه در هر یک از این حوزه‌ها، فناوری‌های دیجیتال ابزارهای سنتی اقتدارگرایی کارآمدتر، نامرئی‌تر و کم‌هزینه‌تر است. دیجیتالی‌شدن، مرز میان کنترل نرم و کنترل سخت را از میان می‌برد. به ترتیبی که رژیم‌های اقتدارگرا اکنون می‌توانند با استفاده از داده‌های کلان، هوش مصنوعی و نظارت شبکه‌ای، رفتار شهروندان را پیش‌بینی و مدیریت کنند، بدون آنکه به سرکوب فیزیکی گسترده نیاز داشته باشند. این تحول، نوعی «اقتدارگرایی پیش‌بینی‌گر» را ایجاد می‌کند که در آن، کنترل پیش از وقوع رفتار نامطلوب اعمال می‌شود. در این وضعیت پلتفرم‌ها به‌عنوان واسطه‌های اطلاعاتی، به ابزارهایی برای سانسور، حذف‌گزینی محتوا، دستکاری الگوریتمی و نظارت پنهان تبدیل می‌شوند. در نتیجه نوعی هم‌زیستی قدرت میان دولت و پلتفرم ایجاد می‌شود که در آن، مرز مسئولیت‌ها مبهم و پاسخگویی دشوار می‌شود. به علاوه دیجیتالی‌شدن، منطق مشروعیت‌سازی رژیم‌های اقتدارگرا را نیز تغییر می‌دهد. دولت‌ها با استفاده از فناوری، کارآمدی اداری، خدمات دیجیتال و روایت‌های رسانه‌ای کنترل شده را به‌عنوان نشانه‌های «پیشرفت» و «ثبات» عرضه می‌کنند و از این طریق، مشروعیت خود را باز تولید می‌کنند. این امر نشان می‌دهد که دیکتاتوری دیجیتال صرفاً سرکوب نیست؛ بلکه ترکیبی از کنترل، رضایت‌سازی و مهندسی ادراک است. النهایه اینکه دیجیتالی‌شدن، اقتدارگرایی را نه فقط تقویت، بلکه بازآفرینی می‌کند. رژیم‌های اقتدارگرا با بهره‌گیری از فناوری، به شکل‌هایی از حکمرانی روی می‌آورند که از دیکتاتوری‌های کلاسیک متمایز است.^۲ بنابراین رعایت حقوق بشر دیجیتال در سیاست‌گذاری جنایی مرتبط با جرایم حکومتی پلتفرمی ضرورتی بنیادین است، زیرا در حال حاضر فضای دیجیتال به زیربنای اصلی اعمال یا محدودیت حقوق و آزادی‌های اساسی شهروندان تبدیل شده است. در این فضا، رعایت حریم خصوصی، آزادی بیان، حق دسترسی به اطلاعات، حق مشارکت سیاسی و حق امنیت ارتباطات نسبت به جهان فیزیکی آسیب‌پذیری بیشتری دارند. این آسیب‌پذیری می‌تواند انگیزه لازم را برای دولت‌ها در جهت نقض کم‌هزینه حقوق شهروندی فراهم آورد. دولت‌ها با اتکا به ظرفیت‌های فناورانه و دسترسی گسترده به داده‌های کاربران می‌توانند از طریق پلتفرم‌ها به نظارت فراگیر، سانسور الگوریتمی، دستکاری اطلاعات و کنترل رفتار جمعی بپردازند؛ اموری که ماهیتاً تهدیدی مستقیم علیه کرامت انسانی و آزادی‌های بنیادین محسوب می‌شوند. از این رو، سیاست‌گذاری جنایی باید به‌گونه‌ای طراحی شود که هرگونه مداخله حکومتی در فضای پلتفرمی را مقید به

1. Schlumberger

۲. برای مطالعه بیشتر رک به:

Roberts, T., & Oosterom, M. (2025). Digital authoritarianism: A systematic literature review. *Information Technology for Development*, 31(4), 860–884. <https://doi.org/10.1080/02681102.2024.2425352>
 Schlumberger, O., Edel, M., Maati, A., & Saglam, K. (2024). How authoritarianism transforms: A framework for the study of digital dictatorship. *Government and Opposition*, 59(3), 761–783. <https://doi.org/10.1017/gov.2023.20>
 Michaelsen, M., & Ruijgrok, K. (2024). Digital authoritarianism. In *The Oxford Handbook of Authoritarian Politics*. Oxford University Press. <https://doi.org/10.1093/oxfordhb/9780198871996.013.59>
 Pearson, J. S. (2024). Defining digital authoritarianism. *Philosophy & Technology*, 37, Article 73. <https://doi.org/10.1007/s13347-024-00700-9> (doi.org in Bing)

اصول حقوق بشر دیجیتال سازد و نقض این اصول را در قالب ضمانت‌اجراهای کیفری و نظارتی قابل پیگرد کند. از سوی دیگر، رعایت حقوق بشر دیجیتال شرط لازم برای اعتماد عمومی و مشروعیت حکمرانی دیجیتال است. هنگامی که کاربران احساس کنند داده‌هایشان بدون رضایت جمع‌آوری می‌شود، محتواهایشان به‌طور نامرئی دستکاری می‌شود یا ارتباطاتشان تحت نظارت قرار دارد، مشارکت اجتماعی و سیاسی آنان کاهش می‌یابد و فضای عمومی دیجیتال به محیطی نا امن و غیرشفاف تبدیل می‌شود. بنابراین سیاست‌گذاری جنایی باید تضمین کند که پلتفرم‌ها در برابر دولت مسئولیت‌پذیر باشند، درخواست‌های حکومتی برای حذف محتوا یا دسترسی به داده‌ها شفاف، مستند و قابل اعتراض باشد، و کاربران از سازوکارهای مؤثر برای جبران خسارت برخوردار شوند. بدین ترتیب، حقوق بشر دیجیتال نه یک اصل اخلاقی، بلکه یک ضرورت ساختاری برای حفظ آزادی‌های مدنی و جلوگیری از تبدیل قدرت دیجیتال دولت به قدرتی غیرپاسخ‌گو است.

اجتناب از سوءگیری در سیاست جنایی و هنجارگذاری تبعیض آمیز

اجتناب از سوءگیری در سیاست جنایی یکی از بنیادی‌ترین الزامات حکمرانی عادلانه در عصر پلتفرم‌هاست. در شرایطی که دولت و پلتفرم‌ها به‌طور هم‌زمان در تولید، اعمال و تفسیر قواعد کیفری نقش دارند، کوچک‌ترین انحراف از بی‌طرفی می‌تواند به بازتولید نابرابری‌های ساختاری و تقویت سازوکارهای حذف سیاسی یا اجتماعی منجر شود. سیاست جنایی زمانی دچار سوءگیری می‌شود که جرم‌انگاری، تنظیم‌گری محتوا یا اعمال ضمانت‌اجراها بر اساس سوگیری‌های سیاسی، ایدئولوژیک یا فرهنگی صورت گیرد و نه بر مبنای معیارهای عینی و حقوقی. این وضعیت، سیاست جنایی را از کارکرد حمایتی خود دور کرده و آن را به ابزاری برای مهندسی رفتار و کنترل‌گزینشی تبدیل می‌کند. در این میان، هنجارگذاری تبعیض‌آمیز یکی از پیامدهای مستقیم سوءگیری در سیاست جنایی است. هنگامی که قواعد ناظر بر حذف محتوا، مسدودسازی حساب‌ها، رتبه‌بندی الگوریتمی یا جمع‌آوری داده‌ها به‌گونه‌ای طراحی شوند که برخی گروه‌ها را بیش از دیگران در معرض آسیب قرار دهند، نوعی خشونت دیجیتال ساختاری شکل می‌گیرد. این تبعیض می‌تواند مانند هدف‌گیری مستقیم گروه‌های سیاسی یا اقلیت‌ها آشکار باشد یا پنهان، مانند تبعیض الگوریتمی که در لایه‌های فنی و غیرقابل مشاهده رخ می‌دهد. در هر دو حالت، نتیجه تضعیف عدالت و کاهش اعتماد عمومی به نظام حکمرانی است. از سوی دیگر، سوءگیری در سیاست جنایی اغلب در پوشش «ضرورت‌های امنیتی» یا «مصلحت‌های عمومی» توجیه می‌شود؛ در حالی که این توجیهات می‌توانند به ابزاری برای هنجارگذاری گزینشی تبدیل شوند. هنگامی که دولت یا پلتفرم، قواعد کیفری را به‌صورت گزینشی علیه مخالفان، منتقدان یا گروه‌های آسیب‌پذیر به کار می‌گیرد، سیاست جنایی از مسیر عدالت خارج شده و به سازوکاری برای کنترل اجتماعی نامتقارن بدل می‌شود. این وضعیت، ضرورت وجود سازوکارهای ممیزی مستقل دیجیتال را برجسته می‌کند تا تصمیمات دولت پلتفرم از منظر بی‌طرفی و تناسب مورد ارزیابی قرار گیرد. افزون بر این، هنجارگذاری تبعیض‌آمیز در فضای پلتفرمی می‌تواند پیامدهای گسترده‌ای برای حقوق بنیادین دیجیتال داشته باشد. تبعیض در حذف محتوا یا محدودسازی دسترسی، آزادی بیان را تهدید می‌کند؛ تبعیض در جمع‌آوری داده، حق بر حریم خصوصی را نقض می‌کند؛ و تبعیض در رتبه‌بندی محتوا، حق بر دسترسی برابر به اطلاعات را مخدوش می‌سازد. برای جلوگیری از این وضعیت، سیاست جنایی باید بر اصول شفافیت، تناسب، بی‌طرفی و پاسخگویی استوار باشد و سازوکارهای الزام‌آور برای پاسخگویی الگوریتمی ایجاد کند. در کنار این، پرهیز از سوءگیری و تبعیض مستلزم ایجاد تعادل قدرت میان دولت و کاربر است. در بسیاری از موارد، کاربران در برابر دولت-پلتفرم در موقعیتی کاملاً نامتقارن قرار دارند و امکان اعتراض مؤثر یا مطالبه حق برای آنان محدود است. تودین سیاست جنایی در قلمرو جرایم حکومتی پلتفرمی می‌تواند این عدم تقارن را کاهش دهد و از تبدیل سیاست جنایی به ابزار سلطه جلوگیری کند. در نهایت، تحقق سیاست جنایی عادلانه در فضای پلتفرمی نیازمند طراحی چارچوب‌هایی است که در آن، سوگیری ساختاری و هنجارگذاری تبعیض‌آمیز به‌طور فعال شناسایی، کنترل و اصلاح شود. این امر تنها با ترکیب سه عنصر ممکن است: شفافیت در فرآیندهای تصمیم‌گیری، نظارت مستقل بر عملکرد دولت پلتفرم، و تضمین برابری دسترسی به حقوق دیجیتال برای همه کاربران.

تنها در چنین چارچوبی است که می‌توان اطمینان یافت سیاست جنایی در عصر پلتفرم‌ها نه ابزار تبعیض، بلکه سازوکاری برای حمایت برابر از همه شهروندان خواهد بود.

نتیجه‌گیری

سیاست جنایی فعلی ایران در قبال جرایم سایبری عمدتاً کاربران یا شرکت‌ها را هدف قرار می‌دهد و نسبت به رفتارهای مجرمانه دولت در عرصه فضای مجازی بی‌توجه است. در حوزه پلتفرم‌ها نیز اعمال زیان‌بار حکومتی در این عرصه فاقد عنوان مجرمانه‌اند، ضمانت اجرای کیفری برای دولت یا مأموران آن پیش‌بینی نشده و مسئولیت‌پذیری حکومتی در فضای دیجیتال در هاله‌ای از ابهام قرار دارد. این در حالی است که با گسترش پلتفرم‌ها و استفاده گسترده شهروندان از آن‌ها، در کنار آثار مثبت، مسئله سوءاستفاده حکومت‌ها از این فضا نیز به‌طور جدی مطرح شده است. امروزه شاهد تهدیدات نوظهور حکومتی در عرصه فضای مجازی، به‌ویژه در بستر پلتفرم‌ها، هستیم که ضرورت پاسخ‌شناسی و مواجهه نظام‌مند با این تهدیدات را به ضرورتی اجتناب‌ناپذیر تبدیل کرده است.

در شرایط کنونی، دولت‌ها از طریق پلتفرم‌ها به ابزارهایی همچون دستکاری الگوریتمی برای جهت‌دهی به افکار عمومی، سانسور هوشمند و نامرئی، انتشار سازمان‌یافته اطلاعات گمراه‌کننده و بهره‌گیری از هوش مصنوعی برای نظارت و پیش‌بینی رفتار کاربران متوسل می‌شوند؛ اقداماتی که در دهه‌های گذشته سابقه نداشته است. این اقدامات، هنگامی که در سطحی گسترده و توسط سازمان حکومتی انجام شود و منجر به نقض حقوق شهروندان گردد، در قالب جرایم حکومتی پلتفرمی قابل تحلیل و بررسی است. در واقع، قدرت دیجیتالی که حکومت‌ها در حال حاضر به آن دست یافته‌اند، چنانچه از طریق سیاست‌گذاری مناسب مهار نشود، می‌تواند به یکی از بزرگترین تهدیدها برای آزادی‌های مدنی تبدیل گردد. از این‌رو، نیازمند سازوکارهایی هستیم که در این عرصه، قدرت دولت را محدود، شفافیت را تقویت، مسئولیت‌پذیری را تضمین و حقوق کاربران را در کانون توجه قرار دهد. سیاست‌گذاری جنایی در خصوص جرایم حکومتی پلتفرمی از آن جهت واجد اهمیت است که پلتفرم‌ها بتوانند در برابر درخواست‌های غیرقانونی دولت‌ها مقاومت کنند و شهروندان نیز از سازوکارهای مؤثر برای پیگیری نقض حقوق خود برخوردار شوند. سیاست جنایی در این حوزه باید از کاربران در برابر نظارت‌های غیرقانونی و نقض حریم خصوصی حمایت کرده و با تعریف تعهدات ضد سوءاستفاده برای پلتفرم‌ها، در راستای استانداردهای بین‌المللی حقوق بشر و چارچوب‌های امنیت سایبری تدوین شود. همچنین، ضرورت سیاست‌گذاری در این حوزه از آن جهت است که پاسخگویی و شفافیت تضمین شده و حقوق بنیادین شهروندان در استفاده از پلتفرم‌ها حفظ گردد. این ضرورت در نظام عدالت کیفری ایران نیز ریشه در سیاست‌های کلان دارد؛ به‌گونه‌ای که بر اساس بند نهم سیاست‌های کلی نظام قانون‌گذاری (ابلاغی ۱۳۹۹/۰۷/۰۶)، عدالت‌محوری در قوانین، اجتناب از تبعیض‌های ناروا و حتی‌الامکان پرهیز از استثنای قانونی مورد تأکید قرار گرفته است. همچنین پالایش قوانین بر اساس قانون اساسی به عنوان یکی از سیاست‌های کلی نظام قانون‌گذاری مطرح شده است (Shiri & Jafarpour Sadegh, 2022: 4). بنابراین، نادیده‌انگاری سیاست‌گذاری جنایی در عرصه جرایم حکومتی پلتفرمی، از آن جهت که منجر به سلب حقوق شهروندان می‌شود و با اصول قانون اساسی، به‌ویژه اصول ۲۰، ۲۲، ۲۳ و ۲۵، در تعارض است. بر این اساس، طرح‌هایی نظیر «صیانت از حقوق کاربران در فضای مجازی و سامان‌دهی پیام‌رسان‌های اجتماعی» که بدون توجه به الزامات مذکور و به‌صورت تبعیض‌آمیز به محدودسازی حقوق شهروندان پرداخته و نسبت به رفتارهای آسیب‌رسان دولت در این حوزه سکوت کرده‌اند، با موازین یادشده همخوانی ندارند. یکی از دلایل این نوع سیاست‌گذاری آن است که از منظر برخی سیاست‌گذاران، جرم‌انگاری رفتارهای حکومتی ممکن است به محدودسازی قدرت حاکمیت و ایجاد چالش‌هایی برای نظام سیاسی بینجامد؛ از این‌رو، تمایلی به مفهوم‌سازی بزهکاری دولت و تدوین سیاست جنایی در این حوزه وجود ندارد. این در حالی است که هنجارگذاری جنایی در عرصه جرایم حکومتی نه‌تنها به معنای تقابل با نظام سیاسی نیست، بلکه منطبق با اصول قانون اساسی و موازین اسلامی، از جمله لزوم رعایت حریم خصوصی و

حقوق شهروندی، بوده و در چارچوب اصل چهارم قانون اساسی قابل توجیه است. افزون بر این، تدوین سیاست جنایی در قلمرو جرایم حکومتی پلتفرمی می‌تواند موجب افزایش اعتماد عمومی، تقویت سرمایه اجتماعی و ارتقای مشروعیت نظام سیاسی گردد. تحقق این امر مستلزم تحول در نظام سیاستگذاری جنایی، بهره‌گیری از متخصصان این حوزه، گرایش به سیاست جنایی مشارکتی و استفاده از ظرفیت سازمان‌های مردم‌نهاد در فرآیند قانون‌گذاری است. در واقع، سیاستگذاری جنایی در این عرصه نیازمند حضور تمامی کنشگران مرتبط و نهادهایی است که بتوانند تعارض منافع را مدیریت کنند؛ چراکه در غیر این صورت، تعارض میان منافع دولت و وظیفه سیاستگذاری، مانع از تدوین یک سیاست جنایی بی‌طرفانه خواهد شد. چنین وضعیتی می‌تواند به انحراف در سیاستگذاری جنایی، گسترش فساد، سوءاستفاده از قدرت و نقض حقوق شهروندان بینجامد. در نتیجه، سیاستگذاری جنایی به‌صورت نامتوازن شکل گرفته و در حالی که قوانین محدودکننده حقوق و آزادی‌های عمومی به تصویب می‌رسند، جرایم حکومتی، به‌ویژه در عرصه فضای مجازی، نادیده گرفته می‌شوند. برای غلبه بر این وضعیت، علاوه بر بهره‌گیری از ابزارهای مذکور، ضروری است سیاستگذاری جنایی در فضای مجازی مبتنی بر اصول قانون اساسی صورت گیرد چرا که رویکرد متوازن قانون اساسی نسبت به حقوق دولت و شهروندان این امکان را فراهم می‌آورد که در کنار جرایم شهروندان علیه حکومت، به جرایم حکومت علیه شهروندان نیز به‌طور جدی پرداخته شود.

تعارض منافع

متن حاضر فاقد هرگونه تعارض منافع است.

References

1. Aghababaei Taghanaki, A. , Mousavi Mojab, S. D. , Habibzadeh, M. J. and Mohammadi, P. (2025). Criminal policy-making against the criminal activity of information technology commercial platforms: Necessities and Obligations. *Criminal Law Research*, 16(2), 7-21. <https://doi.org/10.22124/jol.2025.28367.2507> (In Persian)
2. Aghababaei Taghanaki, A. , Mousavi Mojab, S. D. , Habibzadeh, M. J. and Mohammadi, P. (2025). Iran's preventive legislative criminal policy regarding the activities of information technology commercial platforms. *Journal of Legal Studies*, (), -. <https://doi.org/10.22099/jls.2025.53924.5367> (In Persian)
3. Alexander, S. (2020). THE INADEQUACY OF CURRENT REMEDIES FOR VIOLATION OF DATA SUBJECTS' RIGHTS AND HOW TO FIX IT. *Legal Issues in the digital Age*, (2), 24-62.
4. Anderson Jr, E. G., Parker, G. G., & Tan, B. (2014). Platform performance investment in the presence of network externalities. *Information systems research*, 25(1), 152-172
5. Ardebili, M. A. (2015). *General Criminal Law* (Vol. 3). Tehran: Mizan Publishing. (In Persian).
6. Bergvall-Kåreborn, B., & Howcroft, D. (2014). Persistent problems and practices in information systems development: a study of mobile applications development and distribution. *Information Systems Journal*, 24(5), 425-444
7. Bloch-Wehba, H. (2019). Global platform governance: private power in the shadow of the state. *SMU L. Rev.*, 72, 27-80
8. Bracken, M. (2015). Government as a Platform: the next phase of digital transformation. *Government Digital Service*, 29
9. Ceccagnoli, M., Forman, C., Huang, P., & Wu, D. (2012). Cocreation of value in a platform ecosystem! The case of enterprise software. *MIS quarterly*, 263-290
10. Chappell, D. (2011). What Is an Application Platform? Available online (retrieved 5 January, 2013): http://www.davidchappell.com/writing/white_papers/What_is_an_Application_Platform-Chappell.pdf
11. Davies, A., Donald, B., & Gray, M. (2023). The power of platforms—precarity and place. In (Vol. 16, pp. 245-256): Oxford University Press UK
12. Dhar, V., & Sundararajan, A. (2007). Issues and Opinions—Information technologies in business: A blueprint for education and research. *Information systems research*, 18(2), 125-141
13. Dictionary, O. (2008). *Oxford Learner's Pocket Dictionary*. In: New York: Oxford University Press.
14. Drew, J. M. (2020). A study of cybercrime victimisation and prevention: exploring the use of online crime prevention behaviours and strategies. *Journal of Criminological Research, Policy and Practice*, 6(1), 17-33
15. Fathaigh, R. Ó., Möller, J., & Bellanova, R. (2021). Digital Platforms and the Digitisation of Government Surveillance. *AoIR Selected Papers of Internet Research*. <https://doi.org/10.5210/spir.v2021i0.12220>
16. Fichman, R. G. (2004). Real options and IT platform adoption: Implications for theory and practice. *Information systems research*, 15(2), 132-154
17. Gillespie, T. (2017). Governance of and by platforms. *SAGE handbook of social media*, 254-278 .
18. Gorwa, R. (2019). What is platform governance? *Information, Communication & Society*, 22(6), 854-871 .
19. Hagiu, A. (2014). Strategic decisions for multisided platforms. *MIT Sloan management review*, 55(2), 71
20. Hamilton, R. J. (2022). Platform-Enabled Crimes: Pluralizing Accountability When Social Media Companies Enable Perpetrators to Commit Atrocities. *BCL Rev.*, 63, 1349
21. Hashmi, M. A. I., Junaid, U., & Qadir, G. M. M. (2025). Cybercrime and Digital Offenses: Challenges of Applying Traditional Criminal Law. *Journal of Social and Organizational Matters*, 4(4), 255-269. <https://doi.org/10.56976/jsom.v4i4.343>

22. Hessam, A., Modibo Joni, M., Miri, H., & Yamerli, S. (2021). Liability of Online Platforms for Violating Information Privacy by Users; A Comparative Study Among Iran, the United States and the European Union. *Communication Research*, 28(107), 69-91. <https://doi.org/10.22082/cr.2021.530918.2202> (In Persian)
23. Jain, H., Rothenberger, M., & Sugumaran, V. (2006). Flexible software component design using a product platform approach
24. Javadi Hosseinabadi, H. (2021). Toward an integrated theory of state crime (Doctoral dissertation, Faculty of Law and Political Science, Allameh Tabataba'i University, Tehran, Iran). (In Persian).
25. Kosta, E. (2022). Algorithmic state surveillance: Challenging the notion of agency in human rights. *Regulation & Governance*, 16(1), 212-224. <https://doi.org/10.1111/rego.12331>
26. Kraemer, T., Hinz, O., & Skiera, B. (2010). Return on IT investments in two-sided markets
27. Lahiri, A., Dewan, R. M., & Freimer, M. (2010). The disruptive effect of open platforms on markets for wireless services. *Journal of Management Information Systems*, 27(3), 81-110
28. Meyer, M. H., & Seliger, R. (1998). Product platforms in software development. *MIT Sloan management review*
29. Michaelsen, M., & Ruijgrok, K. (2024). Digital authoritarianism. In *The Oxford Handbook of Authoritarian Politics*. Oxford University Press. <https://doi.org/10.1093/oxfordhb/9780198871996.013.59>
30. Moro Visconti, R. (2020). Corporate governance, digital platforms, and network theory: Information and risk-return sharing of connected stakeholders. *Management Control*: 2, 2020, 179-204
31. Moro Visconti, R. (2020). Corporate governance, digital platforms, and network theory: Information and risk-return sharing of connected stakeholders. *Management Control*: 2, 2020, 179-204.
32. O'Reilly, T. (2011). Government as a Platform. *Innovations: technology, governance, globalization*, 6(1), 13-40
33. Pearson, J. S. (2024). Defining digital authoritarianism. *Philosophy & Technology*, 37, Article 73. <https://doi.org/10.1007/s13347-024-00700-9> (doi.org in Bing)
34. Perakslis, E., & Quintana, Y. (2023). Social Media is Addictive and Influences Behavior: Should it Be Regulated as a Digital Therapeutic? [Viewpoint]. *J Med Internet Res*, 25, e43174. <https://doi.org/10.2196/43174>
35. Perakslis, E., & Quintana, Y. (2023). Social Media is Addictive and Influences Behavior: Should it Be Regulated as a Digital Therapeutic? [Viewpoint]. *J Med Internet Res*, 25, e43174. <https://doi.org/10.2196/43174>
36. Rai, A., Patnayakuni, R., & Seth, N. (2006). Firm performance impacts of digitally enabled supply chain integration capabilities. *MIS quarterly*, 225-246
37. Razmetaeva, Y., Ponomarova, H., & Bylya-Sabadash, I. (2021). Jurisdictional issues in the digital age. *Ius Humani, Revista de Derecho*, 10, 167-183
38. Riemer, K., & Richter, A. (2010). Social software: agents for change or platforms for social reproduction? A case study on enterprise microblogging
39. Roberts, T., & Oosterom, M. (2025). Digital authoritarianism: A systematic literature review. *Information Technology for Development*, 31(4), 860-884. <https://doi.org/10.1080/02681102.2024.2425352>
40. Sander, B. (2021). Democratic disruption in the age of social media: Between marketized and structural conceptions of human rights law. *European Journal of International Law*, 32(1), 159-193. <https://doi.org/10.1093/ejil/chab022>
41. Schlumberger, O., Edel, M., Maati, A., & Saglam, K. (2024). How authoritarianism transforms: A framework for the study of digital dictatorship. *Government and Opposition*, 59(3), 761-783. <https://doi.org/10.1017/gov.2023.20>
42. Shiri, A. (2021). Investigating the development of criminal control of state crime in Iran.. *Iranian Journal of Public Policy*, 6(4), 193-209. <https://doi.org/10.22059/jppolicy.2021.80487> (In Persian)
43. Shiri, A. and Jafarpour Sadeh, E. (2022). Governing Requirements on the Criminalization of State Crimes in Iran's Criminal Policy Process. *Iranian Journal of Public Policy*, 7(4), 145-165. <https://doi.org/10.22059/jppolicy.2021.84827> (In Persian)
44. Sun, R., Gregor, S., & Keating, B. (2015). Information technology platforms: Conceptualisation and a review of emerging research in IS research. *Australasian Conference on Information Systems (ACIS) 2015 Proceedings*
45. Sun, R., Gregor, S., & Keating, B. (2015). Information technology platforms: Conceptualisation and a review of emerging research in IS research. *Australasian Conference on Information Systems (ACIS) 2015 Proceedings*,
46. Susser, D., Roessler, B., & Nissenbaum, H. (2019). Online manipulation: Hidden influences in a digital world. *Geo. L. Tech. Rev.*, 4, 1.
47. Taudes, A., Feurstein, M., & Mild, A. (2000). Options analysis of software platform decisions: A case study. *MIS quarterly*, 227-243
48. Tiwana, A., Konsynski, B., & Bush, A. A. (2010). Research commentary—Platform evolution: Coevolution of platform architecture, governance, and environmental dynamics. *Information systems research*, 21(4), 675-687
49. Ulbricht, L., & Egbert, S. (2024). In Palantir we trust? Regulation of data analysis platforms in public security. *Big Data & Society*, 11(3), 20539517241255108. <https://doi.org/10.1177/20539517241255108>
50. Van Dijck, J. (2021). Seeing the forest for the trees: Visualizing platformization and its governance. *New Media & Society*, 23(9), 2801-2819. <https://doi.org/10.1177/1461444820940293>
51. Volkov, V., & Sidorenko, E. (2022). Digital Platforms and Issues of Corporate Criminal Responsibility, Self-regulation. *Proceedings of the International Scientific Conference "Smart Nations: Global Trends In The Digital Economy" Volume 1*
52. Volkov, V., & Sidorenko, E. (2022). Digital Platforms and Issues of Corporate Criminal Responsibility, Self-regulation. *Proceedings of the International Scientific Conference "Smart Nations: Global Trends In The Digital Economy" Volume 1*
53. West, J. K. (2019). An introduction to online platforms and their role in the digital transformation. Available at SSRN 4669281
54. Yakhchali, M., Tahmasebi, R., Latifi, M. and Faraji Mollaie, A. (2020). Investigating Government as a Platform Characteristics: A Systematic Literature Review and Meta-Synthesis. *Journal of Public Administration*, 12(2), 204-237. <https://doi.org/10.22059/jipa.2020.303652.2755> (In Persian)
55. Yang, C., Mousavi, S., Dash, A., Gummadi, K. P., & Weber, I. (2025). Studying Behavioral Addiction by Combining Surveys and Digital Traces: A Case Study of TikTok. *Proceedings of the International AAAI Conference on Web and Social Media*