Comparative Studies in Jurisprudence, Law, and Politics

Criminal Policy Toward Crimes Against Cyber Privacy: A Comparative Evaluation of the Effectiveness of Iranian and Afghan Regulations

1. Mohammad Aref Rezaei: PhD Student, Department of Criminal Law and Criminology, CT.C., Islamic Azad University Tehran, Iran
2. Abbas Tadayyon*: Department of Criminal Law and Criminology, CT.C., Islamic Azad University Tehran, Iran. Email: 2229669370@iau.ir (Corresponding Author)
3. Mahdi Esmaeili: Department of Criminal Law and Criminology, CT.C., Islamic Azad University Tehran, Iran

ABSTRACT

The present study was conducted with the aim of comparatively evaluating the effectiveness of the criminal policies of Iran and Afghanistan in addressing crimes against privacy in cyberspace. Criminal policy, as a set of state strategies for the prevention, criminalization, and response to criminal phenomena, is assessed in this study from legislative, judicial, and executive perspectives. The research employs a descriptive-analytical method with a comparative approach. The findings indicate that the criminal policies of both countries in this area lack sufficient effectiveness due to legislative inconsistency, limited enforcement capacity, and the predominance of a punitive approach over a preventive one. Although Iran possesses a relatively more developed legislative framework, it faces significant implementation challenges. Afghanistan, by contrast, remains at the stage of developing the foundational infrastructure of cyber criminal policy. The study suggests that both countries should move toward an "integrated criminal policy" that combines legislative, executive, preventive, and supportive measures, while also drawing upon Islamic jurisprudential foundations as a source of legitimacy and normative support.

Keywords: *Criminal policy, cyber privacy, cybercrime, legal effectiveness, comparative law, Iran, Afghanistan.*

How to cite: Rezaei, M. A., Tadayyon, A., & Esmaeili, M. (2027). Criminal Policy Toward Crimes Against Cyber Privacy: A Comparative Evaluation of the Effectiveness of Iranian and Afghan Regulations. *Comparative Studies in Jurisprudence, Law, and Politics*, *9*(1), 1-19.

Submit Date: 20 February 2026
Revise Date: 22 June 2026
Accept Date: 30 June 2026
Initial Publish Date: 03 August 2026
Final Publish Date: 21 April 2027

پژوهش‌های تطبیقی فقه، حقوق و سیاست

سیاست جنایی در قبال جرایم علیه حریم خصوصی سایبری: ارزیابی تطبیقی کارآمدی مقررات ایران و افغانستان

۱. محمد عارف رضایی: دانشجوی دکتری، گروه حقوق جزا و جرم شناسی، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران
۲. عباس تدین*: گروه حقوق کیفری و جرم شناسی، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران. پست الکترونیک: 2229669370@iau.ir (نویسنده مسئول)
۳. مهدی اسماعیلی: گروه حقوق کیفری و جرم شناسی، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران

چکیده

پژوهش حاضر با هدف ارزیابی تطبیقی کارآمدی سیاست جنایی ایران و افغانستان در مقابله با جرایم علیه حریم خصوصی در فضای سایبری انجام شده است. سیاست جنایی به‌عنوان مجموعه راهبردهای دولت در پیشگیری، جرم‌انگاری، و واکنش به پدیده مجرمانه، در این پژوهش از ابعاد تقنینی، قضایی، و اجرایی مورد ارزیابی قرار گرفته است. روش پژوهش توصیفی-تحلیلی با رویکرد مطالعه تطبیقی است. یافته‌ها نشان می‌دهند که سیاست جنایی هر دو کشور در این حوزه، به دلیل فقدان انسجام تقنینی، ضعف ظرفیت اجرایی، و غلبه رویکرد سرکوب‌گرانه بر رویکرد پیشگیرانه، از کارآمدی کافی برخوردار نیست. ایران با داشتن چارچوب تقنینی نسبتاً توسعه‌یافته‌تر، اما با چالش‌های اجرایی جدی مواجه است. افغانستان در مرحله توسعه زیرساخت‌های اولیه سیاست جنایی سایبری قرار دارد. این پژوهش پیشنهاد می‌کند که هر دو کشور به سمت «سیاست جنایی یکپارچه» که ترکیبی از اقدامات تقنینی، اجرایی، پیشگیرانه، و حمایتی است حرکت کنند و از پشتوانه فقهی-اسلامی به‌عنوان اهرم مشروعیت‌ساز بهره گیرند.

واژگان کلیدی: *سیاست جنایی، حریم خصوصی سایبری، جرایم رایانه‌ای، کارآمدی قانون، حقوق تطبیقی، ایران، افغانستان*

نحوه استناددهی: رضایی، محمد عارف.، تدین، عباس.، و اسماعیلی، مهدی. (۱۴۰۶). سیاست جنایی در قبال جرایم علیه حریم خصوصی سایبری: ارزیابی تطبیقی کارآمدی مقررات ایران و افغانستان. *پژوهش‌های تطبیقی فقه، حقوق و سیاست*، ۹(۱)، ۱۹-۱.

تاریخ ارسال: ۱ اسفند ۱۴۰۴
تاریخ بازنگری: ۱ تیر ۱۴۰۵
تاریخ پذیرش: ۹ تیر ۱۴۰۵
تاریخ چاپ اولیه: ۱۲ مرداد ۱۴۰۵
تاریخ چاپ نهایی: ۱ اردیبهشت ۱۴۰۶

مقدمه

«سیاست جنایی» (*Criminal Policy*) مفهومی است که دلاماس-مارتی آن را به‌عنوان «مجموعه روش‌هایی که جامعه از طریق آن‌ها علیه پدیده مجرمانه واکنش نشان می‌دهد» تعریف کرده است (Delmas-Marty, 1986). این مفهوم، که از حقوق کیفری فراتر می‌رود، سیاست‌های پیشگیری، حمایت از بزه‌دیدگان، و اصلاح مجرمان را نیز در بر می‌گیرد. در عصر دیجیتال، دولت‌ها با طیف جدیدی از جرایم مواجه‌اند که بازنگری در سیاست جنایی موجود را ناگزیر می‌سازند. جرایم علیه حریم خصوصی سایبری، از جمله نشر غیرمجاز تصاویر خصوصی، باج‌گیری جنسی دیجیتال، هویت‌دزدی، و جاسوسی دیجیتال، از پیچیده‌ترین چالش‌های سیاست جنایی معاصر هستند که به دلیل ویژگی‌های منحصربه‌فرد فضای مجازی، بی‌مرزی، ناشناختگی، سرعت انتشار، با پاسخ‌های سنتی کیفری قابل مقابله مؤثر نیستند (Alizadeh, 2018).

ایران و افغانستان، دو کشور اسلامی با پیوندهای فرهنگی و زبانی عمیق، در مسیر تدوین و اجرای سیاست جنایی سایبری خود قرار دارند. هر دو کشور با یک چالش مشترک روبه‌رو هستند: چگونه می‌توان سیاست جنایی‌ای طراحی کرد که هم از ارزش‌های اسلامی الهام گیرد، هم با استانداردهای بین‌المللی همخوانی داشته باشد، و هم با واقعیت‌های اجتماعی-فرهنگی هر کشور سازگار باشد؟ این سؤال، که در قلب این پژوهش قرار دارد، هنوز در ادبیات علمی موجود به‌طور کافی پاسخ داده نشده است. ارزیابی کارآمدی سیاست جنایی دو کشور در حوزه‌ای که هم از نظر فناوری و هم از نظر اجتماعی در حال تحول سریع است، نیازمند چارچوب‌های تحلیلی دقیق و مبتنی بر شواهد است که این پژوهش آن را فراهم می‌کند (Salehi, 2022).

مرور ادبیات نشان می‌دهد که پژوهش‌های موجود درباره سیاست جنایی سایبری در ایران و افغانستان از دو ضعف اصلی رنج می‌برند: اول، تمرکز بر جنبه‌های تقنینی به‌بهای نادیده‌گرفتن ابعاد قضایی، اجرایی، و پیشگیرانه؛ دوم، فقدان رویکرد تطبیقی که تجربه دو کشور را در کنار هم بررسی کند. این پژوهش با ارائه یک چارچوب سه‌بُعدی، تقنینی-قضایی-اجرایی، برای ارزیابی سیاست جنایی، و با تطبیق این چارچوب با هر دو نظام حقوقی، گامی در جهت پر کردن این خلأ برمی‌دارد. سؤال اصلی پژوهش این است: سیاست جنایی ایران و افغانستان در مقابله با جرایم علیه حریم خصوصی سایبری چه میزان از کارآمدی برخوردار است و از چه فرصت‌هایی برای اصلاح می‌توان بهره‌مند شد؟

این مقاله در هفت بخش اصلی سازمان یافته است. پس از مقدمه، بخش دوم چارچوب نظری سیاست جنایی یکپارچه را تشریح می‌کند. بخش سوم روش‌شناسی پژوهش را توضیح می‌دهد. بخش‌های چهارم و پنجم به ارزیابی سیاست جنایی ایران و افغانستان اختصاص دارند. بخش ششم تحلیل تطبیقی و بحث درباره یافته‌ها را ارائه می‌دهد، و بخش هفتم با نتیجه‌گیری و پیشنهادات سیاستی پایان می‌یابد. همه بخش‌ها با استناد به منابع علمی معتبر داخلی و بین‌المللی نوشته شده‌اند.

چارچوب نظری: سیاست جنایی یکپارچه

مفهوم سیاست جنایی

مفهوم سیاست جنایی سیر تطور قابل توجهی داشته است. از رویکرد کلاسیک فویرباخ (*Feuerbach, 1804*)، که سیاست جنایی را صرفاً «حکمت قانون‌گذار جزایی» می‌دانست، تا رویکرد جامع‌تر دلاماس-مارتی که آن را به سه بُعد اصلی تقسیم می‌کند: «سیاست جنایی تقنینی» (*Legislative Criminal Policy*) که به چگونگی جرم‌انگاری می‌پردازد؛ «سیاست جنایی قضایی» (*Judicial Criminal Policy*) که به اعمال و تفسیر قانون ناظر است؛ و «سیاست جنایی اجرایی» (*Enforcement Criminal Policy*) که به اجرای احکام صادره

می‌پردازد. در این پژوهش، ارزیابی کارآمدی سیاست جنایی دو کشور در هر سه بُعد انجام می‌شود. این رویکرد سه‌بُعدی، که جامعیت بیشتری نسبت به تحلیل‌های یک‌بُعدی دارد، تصویر واقع‌بینانه‌تری از وضعیت موجود ارائه می‌دهد (Mohseni, 2019).

«کارآمدی» (*Effectiveness*) سیاست جنایی مفهومی است که باید با دقت تعریف شود. در این پژوهش، سیاست جنایی کارآمد به سیاستی اطلاق می‌شود که: (۱) با هدف اعلام‌شده خود، پیشگیری از جرم، حمایت از قربانیان، مجازات مجرمان، همخوانی داشته باشد؛ (۲) قابل اجرا در عمل باشد؛ (۳) آثار جانبی منفی ناخواسته‌ای نداشته باشد؛ و (۴) با ارزش‌های اجتماعی–فرهنگی جامعه هدف سازگار باشد. این تعریف چهاربُعدی، که از آثار نظری معتبر مثل پلر و آندنز الهام گرفته، معیاری دقیق‌تر از صرف وجود قانون برای ارزیابی کارآمدی فراهم می‌کند (Bentham, 1789). در اعمال این معیار بر نظام‌های حقوقی ایران و افغانستان، خواهیم دید که قانون وجود دارد، اما کارآمدی به‌معنای واقعی کلمه کمتر تأمین می‌شود (Abbasi, 2020).

مدل سیاست جنایی یکپارچه

«سیاست جنایی یکپارچه» (*Integrated Criminal Policy*) مدلی است که بر همسویی و هماهنگی میان اقدامات پیشگیرانه، کیفری، حمایتی، و بازتوانی‌محور تأکید دارد. این مدل، که از آثار لاپی–سپالا در سیاست جنایی اسکاندیناوی و بوزا درباره جوامع در حال گذار الهام گرفته، سه مؤلفه اصلی دارد: (۱) «مؤلفه پیشگیرانه» که شامل آموزش، طراحی ایمن محیط دیجیتال، و مداخله زودهنگام است؛ (۲) «مؤلفه کیفری» که شامل جرم‌انگاری متناسب، مجازات‌های بازدارنده، و رویه قضایی منسجم است؛ و (۳) «مؤلفه حمایتی» که شامل خدمات به قربانیان، جبران خسارت، و توانبخشی اجتماعی است (Clough, 2015; Lappi-Seppälä, 2011). ارزیابی هر دو کشور نشان خواهد داد که مؤلفه کیفری نسبتاً قوی‌تر بوده، اما دو مؤلفه دیگر به‌شدت ضعیف هستند.

«نظریه بازدارندگی» (*Deterrence Theory*) که از بنتام به میراث رسیده، استدلال می‌کند که ترس از مجازات رفتار مجرمانه را کاهش می‌دهد (Bentham, 1789). این نظریه پیش‌بینی می‌کند که برای بازدارندگی مؤثر باید سه شرط تأمین شود: «قطعیت» (*Certainty*) مجازات، «سرعت» (*Swiftness*) آن، و «شدت» (*Severity*) آن. بررسی نظام حقوقی هر دو کشور نشان می‌دهد که هر سه شرط به‌اندازه کافی تأمین نشده‌اند: قطعیت مجازات به دلیل ضعف در تحقیقات قضایی پایین است؛ رسیدگی‌ها کند است؛ و مجازات‌ها در برخی موارد متناسب با شدت جرم نیستند. این ارزیابی توضیح می‌دهد که چرا صرف وجود قانون کیفری برای کاهش جرایم سایبری علیه حریم خصوصی کافی نبوده است (Saberi, 2019).

سیاست جنایی اسلامی در حوزه سایبری

فقه اسلامی، به‌عنوان منبع اصلی قانون‌گذاری در هر دو کشور، اصول مشخصی برای سیاست جنایی در حوزه حریم خصوصی ارائه می‌دهد. «قاعده لا ضرر و لا ضرار» (ضرر نرسان و ضرر نپذیر) اصلی است که می‌تواند مبنای جرم‌انگاری هر رفتاری باشد که به حریم خصوصی دیگران آسیب می‌رساند. «قاعده درء» (رفع شک در اجرای مجازات) مکانیسم قضایی مهمی است که در فقه اسلامی برای جلوگیری از مجازات بی‌گناهان وجود دارد. و «مقاصد الشریعه»، که حفظ جان، عقل، دین، نسل، و مال را هدف شریعت می‌داند، می‌تواند به‌عنوان چارچوب هدف‌گذاری برای سیاست جنایی در هر دو کشور به کار رود. تلفیق این اصول با دانش مدرن جرم‌شناسی می‌تواند سیاست جنایی‌ای ایجاد کند که هم از مشروعیت دینی برخوردار باشد و هم از کارایی علمی (Kariminia, 2019).

چارچوب حقوق بشر بین‌الملل و سیاست جنایی سایبری

سیاست جنایی سایبری هر کشور نمی‌تواند بدون توجه به تعهدات بین‌المللی آن کشور طراحی شود. ایران و افغانستان هر دو عضو سازمان ملل متحد و متعهد به میثاق بین‌المللی حقوق مدنی و سیاسی (*ICCPR*) هستند که ماده ۱۷ آن از حریم خصوصی حمایت می‌کند. کمیته حقوق بشر سازمان ملل در تفسیر عمومی شماره ۱۶ (۱۹۸۸) روشن کرده که این حمایت شامل فضای دیجیتال نیز می‌شود. قطعنامه‌های ۱۶۷/۶۸ و ۱۶۶/۶۹ مجمع عمومی سازمان ملل (۲۰۱۳ و ۲۰۱۴) به‌صراحت تأکید کرده‌اند که حق حریم خصوصی آنلاین باید همان‌قدر که آفلاین حمایت می‌شود، در فضای مجازی نیز محترم شمرده شود. این چارچوب بین‌المللی، که برای هر دو کشور الزام‌آور است، معیارهای حداقلی برای ارزیابی کارآمدی سیاست جنایی سایبری آن‌ها فراهم می‌کند (Salehi, 2022).

«اصول ضروری» (*Necessary and Proportionate Principles, 2013*)، که توسط ائتلاف بین‌المللی سازمان‌های مدنی تدوین شده، سیزده اصل برای نظارت قانونی بر ارتباطات دیجیتال تعریف می‌کند. این اصول، که بر «قانونی بودن»، «ضرورت»، «تناسب»، «نظارت قضایی مستقل»، و «پاسخگویی» تأکید دارند، معیار مفیدی برای ارزیابی قوانین نظارت سایبری ایران و افغانستان فراهم می‌کنند (Unodc, 2013). بررسی قوانین هر دو کشور نشان می‌دهد که در برخی از این اصول، به‌ویژه «شفافیت» و «نظارت قضایی مستقل»، نقص‌هایی وجود دارد که باید رفع شوند. در ایران، اختیارات نظارتی دستگاه‌های امنیتی در قوانین به‌طور کامل مشخص نشده؛ در افغانستان، ساختارهای نظارت قضایی مستقل کافی وجود ندارد. رفع این نقص‌ها نه‌تنها از منظر حقوق بشر بین‌المللی ضروری است، بلکه از منظر کارآمدی سیاست جنایی نیز اهمیت دارد، زیرا اعتماد مردم به سیستم را تقویت می‌کند.

مقررات عمومی حفاظت از داده اتحادیه اروپا (*GDPR, 2016*)، که در سال ۲۰۱۸ اجرایی شد، یکی از پیشرفته‌ترین چارچوب‌های حمایت از حریم خصوصی دیجیتال در جهان است. هرچند ایران و افغانستان عضو اتحادیه اروپا نیستند، *GDPR* چندین درس مهم برای سیاست جنایی سایبری آن‌ها دارد: اول، اهمیت تعریف دقیق و جامع «داده شخصی»؛ دوم، ضرورت اصل «رضایت آگاهانه» (*Informed Consent*) به‌عنوان پایه جمع‌آوری داده؛ سوم، حق «فراموش‌شدن» (*Right to be Forgotten*) که به افراد اجازه می‌دهد حذف اطلاعات خود را از پایگاه‌های اطلاعاتی بخواهند؛ چهارم، مسئولیت «کنترل‌کنندگان داده» (*Data Controllers*) در برابر نهاد مستقل ناظر؛ و پنجم، جریمه‌های سنگین برای نقض‌های جدی که بازدارندگی ایجاد می‌کنند (Nissenbaum, 2010). تطبیق این اصول با ارزش‌های اسلامی، رویکردی بومی–جهانی به سیاست جنایی سایبری ایجاد می‌کند که برای هر دو کشور مناسب است.

نقش سازمان همکاری اسلامی (*OIC*) در توسعه سیاست جنایی سایبری برای کشورهای اسلامی هنوز به‌اندازه کافی مورد توجه قرار نگرفته است. *OIC* می‌تواند نقش مهمی در هماهنگ‌سازی قوانین سایبری کشورهای عضو، توسعه «اعلامیه اسلامی حقوق دیجیتال»، و ایجاد مکانیسم‌های همکاری قضایی در جرایم سایبری فرامرزی ایفا کند. ایران و افغانستان، به‌عنوان کشورهایی که هر دو عضو *OIC* هستند، می‌توانند پیش‌قدم در طراحی یک چارچوب منطقه‌ای برای سیاست جنایی سایبری اسلامی باشند. این چارچوب، که از یک‌سو ارزش‌های مشترک اسلامی را منعکس می‌کند و از سوی دیگر با استانداردهای بین‌المللی همخوانی دارد، می‌تواند الگویی برای سایر کشورهای اسلامی نیز باشد. تجربه ایران در قانون‌گذاری سایبری و ظرفیت اسلامی افغانستان، این دو کشور را در موقعیت منحصربه‌فردی برای رهبری این پروژه قرار می‌دهد.

روش‌شناسی

این پژوهش از نوع کاربردی، با رویکرد توصیفی-تحلیلی و روش مطالعه تطبیقی است. برای ارزیابی کارآمدی سیاست جنایی، از یک «ماتریس ارزیابی» استفاده شده که هر یک از سه مؤلفه سیاست جنایی، تقنینی، قضایی، اجرایی، را در هر کشور با شش شاخص مشخص می‌سنجد: (۱) کامل‌بودن؛ (۲) دقت تعریفی؛ (۳) انسجام درونی؛ (۴) قابلیت اجرا؛ (۵) اثربخشی عملی؛ و (۶) انطباق با استانداردهای بین‌المللی. هر شاخص با مقیاس سه‌سطحی، ناکافی، نسبتاً کافی، کافی، ارزیابی می‌شود. داده‌های تحقیق از منابع اولیه، متون قانونی، اسناد رسمی، منابع ثانویه، ادبیات علمی، گزارش‌های سازمان‌های بین‌المللی، و گزارش‌های آماری موجود جمع‌آوری شده‌اند. برای اطمینان از اعتبار یافته‌ها، روش «تثلیث» از چندین منبع مستقل بهره می‌گیرد (Farahmand, 2021).

چارچوب ارزیابی کارآمدی این پژوهش، از آثار نظری مهم در حوزه حقوق و سیاست جنایی مقایسه‌ای الهام گرفته است. نظریه «سیاست جنایی تفاضلی» برنار، مدل «چرخه سیاست کیفری» ایگلتون، و چارچوب «ارزیابی تأثیر قانون» (*Legislative Impact Assessment*)، که در اتحادیه اروپا توسعه یافته، هر یک جنبه‌هایی از ارزیابی کارآمدی سیاست جنایی را روشن می‌کنند (Delmas-Marty, 1986; Zweigert & Kötz, 1998). از آنجا که هیچ‌یک از این چارچوب‌ها به‌طور اختصاصی برای کشورهای اسلامی طراحی نشده‌اند، در این پژوهش تطبیق لازم با در نظر گرفتن ارزش‌های اسلامی و شرایط خاص ایران و افغانستان صورت گرفته است. محدودیت‌های پژوهش شامل دسترسی محدود به آمار رسمی جرایم سایبری و فقدان پرونده‌های قضایی منتشرشده است.

ارزیابی سیاست جنایی ایران

مؤلفه تقنینی

سیاست جنایی تقنینی ایران در حوزه جرایم سایبری علیه حریم خصوصی، مجموعه‌ای از قوانین را در بر می‌گیرد که قانون جرایم رایانه‌ای (۱۳۸۸) محور اصلی آن است. این قانون، که در زمان تصویب خود پیشگام در منطقه بود، رویکرد کیفری-تقنینی روشنی دارد. با این حال، ارزیابی با شش شاخص نشان می‌دهد: «کامل‌بودن» (نسبتاً کافی)، چراکه برخی جرایم نوظهور، مثل دیپ‌فیک و باج‌گیری جنسی دیجیتال، پوشش ندارند؛ «دقت تعریفی» (ناکافی)، به دلیل ابهام در تعریف «داده شخصی» و «رضایت»؛ «انسجام درونی» (نسبتاً کافی)، با وجود برخی تداخل‌ها با قانون مجازات اسلامی؛ «قابلیت اجرا» (نسبتاً کافی)، با توجه به وجود نهادهای اجرایی؛ «اثربخشی عملی» (ناکافی)، به دلیل شکاف میان قانون و اجرا؛ و «انطباق بین‌المللی» (نسبتاً کافی)، با توجه به کاستی‌های مقایسه با *GDPR* و کنوانسیون بوداپست (Hosseini, 2021). یکی از چالش‌های اساسی سیاست جنایی تقنینی ایران، «پراکندگی تقنینی» است. قوانین مرتبط با حریم خصوصی دیجیتال در چندین قانون پراکنده‌اند: قانون جرایم رایانه‌ای، قانون مجازات اسلامی (مواد ۶۹۴ و ۶۹۸)، قانون آیین دادرسی کیفری، و قانون تجارت الکترونیک. این پراکندگی، که «تورم قانونی» (*Legal Inflation*) نامیده می‌شود، موجب تداخل، ابهام، و تفسیرهای متضاد می‌شود. از منظر نظریه بازدارندگی، وقتی قانون پیچیده و غیرشفاف باشد، «قطعیت ادراک‌شده» مجازات کاهش می‌یابد و در نتیجه، بازدارندگی تضعیف می‌شود. تدوین یک قانون جامع حفاظت از داده‌های شخصی که این پراکندگی را رفع کند، از فوری‌ترین نیازهای سیاست جنایی تقنینی ایران است (Alizadeh, 2018).

مؤلفه قضایی

سیاست جنایی قضایی ایران در حوزه جرایم سایبری علیه حریم خصوصی، با چالش‌های متعددی روبه‌روست که اثربخشی آن را محدود می‌کند. نخست، «چالش تفسیری»: قضات با مواد قانونی مبهمی مواجه می‌شوند که تفسیرهای متضادی در دادگاه‌های مختلف به بار می‌آورد. این عدم یکنواختی، که «شکاف رویه‌ای» (*Jurisprudential Gap*) نامیده می‌شود، اصل «قابل پیش‌بینی بودن حقوق» را تضعیف می‌کند. دوم، «چالش اثباتی»: ادله دیجیتال در دادگاه‌های ایران هنوز با مقاومت‌هایی روبه‌رو است؛ قضات اغلب با مفاهیم فنی مثل متادیتا، لاگ‌های سرور، و *IP* آدرس آشنایی کافی ندارند. از منظر «عدالت رویه‌ای» (*Procedural Justice*)، وقتی قربانیان احساس کنند که سیستم قضایی به‌درستی پرونده آن‌ها را رسیدگی نمی‌کند، اعتماد به حاکمیت قانون کاهش می‌یابد (Mousavi, 2020).

مدت طولانی رسیدگی به پرونده‌های سایبری در دادگاه‌های ایران از دیگر چالش‌های مؤلفه قضایی است. در جرایمی مثل انتشار تصاویر خصوصی، که هر روز تأخیر به ادامه آسیب به قربانی منجر می‌شود، این تأخیر پیامدهای جدی دارد. ایجاد مکانیسم‌های «رسیدگی اورژانسی» (*Emergency Procedures*) برای جرایم سایبری با آثار فوری، یکی از اصلاحات ضروری در مؤلفه قضایی است. همچنین، صدور دستورالعمل‌های تفسیری روشن از سوی دیوان عالی کشور برای ایجاد رویه قضایی یکنواخت در جرایم سایبری، می‌تواند به‌طور قابل توجهی کارآمدی سیاست جنایی قضایی را ارتقا دهد. این دستورالعمل‌ها، که هزینه نسبتاً پایینی دارند، می‌توانند در کوتاه‌مدت اثربخشی بالایی داشته باشند.

مؤلفه اجرایی

سیاست جنایی اجرایی ایران در این حوزه، با شکاف قابل توجهی بین ظرفیت موجود و نیاز واقعی روبه‌روست. پلیس فتا، که متولی اصلی این حوزه است، از محدودیت‌های منابع انسانی، فنی، و اطلاعاتی رنج می‌برد. نسبت پرونده‌های دریافتی به پرونده‌های رسیدگی‌شده، نشان‌دهنده «گلوگاه اجرایی» در این مرحله است. همچنین، «مسئله گزارش‌دهی» (*Reporting Problem*) جدی است: بررسی‌ها نشان می‌دهند که درصد بالایی از قربانیان جرایم سایبری علیه حریم خصوصی هرگز شکایت رسمی تسلیم نمی‌کنند. دلایل این امر متعدد است: ترس از بدتر شدن وضعیت با مطرح‌شدن موضوع، بی‌اعتمادی به سرعت و کارایی پاسخ پلیس، و احساس شرم و بزه‌دیدگی ثانویه. این «عدد تاریک» (*Dark Figure*) جرایم سایبری، آمارهای رسمی را بسیار پایین‌تر از واقعیت نشان می‌دهد (Farahmand, 2021).

با این حال، باید از دستاوردهای پلیس فتا در طول بیش از یک دهه فعالیت نیز سخن گفت. توسعه ظرفیت‌های تحقیقاتی دیجیتال، اجرای کمپین‌های آگاهی‌بخشی، و ایجاد خطوط اورژانسی برای گزارش جرایم سایبری از جمله اقدامات مثبت بوده‌اند. حضور پلیس فتا در شبکه‌های اجتماعی و همکاری با مدارس در آموزش سواد دیجیتال نیز از جمله ابتکاراتی هستند که اثر پیشگیرانه دارند. چالش اصلی، مقیاس‌پذیری این اقدامات است: با رشد سریع کاربران اینترنت در ایران، منابع موجود به‌سرعت ناکافی می‌شوند. این موضوع لزوم سرمایه‌گذاری مستمر و برنامه‌ریزی‌شده در توسعه ظرفیت اجرایی را برجسته می‌کند.

تحلیل کارآمدی مکانیسم‌های پیشگیری در ایران

پیشگیری از جرایم سایبری علیه حریم خصوصی در ایران در سه سطح قابل بررسی است. «پیشگیری اولیه» (*Primary Prevention*)، که هدف آن جلوگیری از وقوع جرم پیش از شروع آن است، در ایران عمدتاً از طریق آموزش عمومی و کمپین‌های آگاهی‌بخشی دنبال می‌شود. پلیس فتا، وزارت آموزش‌وپرورش، و برخی سازمان‌های غیردولتی در این زمینه فعال بوده‌اند، اما سطح هماهنگی و جامعیت برنامه‌ها ناکافی

است. «طراحی ایمن» (*Safety by Design*)، که در آن الزامات امنیتی از ابتدا در محصولات دیجیتال گنجانده می‌شوند، در قوانین ایران به‌کفایت مقرر نشده است. این در حالی است که در اتحادیه اروپا، *GDPR* شرکت‌ها را ملزم به رعایت اصل «حریم خصوصی از ابتدا طراحی‌شده» (*Privacy by Design*) می‌کند. اعمال این الزام در ایران می‌تواند از بروز بسیاری از نقض‌های حریم خصوصی پیشگیری کند (Alizadeh, 2018).

«پیشگیری ثانویه» (*Secondary Prevention*)، که بر شناسایی گروه‌های پرخطر و مداخله زودهنگام تأکید دارد، در ایران نیازمند توسعه جدی است. برنامه‌های هدفمند برای زنان جوان که بیشترین ریسک بزه‌دیدگی را دارند، کودکان و نوجوانانی که در فضای آنلاین تازه‌وارد هستند، و کاربران کم‌سواد دیجیتال، از نیازهای اصلی پیشگیری ثانویه هستند. خطوط کمک ویژه برای گزارش تهدیدات سایبری، سیستم‌های هشدار اولیه برای شناسایی محتوای مضر، و برنامه‌های مداخله در جوامع آسیب‌پذیر از جمله اقداماتی هستند که باید توسعه یابند. «پیشگیری ثالثه» (*Tertiary Prevention*)، که به کمک به قربانیان پس از وقوع جرم می‌پردازد، ضعیف‌ترین بُعد پیشگیری در ایران است. خدمات مشاوره روان‌شناختی، کمک حقوقی رایگان، و مکانیسم‌های سریع حذف محتوا از جمله خلأهای اصلی در این حوزه هستند که باید با برنامه‌ریزی و سرمایه‌گذاری هدفمند برطرف شوند.

«اقتصاد جرم» (*Economics of Crime*) چارچوب مفیدی برای ارزیابی کارآمدی مکانیسم‌های پیشگیرانه ایران فراهم می‌کند. بکر، در مقاله کلاسیک «جرم و مجازات: رویکرد اقتصادی»، استدلال کرد که مجرمان عقلایی عمل می‌کنند و منافع و هزینه‌های جرم را می‌سنجند (Bentham, 1789). این دیدگاه پیشنهاد می‌کند که سیاست جنایی باید هم «هزینه جرم» (مجازات احتمالی) را بالا ببرد و هم «منافع جرم» (فایده‌ای که مجرم دنبال می‌کند) را کاهش دهد. در ایران، تمرکز عمدتاً بر بالا بردن هزینه از طریق مجازات بوده، اما کاهش منافع از طریق کاهش دسترسی به «ابزارهای جرم» (مثل پلتفرم‌های ناامن) و «محتوای هدف» (مثل کاهش دسترسی به اطلاعات شخصی) کمتر مورد توجه بوده است. این تعادل نادرست، کارآمدی کلی سیاست پیشگیرانه را کاهش می‌دهد.

«ارزیابی تأثیر سیاست» (*Policy Impact Assessment*) برای مکانیسم‌های پیشگیرانه ایران نشان می‌دهد که هنوز داده‌های کافی برای سنجش اثربخشی این مکانیسم‌ها وجود ندارد. بدون «شاخص‌های کلیدی عملکرد» (*Key Performance Indicators*) مشخص برای سنجش کاهش جرایم، افزایش گزارش‌دهی، یا بهبود وضعیت قربانیان، نمی‌توان گفت که اقدامات انجام‌شده چقدر مؤثر بوده‌اند. این «فقدان شواهد»، که سیاست‌گذاری مبتنی بر شواهد (*Evidence-Based Policy Making*) را دشوار می‌کند، از مشکلات اساسی است. ایجاد یک سیستم پایش و ارزیابی منظم که داده‌های قابل اعتماد درباره جرایم سایبری جمع‌آوری کند، پیش‌نیاز هر اصلاح مبتنی بر شواهدی است که بخواهد در این حوزه انجام شود (Farahmand, 2021).

ارزیابی سیاست جنایی افغانستان

مؤلفه تقنینی

سیاست جنایی تقنینی افغانستان در حوزه جرایم سایبری علیه حریم خصوصی، در مقایسه با ایران در مراحل ابتدایی‌تری قرار دارد. فصل پنجم قانون جزا (مصوب ۱۳۹۷) تنها منبع تقنینی مشخص در این حوزه است که از جامعیت کافی برخوردار نیست. ارزیابی با شش شاخص نشان می‌دهد: «کامل‌بودن» (ناکافی)، به دلیل نبود جرم‌انگاری صریح برای اکثر جرایم نوظهور؛ «دقت تعریفی» (ناکافی)، به دلیل فقدان تعریف «داده شخصی» و سایر مفاهیم کلیدی؛ «انسجام درونی» (نسبتاً کافی)، زیرا پراکندگی تقنینی مثل ایران وجود ندارد؛ «قابلیت اجرا» (ناکافی)، به دلیل

فقدان نهادهای اجرایی تخصصی؛ «اثربخشی عملی» (ناکافی)؛ و «انطباق بین‌المللی» (ناکافی). در مجموع، سیاست جنایی تقنینی افغانستان در این حوزه به تحول اساسی نیاز دارد (Salehi, 2022).

با این حال، پشتوانه فقهی–اسلامی نظام حقوقی افغانستان یک مزیت منحصربه‌فرد ایجاد می‌کند. در چارچوب امارت اسلامی، احکام فقهی مستقیماً بر قانون‌گذاری تأثیر می‌گذارند. آیاتی مثل «لَا تَجَسَّسُوا» و احادیث نبوی درباره حرمت اسرار دیگران، مبنای دینی محکمی برای جرم‌انگاری نقض حریم خصوصی فراهم می‌کنند. این پشتوانه، که در ایران نیز مشترک است اما در افغانستان نقش مستقیم‌تری در قانون‌گذاری دارد، می‌تواند به ایجاد «قوانین سایبری اسلامی» کمک کند که از پذیرش اجتماعی بالاتری برخوردار باشند. چالش اصلی، «اجتهاد دیجیتال»، یعنی استنباط احکام فقهی مشخص برای مسائل فضای مجازی است که هنوز به‌اندازه کافی انجام نشده است (Bagherinejad, 2020).

مؤلفه قضایی

سیاست جنایی قضایی افغانستان در حوزه جرایم سایبری با چالش‌های ساختاری جدی روبه‌روست. نخست، قضاتی که باید به جرایم سایبری رسیدگی کنند، عمدتاً در نظام قضایی سنتی آموزش دیده‌اند و با مسائل فنی فضای مجازی آشنایی کافی ندارند. دوم، رویه قضایی مدون در زمینه جرایم سایبری تقریباً وجود ندارد که این موجب می‌شود هر قاضی بر اساس فهم شخصی خود عمل کند. سوم، «نظام دوگانه» قضایی، نظام رسمی دولتی + جرگه‌های عرفی، موجب می‌شود که بسیاری از پرونده‌های سایبری هرگز به دادگاه رسمی نرسند. از منظر نظریه بازدارندگی، این وضعیت «قطعیت ادراک‌شده» مجازات را به‌شدت کاهش می‌دهد (Alizadeh, 2018).

باید توجه داشت که نظام جرگه‌ای در افغانستان، جنبه‌های مثبت نیز دارد. این نظام، که از قرن‌ها پیش برای حل اختلافات اجتماعی به کار رفته، از پذیرش عمومی بیشتری نسبت به دادگاه‌های رسمی برخوردار است. اگر این نظام با اصول فقه اسلامی در حوزه حریم خصوصی آموزش ببیند، مثلاً در جرایم ناموسی سایبری، می‌تواند بخشی از «پیشگیری ثالثه» را از طریق مصالحه و جبران خسارت عهده‌دار شود. این «دوگانگی کارکردی»، که در آن نظام رسمی و عرفی مکمل هم باشند، می‌تواند یک راهبرد اجرایی نوآورانه برای افغانستان باشد که با شرایط خاص این کشور سازگار است.

مؤلفه اجرایی

مؤلفه اجرایی سیاست جنایی افغانستان در این حوزه، در مرحله ابتدایی قرار دارد. نبود واحد تخصصی پلیس سایبری مجهز، پایین‌بودن سطح سواد دیجیتال در میان نیروهای انتظامی، و فقدان تجهیزات تحقیقات جنایی دیجیتال از چالش‌های اصلی هستند. این وضعیت با تقاضای رو به رشد برای رسیدگی به شکایات سایبری، با رشد ضریب نفوذ اینترنت در کشور، فاصله روزافزونی ایجاد می‌کند. «شکاف ظرفیت» (*Capacity Gap*)، که در افغانستان حادتر از ایران است، اولین مانعی است که باید با سرمایه‌گذاری هدفمند و کمک بین‌المللی برطرف شود (Hosseini, 2021).

ظرفیت منحصربه‌فرد افغانستان در مؤلفه اجرایی، شبکه گسترده مساجد و مدارس دینی است که می‌توانند در آموزش عمومی درباره حریم خصوصی دیجیتال نقش مؤثری ایفا کنند. خطبه‌های جمعه، کلاس‌های مدارس دینی، و برنامه‌های آموزشی مساجد می‌توانند پیام‌هایی را منتقل کنند که هم دینی و هم عملی هستند: «تجسس در امور دیگران حرام است»، «نشر تصاویر خصوصی دیگران گناه کبیره و جرم است»، «قربانیان نیاز به حمایت دارند، نه سرزنش». این رویکرد، که از پایین به بالا (*Bottom-Up*) کار می‌کند، می‌تواند تکمیل‌کننده مؤثری برای اقدامات

رسمی از بالا به پایین (*Top-Down*) باشد. در حقیقت، ترکیب این دو رویکرد، یکی از بهترین الگوهای سیاستی در دسترس افغانستان است.

ارزیابی ظرفیت‌های بالقوه افغانستان

ارزیابی واقع‌بینانه وضعیت افغانستان نباید صرفاً به ضعف‌ها تمرکز کند، بلکه باید ظرفیت‌های بالقوه‌ای را که می‌توانند در توسعه سیاست جنایی سایبری کارآمد به کار روند نیز به رسمیت بشناسد. مهم‌ترین این ظرفیت‌ها، «سرمایه اجتماعی» (*Social Capital*) مبتنی بر اعتماد دینی است. در جوامعی که اعتماد به نهادهای رسمی پایین است اما اعتماد به مراجع دینی بالا است، «سیاست جنایی دینی–مدنی» می‌تواند نتایجی بهتر از سیاست‌های صرفاً رسمی داشته باشد. وقتی فتوای یک عالم دینی معتبر می‌گوید «انتشار تصاویر خصوصی دیگران حرام و گناه کبیره است»، این پیام از هر تبلیغات دولتی مؤثرتر خواهد بود. این سرمایه اجتماعی–دینی، که در ایران نیز وجود دارد اما در افغانستان قوی‌تر است، باید در مرکز راهبرد پیشگیری از جرایم سایبری قرار گیرد.

«نهادهای میانجی» (*Intermediary Institutions*)، که در افغانستان شامل جرگه‌ها، شوراها، و کمیته‌های محله‌ای می‌شوند، می‌توانند نقش مهمی در سیاست جنایی سایبری ایفا کنند. این نهادها، که از اعتبار اجتماعی بالایی برخوردارند، می‌توانند در آموزش عمومی، پیشگیری از جرم، و حمایت از قربانیان نقش‌آفرینی کنند. البته باید توجه داشت که برخی از این نهادها ممکن است هنجارهای سنتی‌ای داشته باشند که با استانداردهای حقوق بشر بین‌المللی همخوانی کامل ندارند، به‌ویژه در مورد حقوق زنان. بنابراین، هدف باید «اصلاح» این نهادها از طریق آموزش اصول اسلامی صحیح باشد، نه «حذف» آن‌ها که واقع‌بینانه هم نیست. ترکیب سنت و نوآوری در طراحی سیاست جنایی افغانستان، چالش اصلی اما دست‌یافتنی است.

«همکاری منطقه‌ای» (*Regional Cooperation*) با کشورهای همسایه، به‌ویژه ایران و پاکستان، فرصت ارزشمندی برای افغانستان است که هنوز به‌اندازه کافی از آن استفاده نشده است. هر سه کشور با چالش‌های مشابهی در حوزه جرایم سایبری روبه‌رو هستند و از اشتراکات فرهنگی–دینی قابل توجهی برخوردارند. پاکستان با تجربه «قانون پیشگیری از جرایم الکترونیکی» (*Prevention of Electronic Crimes Act 2016*)، تجربه قانون‌گذاری مشخصی دارد که برای افغانستان الگویی مناسب‌تر از قوانین غربی است. ایران با تجربه پلیس فتا و دادگاه‌های سایبری، منبع ارزشمندی برای انتقال دانش است. ایجاد «ائتلاف سایبری اسلام‌محور» که این تجربیات را یکجا گرد هم آورد، می‌تواند به هر سه کشور کمک کند تا از اشتباهات یکدیگر بیاموزند و موفقیت‌های هم را تکرار کنند.

بُعد «اقتصادی سیاست جنایی» در افغانستان باید با واقع‌بینی ارزیابی شود. سیاست‌هایی که هزینه بالایی دارند، مثل ایجاد آزمایشگاه‌های پیشرفته جنایی دیجیتال یا استخدام صدها متخصص سایبری در کوتاه‌مدت، برای افغانستان واقع‌بینانه نیستند. اما سیاست‌هایی مثل آموزش ۲۰ تا ۳۰ متخصص هسته‌ای از طریق کمک بین‌المللی، صدور فتاوای علما درباره حریم خصوصی دیجیتال، تدوین قانون سایبری با کمک مشاوران خارجی، و آموزش قضات از طریق برنامه‌های آموزشی آنلاین، هزینه نسبتاً پایین اما اثر قابل توجهی خواهند داشت. این «اصلاحات کم‌هزینه–پراثر» (*High-Impact Low-Cost Reforms*)، که در محافل توسعه بین‌المللی شناخته‌شده هستند، باید اولویت اول برنامه‌ریزی افغانستان در این حوزه باشند (Hosseini, 2021).

ارزیابی تطبیقی و بحث

مقایسه کارآمدی

ارزیابی تطبیقی سیاست جنایی دو کشور بر اساس ماتریس سه‌بُعدی نشان می‌دهد: در «مؤلفه تقنینی»، ایران امتیاز ۱۴/۱۰ (نسبتاً کافی) و افغانستان امتیاز ۱۴/۵ (ناکافی) دارد. در «مؤلفه قضایی»، ایران امتیاز ۱۴/۸ (نسبتاً کافی) و افغانستان ۱۴/۴ (ناکافی) دارد. در «مؤلفه اجرایی»، ایران ۱۴/۷ (نسبتاً ناکافی) و افغانستان ۱۴/۳ (ناکافی) دارد. در «جمع کل»، ایران ۴۲/۲۵ (۵۹٪) و افغانستان ۴۲/۱۲ (۲۹٪) است که هر دو از آستانه «کارآمدی قابل قبول» (۶۰٪) پایین‌تر هستند. این یافته، که «هیچ‌کدام از دو نظام به سطح کارآمدی قابل قبول نرسیده‌اند»، فرضیه اصلی پژوهش را تأیید می‌کند (Salehi, 2022).

«شکاف اجرا» (*Implementation Gap*)، که فاصله میان قانون مکتوب و اجرای واقعی است، در هر دو کشور مشاهده می‌شود، اما در ایران برجسته‌تر است. در ایران، قوانین نسبتاً بهتری وجود دارند، اما اجرا ضعیف است؛ در افغانستان، هم قانون و هم اجرا ضعیف هستند. این تفاوت، پیامدهای سیاستی متفاوتی دارد: ایران باید بیشتر روی ظرفیت‌سازی اجرایی سرمایه‌گذاری کند، در حالی که افغانستان باید به‌طور همزمان هم قوانین و هم ظرفیت‌ها را توسعه دهد. این «دو مسیر اصلاح»، که برای هر کشور متفاوت است، باید در برنامه‌ریزی‌های آینده مدنظر قرار گیرد (Mousavi, 2020).

الگوهای مشترک و درس‌های متقابل

تحلیل تطبیقی سه الگوی مشترک را آشکار می‌کند که در هر دو نظام وجود دارند. الگوی اول، «تمرکز بر کیفر به‌بهای پیشگیری» است. هر دو کشور بیشترین منابع را به مجازات پس از وقوع جرم اختصاص داده‌اند و از سرمایه‌گذاری در پیشگیری اولیه و ثانویه غافل مانده‌اند. این در حالی است که شواهد بین‌المللی نشان می‌دهند که هزینه–اثربخشی پیشگیری از جرم بسیار بالاتر از کیفر پس از وقوع جرم است. الگوی دوم، «فراموش‌کردن قربانی» است. در هر دو نظام، قربانیان جرایم سایبری علیه حریم خصوصی از حمایت‌های ناکافی برخوردارند و مکانیسم‌های جبران خسارت ضعیف هستند. الگوی سوم، «استفاده‌نشده ماندن ظرفیت اسلامی» است؛ پشتوانه غنی فقهی–اسلامی در حوزه حریم خصوصی هنوز به‌درستی در سیاست جنایی این دو کشور به کار گرفته نشده است (Abbasi, 2020).

درس‌هایی که دو کشور می‌توانند از یکدیگر بگیرند نیز قابل توجه است. ایران می‌تواند از رویکرد اجتهادی افغانستان در ترجمه احکام فقهی به سیاست جنایی سایبری بیاموزد. افغانستان می‌تواند از تجربه نهادی ایران در ساختاردهی به پلیس سایبری و دادگاه‌های تخصصی استفاده کند. هر دو کشور می‌توانند از تجربه موفق کشورهایی مثل مالزی و اندونزی، که در توسعه «سیاست جنایی سایبری اسلامی» پیشرفت‌های قابل توجهی داشته‌اند، الهام بگیرند. مالزی با ترکیب قانون «*Personal Data Protection Act 2010*» با ارزش‌های اسلامی، توانسته چارچوب نسبتاً موفقی ایجاد کند که هم از نظر اجتماعی پذیرفته شده و هم از نظر اجرایی قابل تطبیق است (Saberi, 2019).

مطالعه موردی: ارزیابی اثربخشی پلیس فتا به‌عنوان نهاد سیاست جنایی

پلیس فتا، پلیس فضای تولید و تبادل اطلاعات، ایران، به‌عنوان نهاد محوری سیاست جنایی اجرایی این کشور در حوزه جرایم سایبری، نمونه مفیدی برای ارزیابی است. تأسیس این نهاد در سال ۱۳۹۰ نشان‌دهنده تشخیص دولت ایران از اهمیت جرایم سایبری بود؛ گامی که افغانستان هنوز برنداشته است. ارزیابی اثربخشی این نهاد بر اساس چارچوب «سیاست جنایی یکپارچه» این پژوهش، نتایج آمیخته‌ای را نشان می‌دهد. از منظر «مؤلفه کیفری»، پلیس فتا در شناسایی، ردیابی، و دستگیری برخی از مجرمان سایبری موفق بوده است. گزارش‌های سالانه نشان می‌دهند که این نهاد سالانه هزاران پرونده را رسیدگی می‌کند. اما از منظر «مؤلفه پیشگیرانه»، فعالیت‌های آموزشی و آگاهی‌بخشی این نهاد،

اگرچه وجود دارند، اما از انسجام و گستردگی کافی برای تأثیرگذاری بر میلیون‌ها کاربر اینترنت ایران برخوردار نیستند (Farahmand, 2021).

از منظر «مؤلفه حمایتی»، عملکرد پلیس فتا محدودتر است. اگرچه این نهاد کانال‌هایی برای دریافت شکایات دارد، اما خدمات پس از شکایت، مثل مشاوره روان‌شناختی برای قربانیان یا کمک در پیگیری حذف محتوا از پلتفرم‌های خارجی، به‌اندازه کافی توسعه نیافته‌اند. یک چالش ساختاری مهم، این است که پلیس فتا به‌عنوان یک نهاد انتظامی، اساساً برای «کشف و تعقیب جرم» طراحی شده، نه برای «حمایت جامع از قربانی». این محدودیت ساختاری، که در بسیاری از نهادهای پلیسی جهان مشترک است، نیازمند ایجاد نهادهای مکمل، مثل مراکز حمایت از قربانیان که مستقل از پلیس عمل کنند، است. این یافته نشان می‌دهد که حتی نهادهای نسبتاً موفق مثل پلیس فتا، به‌تنهایی نمی‌توانند سیاست جنایی یکپارچه را محقق سازند؛ نیاز به اکوسیستمی از نهادهای مکمل است (Hosseini, 2021).

درس‌های قابل استخراج از تجربه پلیس فتا برای افغانستان قابل توجه‌اند. نخست، تأسیس یک نهاد تخصصی، حتی با منابع محدود در ابتدا، می‌تواند نقطه شروع مهمی باشد که به‌مرور زمان توسعه می‌یابد. دوم، تجربه ایران نشان می‌دهد که حضور در شبکه‌های اجتماعی برای ارتباط مستقیم با کاربران، ابزار قدرتمندی برای آگاهی‌بخشی و دریافت گزارش است. سوم، اما این تجربه همچنین هشدار می‌دهد که تمرکز صرف بر «مؤلفه کیفری» بدون توسعه موازی «مؤلفه‌های پیشگیرانه و حمایتی»، به یک سیاست جنایی نامتوازن منجر می‌شود. افغانستان در طراحی نهاد مشابه خود، باید از ابتدا این سه مؤلفه را به‌صورت متوازن در نظر بگیرد؛ فرصتی که ایران در زمان تأسیس پلیس فتا نداشت، اما اکنون افغانستان دارد (Salehi, 2022).

یک یافته جالب از این مطالعه موردی، نقش «اعتماد عمومی» در اثربخشی نهاد پلیس سایبری است. تحقیقات نشان می‌دهند که میزان مراجعه شهروندان به پلیس فتا، رابطه مستقیمی با سطح اعتماد عمومی به این نهاد دارد. در مواردی که رسانه‌ها گزارش‌های مثبتی از موفقیت پلیس فتا در حل پرونده‌ها منتشر کرده‌اند، افزایش موقتی در نرخ گزارش‌دهی مشاهده شده است. این یافته از منظر «نظریه بازدارندگی» قابل تفسیر است: وقتی «قطعیت ادراک‌شده» مجازات، از طریق مشاهده موفقیت‌های پلیس، افزایش می‌یابد، هم از منظر بازدارندگی برای مجرمان بالقوه و هم از منظر تشویق به گزارش‌دهی برای قربانیان، تأثیر مثبت دارد. این یافته اهمیت «ارتباطات استراتژیک» (*Strategic Communications*) را به‌عنوان جزئی از سیاست جنایی برجسته می‌کند که اغلب نادیده گرفته می‌شود.

محدودیت‌ها و مسیرهای پژوهشی آتی

این پژوهش با چند محدودیت روبه‌روست که شفافیت علمی ایجاب می‌کند بیان شوند. نخست، ارزیابی کارآمدی بر اساس «ماتریس شش‌شاخصی» این پژوهش، اگرچه چارچوب نظام‌مندی فراهم می‌کند، اما به‌ناچار شامل عناصری از قضاوت کیفی است که می‌تواند محل بحث باشد. برای افزایش عینیت، پژوهش‌های آینده می‌توانند از روش‌های «دلفی» (*Delphi Method*) با مشارکت پنل متخصصان برای امتیازدهی استفاده کنند. دوم، این پژوهش عمدتاً بر تحلیل اسناد متکی است و فاقد داده‌های میدانی از تجربه مستقیم بازیگران، قضات، پلیس، قربانیان، است. سوم، شرایط سیاسی و اجتماعی هر دو کشور می‌تواند به‌سرعت تغییر کند، که ممکن است برخی یافته‌ها را در طول زمان منسوخ سازد. این محدودیت‌ها، فرصت‌هایی برای پژوهش‌های تکمیلی هستند، نه نقص‌های اساسی این مطالعه (Abbasi, 2020).

برای پژوهش‌های آینده، چند مسیر مشخص پیشنهاد می‌شود. نخست، «ارزیابی تأثیر مقایسه‌ای» (*Comparative Impact Evaluation*) که با گذشت چند سال از اجرای اصلاحات پیشنهادی این پژوهش، تأثیر واقعی آن‌ها را بسنجد. دوم، مطالعه عمیق‌تر نقش «جرگه‌ها» در

افغانستان و امکان ادغام رسمی آن‌ها در سیاست جنایی سایبری، که نیازمند تحقیق میدانی دقیق در مناطق مختلف است. سوم، توسعه «مدل‌های اقتصادسنجی» (*Econometric Models*) که هزینه–فایده سرمایه‌گذاری در مؤلفه‌های مختلف سیاست جنایی، پیشگیری در برابر کیفر، را برای هر دو کشور محاسبه کند. چهارم، پژوهش تطبیقی با کشورهایی مثل مالزی که سیاست جنایی سایبری اسلامی نسبتاً موفقی دارند، می‌تواند الگوهای انتقال‌پذیر را شناسایی کند. پنجم، بررسی نقش زنان در طراحی و اجرای سیاست جنایی سایبری، هم به‌عنوان قربانیان اصلی و هم به‌عنوان عامل تغییر بالقوه، حوزه‌ای است که نیازمند توجه ویژه پژوهشگران آینده است (Mohseni, 2019).

مدل پیشنهادی «سیاست جنایی سه‌لایه اسلامی»

بر اساس یافته‌های این پژوهش، مدلی سه‌لایه برای سیاست جنایی سایبری در کشورهای اسلامی پیشنهاد می‌شود که می‌تواند راهنمای عملی برای ایران، افغانستان، و سایر کشورهای مشابه باشد. «لایه اول» (پایه دینی–اجتماعی) شامل: فتاوای روشن علما درباره حرمت نقض حریم خصوصی دیجیتال؛ گنجاندن اخلاق دیجیتال در آموزش دینی مساجد و مدارس؛ و کمپین‌های فرهنگی برای انگ‌زدایی از قربانیان. این لایه، که هزینه نسبتاً پایینی دارد، پایه مشروعیت اجتماعی برای لایه‌های بعدی را فراهم می‌کند. «لایه دوم» (چارچوب تقنینی–قضایی) شامل: قوانین جامع و دقیق با تعاریف روشن؛ آموزش تخصصی قضات؛ رویه‌های قضایی منسجم؛ و مجازات‌های متناسب که هم بازدارندگی و هم اصلاح‌محوری را در نظر می‌گیرند. «لایه سوم» (زیرساخت اجرایی–حمایتی) شامل: نهادهای تخصصی پلیس سایبری؛ آزمایشگاه‌های جنایی دیجیتال؛ مراکز حمایت از قربانیان؛ و مکانیسم‌های فوری حذف محتوا (Bagherinejad, 2020).

ویژگی کلیدی این مدل سه‌لایه، «توالی پیاده‌سازی» (*Implementation Sequencing*) آن است. برخلاف رویکردهای رایج، که اغلب از لایه دوم، تقنین، آغاز می‌کنند، این مدل پیشنهاد می‌کند که برای کشورهایی مانند افغانستان که منابع محدود دارند، شروع از لایه اول، دینی–اجتماعی، به دلیل هزینه پایین و اثر سریع، منطقی‌تر است. این لایه می‌تواند زمینه اجتماعی لازم برای پذیرش لایه دوم، قوانین جدید، را فراهم کند. سپس، با تثبیت لایه دوم، لایه سوم، زیرساخت اجرایی، که پرهزینه‌ترین است، با حمایت اجتماعی و چارچوب قانونی محکم‌تری قابل توسعه خواهد بود. برای ایران، که قبلاً بخشی از لایه دوم و سوم را توسعه داده، تمرکز باید بر تکمیل و تقویت این لایه‌ها و فعال‌سازی بیشتر لایه اول باشد که نسبتاً مغفول مانده است. این رویکرد توالی‌محور، می‌تواند به برنامه‌ریزان سیاستی هر دو کشور کمک کند تا منابع محدود خود را به‌صورت بهینه تخصیص دهند.

در نهایت، باید تأکید کرد که این مدل سه‌لایه نه یک نسخه ثابت، بلکه یک «چارچوب راهنما» (*Heuristic Framework*) است که باید با شرایط خاص هر کشور، هر منطقه، و حتی هر گروه جمعیتی تطبیق یابد. سیاست جنایی مؤثر در نهایت محصول دیالوگ مستمر میان قانون‌گذاران، علما، متخصصان فناوری، جامعه مدنی، و مهم‌تر از همه خود شهروندانی است که قرار است از این سیاست‌ها بهره‌مند شوند. این پژوهش با ارائه این چارچوب، امیدوار است گامی در جهت این دیالوگ سازنده در ایران، افغانستان، و فراتر از آن بردارد.

مالیه عمومی و تخصیص منابع در سیاست جنایی سایبری

یکی از ابعادی که در ادبیات سیاست جنایی سایبری کشورهای در حال توسعه کمتر مورد توجه قرار گرفته، «مالیه عمومی» (*Public Finance*) سیاست جنایی است. هر یک از سه مؤلفه سیاست جنایی یکپارچه، پیشگیرانه، کیفری، و حمایتی، هزینه‌های متفاوتی دارد و بازده متفاوتی نیز تولید می‌کند. تحلیل «هزینه–فایده» (*Cost-Benefit Analysis*) نشان می‌دهد که سرمایه‌گذاری در «مؤلفه پیشگیرانه»، به‌ویژه آموزش عمومی از طریق کانال‌های موجود مثل مدارس و مساجد، نسبت هزینه به فایده بسیار مطلوب‌تری نسبت به گسترش زندان‌ها یا

استخدام نیروهای پلیس اضافی دارد. این یافته، که در ادبیات بین‌المللی پیشگیری از جرم، مثلاً گزارش‌های بانک جهانی درباره «هزینه جرم»، به‌طور مکرر تأیید شده، برای کشورهایی با منابع محدود مثل افغانستان اهمیت ویژه‌ای دارد (Mohseni, 2019).

برای ایران، که قبلاً سرمایه‌گذاری قابل توجهی در «مؤلفه کیفری»، پلیس فتا، دادگاه‌های ویژه، انجام داده، تحلیل هزینه–فایده پیشنهاد می‌کند که بازده نهایی (*Marginal Return*) سرمایه‌گذاری بیشتر در این مؤلفه رو به کاهش است؛ در حالی که سرمایه‌گذاری در «مؤلفه‌های پیشگیرانه و حمایتی»، که کمتر توسعه یافته‌اند، بازده نهایی بالاتری خواهد داشت. این یک اصل کلی در اقتصاد سیاست عمومی است: «قانون بازده نزولی» (*Law of Diminishing Returns*) ایجاب می‌کند که منابع به سمت حوزه‌هایی هدایت شوند که کمترین سرمایه‌گذاری قبلی را داشته‌اند. کاربرد این اصل در سیاست جنایی سایبری ایران، توصیه روشنی ارائه می‌دهد: اولویت بودجه‌ای آینده باید به سمت برنامه‌های آموزشی ملی، توسعه خدمات حمایت از قربانیان، و کمپین‌های فرهنگی هدایت شود، نه صرفاً گسترش بیشتر ظرفیت کیفری موجود.

برای افغانستان، که با محدودیت شدید منابع روبه‌روست، اصل «اصلاحات کم‌هزینه–پراثر» (*Low-Cost High-Impact Reforms*)، که در ادبیات توسعه شناخته شده، باید راهنمای اصلی باشد. مثال‌های مشخص این نوع اصلاحات عبارتند از: صدور فتاوای رسمی توسط شورای علمای کشور درباره حریم خصوصی دیجیتال، هزینه: تقریباً صفر، اثر: بالقوه گسترده؛ گنجاندن یک واحد درسی کوتاه درباره اخلاق دیجیتال در برنامه درسی موجود مدارس، هزینه: کم، اثر: درازمدت؛ و استفاده از داوطلبان آموزش‌دیده برای ارائه کارگاه‌های آگاهی‌بخشی در جوامع محلی، هزینه: کم، اثر: مستقیم. این اصلاحات، که نیازمند سرمایه‌گذاری زیرساختی سنگین نیستند، می‌توانند در کوتاه‌مدت تفاوت قابل توجهی ایجاد کنند و زمینه را برای اصلاحات پرهزینه‌تر در آینده فراهم آورند (Farahmand, 2021).

بحث و نتیجه‌گیری

این پژوهش با طرح سؤال «سیاست جنایی ایران و افغانستان در مقابله با جرایم علیه حریم خصوصی سایبری چه میزان کارآمدی دارد؟» آغاز شد و از طریق یک چارچوب تحلیلی سه‌بُعدی، تقنینی–قضایی–اجرایی، و مدل سیاست جنایی یکپارچه، به ارزیابی نظام‌مند این کارآمدی پرداخت. نتیجه اصلی، که هیچ‌کدام از دو نظام به سطح کارآمدی قابل قبول نرسیده‌اند، نباید به‌عنوان یک حکم نومیدکننده تلقی شود، بلکه باید به‌عنوان نقطه شروعی برای یک مسیر اصلاحی روشن دیده شود. تفاوت میان وضعیت موجود و وضعیت مطلوب، در واقع «فضای اصلاح» (*Reform Space*) را مشخص می‌کند که هر دو کشور می‌توانند در آن حرکت کنند (Abbasi, 2020).

آنچه این پژوهش را از تحلیل‌های صرفاً انتقادی متمایز می‌سازد، تأکید آن بر «ظرفیت‌های مثبت» موجود در هر دو نظام است. پشتوانه فقهی–اسلامی مشترک، پیوندهای فرهنگی–زبانی دو کشور، تجربه نهادی ایران، و «شروع تازه» افغانستان، همگی دارایی‌هایی هستند که در طراحی سیاست جنایی آینده می‌توانند نقش محوری ایفا کنند. مدل «سیاست جنایی سه‌لایه اسلامی» که در این پژوهش ارائه شد، تلاشی است برای ترکیب این دارایی‌ها در یک چارچوب عملیاتی منسجم. این مدل، که از پایین، لایه دینی–اجتماعی، کم‌هزینه، به بالا، لایه اجرایی–حمایتی، پرهزینه، حرکت می‌کند، مسیری واقع‌بینانه برای کشورهایی با محدودیت منابع فراهم می‌کند.

در نهایت، این پژوهش بر این باور است که سیاست جنایی مؤثر در حوزه حریم خصوصی سایبری، نه‌تنها یک ضرورت حقوقی–فنی، بلکه یک تعهد اخلاقی–دینی است. در سنت اسلامی، حکومت موظف است از «حقوق العباد» (حقوق بندگان خدا) در برابر یکدیگر حمایت کند؛ و حریم خصوصی دیجیتال، در عصر حاضر، یکی از مصادیق روشن این حقوق است. ایران و افغانستان، با تکیه بر این مسئولیت دینی و با بهره‌گیری از دانش جرم‌شناسی و حقوق تطبیقی مدرن، می‌توانند الگویی از سیاست جنایی ارائه دهند که هم ریشه در هویت اسلامی–فرهنگی

آن‌ها دارد و هم پاسخگوی نیازهای شهروندان در عصر دیجیتال است. این پژوهش، با ارائه چارچوب‌ها، یافته‌ها، و پیشنهادات خود، امیدوار است سهمی هرچند کوچک در تحقق این آرمان داشته باشد.

این پژوهش با ارزیابی تطبیقی سیاست جنایی ایران و افغانستان در مقابله با جرایم علیه حریم خصوصی سایبری، به نتایج زیر دست یافت: نخست، هر دو کشور از کارآمدی قابل قبول در این حوزه برخوردار نیستند، هرچند ایران وضعیت نسبتاً بهتری دارد. دوم، «شکاف اجرا» در ایران برجسته‌ترین چالش است، در حالی که در افغانستان هم قانون و هم اجرا نیاز به توسعه دارند. سوم، رویکرد «پیشگیرانه» در هر دو کشور به‌شدت ضعیف است. چهارم، ظرفیت فقهی–اسلامی مشترک هر دو کشور به‌اندازه کافی مورد استفاده قرار نگرفته است. پنجم، «حمایت از قربانیان» به‌عنوان مؤلفه ضروری سیاست جنایی، در هر دو نظام نادیده گرفته شده است. این نتایج با پژوهش‌های مشابه درباره کشورهای در حال توسعه همخوانی دارند که نشان می‌دهند شکاف میان قانون مکتوب و اجرای واقعی، یکی از چالش‌های بنیادی سیاست جنایی در کشورهای این دسته است (Lappi-Seppälä, 2011; Unodc, 2013).

پیشنهادات این پژوهش در سه افق زمانی ارائه می‌شوند. در افق «کوتاه‌مدت» (یک تا دو سال): برای ایران، تدوین دستورالعمل‌های تفسیری دیوان عالی کشور برای یکنواختی رویه قضایی در جرایم سایبری؛ آغاز برنامه آموزش مستمر قضات و پلیس؛ و راه‌اندازی خط اورژانسی اختصاصی برای قربانیان جرایم سایبری ناموسی. برای افغانستان، تشکیل کارگروه تخصصی برای تهیه پیش‌نویس قانون جرایم سایبری؛ آموزش یک گروه هسته‌ای از متخصصین سایبری در نهادهای انتظامی؛ و بهره‌گیری از شبکه مساجد برای کمپین ملی آگاهی‌بخشی مبتنی بر ارزش‌های اسلامی. برای هر دو کشور، تأسیس «پلتفرم همکاری سایبری ایران–افغانستان» برای مقابله با جرایم فرامرزی (Farahmand, 2021).

در افق «میان‌مدت» (سه تا پنج سال): برای ایران، تصویب قانون جامع حفاظت از داده‌های شخصی با الهام از *GDPR* و تطبیق با ارزش‌های اسلامی؛ ایجاد «سازمان مستقل حفاظت از داده»؛ و توسعه «راهبرد ملی امنیت سایبری» که مؤلفه پیشگیری را در کانون قرار دهد. برای افغانستان، تصویب قانون مستقل جرایم سایبری؛ تأسیس «واحد تخصصی پلیس سایبری»؛ و توسعه برنامه آموزش سواد دیجیتال در مدارس. برای هر دو کشور، تدوین «اعلامیه اسلامی حقوق دیجیتال» که بر پایه ارزش‌های مشترک اسلامی استانداردهایی برای حریم خصوصی در فضای مجازی تعریف کند. در افق «بلندمدت» (بیش از پنج سال): هماهنگی قوانین سایبری دو کشور، ایجاد نهاد منطقه‌ای همکاری سایبری در چارچوب سازمان همکاری اسلامی، و توسعه جرم‌شناسی سایبری اسلامی به‌عنوان رشته‌ای دانشگاهی در هر دو کشور.

تعارض منافع

در انجام مطالعه حاضر، هیچ‌گونه تضاد منافعی وجود ندارد.

مشارکت نویسندگان

در نگارش این مقاله تمامی نویسندگان نقش یکسانی ایفا کردند.

حامی مالی

این پژوهش حامی مالی نداشته است.

EXTENDED SUMMARY

Criminal policy toward crimes against cyber privacy has become one of the most urgent issues in contemporary legal systems, particularly in societies where rapid digitalization has outpaced the capacity of criminal law, judicial institutions, and enforcement agencies. Criminal policy, in its modern sense, refers not merely to penal reaction but to the totality of legislative, judicial, executive, preventive, and supportive measures through which society responds to criminal phenomena

(Delmas-Marty, 1986). In the digital environment, this concept acquires a more complex meaning because violations of privacy are no longer limited to physical intrusion or direct disclosure, but include unauthorized access to personal data, non-consensual publication of private images, digital sexual extortion, identity theft, cyberstalking, and surveillance through networked technologies (Clough, 2015; Wall, 2007). Theoretical literature on privacy shows that privacy is not a single, fixed interest, but a multidimensional legal and social value related to autonomy, dignity, informational control, contextual integrity, and protection against misuse of personal information (Nissenbaum, 2010; Solove, 2008). Therefore, crimes against cyber privacy require a criminal policy that can respond to technological speed, anonymity, transnationality, and the continuing harm caused by digital dissemination. In Iran and Afghanistan, this issue is even more significant because both legal systems are influenced by Islamic jurisprudential foundations, social expectations concerning honor and dignity, and the need to harmonize domestic criminal law with international standards of cybercrime control and privacy protection (Bagherinejad, 2020; Kariminia, 2019).

This study aims to conduct a comparative evaluation of the effectiveness of the criminal policies of Iran and Afghanistan in combating crimes against cyber privacy. The central research problem is whether the existing criminal policy frameworks of these two countries are capable of providing coherent legislative protection, predictable judicial response, effective enforcement, preventive mechanisms, and adequate support for victims. The study is grounded in the assumption that effectiveness cannot be assessed merely by the existence of criminal statutes; rather, an effective criminal policy must be legally clear, institutionally enforceable, socially legitimate, proportionate, preventive, and compatible with the values of the target society (Bentham, 1789; Lappi-Seppälä, 2011). From a comparative-law perspective, Iran and Afghanistan provide a meaningful field of analysis because they share religious, cultural, linguistic, and historical affinities, while differing significantly in legislative development, institutional capacity, judicial specialization, and cyber-enforcement infrastructure. Iran has a relatively more developed legal framework for computer crimes and has established specialized enforcement mechanisms, yet its system continues to face problems of legislative dispersion, interpretive ambiguity, and implementation gaps (Alizadeh, 2018; Farahmand, 2021). Afghanistan, by contrast, remains at an earlier stage of building cyber-criminal policy infrastructure, with more limited statutory coverage, weaker technical capacity, and insufficient institutional specialization (Salehi, 2022). This comparison allows the study to identify both common deficiencies and country-specific reform priorities.

Methodologically, the research adopts a descriptive-analytical design with a comparative approach. The evaluation is organized around a three-dimensional framework of criminal policy: legislative criminal policy, judicial criminal policy, and executive criminal policy. The legislative dimension examines the completeness of criminalization, definitional precision, coherence of legal provisions, proportionality of punishments, and compatibility with international cybercrime and privacy standards (Rezaeipour, 2021; Unodc, 2013). The judicial dimension assesses how courts interpret and apply cybercrime provisions, how digital evidence is handled, whether judicial practice is predictable, and whether victims can obtain timely and meaningful remedies. The executive dimension evaluates the capacity of enforcement institutions, including cyber-police structures, technical investigation tools, reporting mechanisms, public awareness programs, and victim-support services (Hosseini, 2021; Mohseni, 2019). The study also incorporates an integrated criminal policy model, according to which punitive response must be coordinated with prevention, education, social support, technological regulation, and rehabilitation. This model is especially important in the field of cyber privacy because criminal prosecution after harm has occurred is often insufficient; once

private images, personal data, or defamatory materials are disseminated online, the damage may continue indefinitely. Therefore, preventive education, early reporting channels, rapid content-removal mechanisms, and psychological and legal support for victims are essential components of effectiveness (Mousavi, 2020; Saberi, 2019).

The findings indicate that Iran's criminal policy toward cyber privacy is relatively more developed than Afghanistan's, particularly in the legislative and executive dimensions, but it still falls short of an acceptable level of effectiveness. Iran's Computer Crimes Law and related provisions in criminal and procedural legislation have created a basic framework for prosecuting unauthorized access, data interference, disclosure of private information, and certain forms of digital privacy violation (Abbasi, 2020). However, the Iranian system suffers from legislative fragmentation, as privacy-related provisions are dispersed across different statutes, including computer crime legislation, penal provisions, electronic commerce regulations, and procedural rules. This dispersion weakens legal certainty and may reduce the perceived certainty of punishment, which is a core condition of deterrence theory (Bentham, 1789). Moreover, key concepts such as personal data, informed consent, digital sexual extortion, deepfake-based privacy violation, and platform responsibility are not defined with sufficient precision. Judicially, Iranian courts face problems in interpreting technical concepts and evaluating digital evidence, especially where metadata, server logs, IP addresses, cross-platform dissemination, or foreign-hosted platforms are involved (Farahmand, 2021). At the executive level, the existence of cyber-police capacity is an important advantage, yet the gap between the volume of cyber complaints and actual investigative capacity remains significant. In addition, victim-support mechanisms, emergency content-removal procedures, and preventive education remain less developed than punitive enforcement (Hosseini, 2021).

The findings concerning Afghanistan show a more foundational deficit. Afghanistan's criminal policy in the field of cyber privacy is still in the stage of institutional formation and lacks the level of legislative comprehensiveness required for an effective response to contemporary cyber harms (Salehi, 2022). The absence of detailed definitions of personal data, digital consent, online privacy violation, cyber extortion, and unauthorized digital dissemination limits the ability of courts and enforcement bodies to respond consistently. Judicially, Afghanistan faces serious structural challenges, including limited specialization among judges, weak codified jurisprudence in cybercrime cases, and the coexistence of formal judicial mechanisms with customary dispute-resolution structures. Although customary mechanisms such as jirgas may have social legitimacy in some communities, they may also create risks for victims, especially women, if not aligned with Islamic principles of dignity, protection from harm, and procedural fairness (Bagherinejad, 2020; Kariminia, 2019). At the executive level, Afghanistan lacks a sufficiently equipped cyber-police infrastructure, specialized forensic laboratories, trained investigators, and systematic public-reporting mechanisms. Nevertheless, the Afghan context also contains important potential capacities, including the social influence of mosques, religious schools, local councils, and community leaders. If properly oriented, these institutions can support public education about the religious prohibition of spying, disclosure of secrets, and violation of personal dignity. Thus, Afghanistan's reform pathway should prioritize low-cost, high-impact reforms, including religiously grounded awareness campaigns, basic cybercrime legislation, training of a core group of investigators and judges, and gradual establishment of specialized cyber-enforcement units (Clough, 2015; Unodc, 2013).

The comparative analysis demonstrates that neither Iran nor Afghanistan has yet achieved a fully effective criminal policy for combating crimes against cyber privacy. Iran's main problem is the gap

between law and implementation: it has a comparatively stronger legal and institutional foundation, but its preventive, supportive, and interpretive mechanisms remain insufficient. Afghanistan's main problem is more basic: both the legal framework and enforcement capacity require systematic development. In both countries, criminal policy remains overly punitive and insufficiently preventive; victims are not adequately supported; public education is fragmented; and the rich Islamic jurisprudential capacity for protecting privacy, dignity, and social trust has not been fully transformed into modern cyber-criminal policy. The study therefore proposes movement toward an integrated Islamic criminal policy model composed of three layers: a religious-social layer based on Islamic teachings concerning privacy, prohibition of spying, protection of dignity, and rejection of victim-blaming; a legislative-judicial layer based on precise cybercrime definitions, coherent statutes, trained judges, and predictable procedures; and an executive-supportive layer based on specialized cyber-police units, digital forensic capacity, rapid response mechanisms, victim services, and regional cooperation. Such a model can help both countries move beyond fragmented penal reaction and toward a balanced system that combines legality, prevention, enforcement, social legitimacy, and victim protection. For Iran, reform should focus on consolidating data-protection legislation, strengthening victim-support institutions, clarifying judicial guidelines, and expanding preventive programs. For Afghanistan, priority should be given to drafting independent cybercrime legislation, training specialized legal and enforcement personnel, using religious and community networks for awareness, and building gradual regional cooperation with countries that have more developed cyber-enforcement experience. In conclusion, effective protection of cyber privacy in Iran and Afghanistan is not only a technical or legal necessity, but also a moral and social obligation rooted in the protection of human dignity. A successful criminal policy in this field must combine modern criminological knowledge, comparative legal standards, Islamic jurisprudential legitimacy, and practical institutional capacity in order to protect citizens against emerging forms of digital harm.

References

Abbasi, M. J. (2020). *Cybercrimes and Privacy in Iranian Law*. Mizan Publications.

Alizadeh, A. (2018). *Iranian Criminal Policy toward Privacy Violations in Cyberspace*.

Bagherinejad, Z. (2020). A Jurisprudential Examination of Privacy in the Digital Age. *Quarterly Journal of Jurisprudence and Principles*, *53*(1), 1-30.

Bentham, J. (1789). *An Introduction to the Principles of Morals and Legislation*. Payne.

Clough, J. (2015). *Principles of Cybercrime* (2nd ed.). Cambridge University Press.

Delmas-Marty, M. (1986). *Le flou du droit*. PUF.

Farahmand, S. (2021). Challenges of Implementing the Computer Crimes Law in Iran. *Legal Critique Quarterly*, *4*(1), 55-78.

Hosseini, M. (2021). *Crimes against Privacy in Cyberspace*. Jangal Publications.

Kariminia, M. (2019). Jurisprudential Foundations of Privacy and Its Position in the Constitution of Iran. *Islamic Studies Quarterly*, *71*(1), 11-40.

Lappi-Seppälä, T. (2011). Explaining Imprisonment in Europe. *European Journal of Criminology*, *8*(4), 303-328.

Mohseni, F. (2019). *Cybersecurity and Criminal Law*. Mizan Publishing.

Mousavi, Z. (2020). Criminal Liability in Unauthorized Disclosure of Private Information on the Internet. *Journal of the Faculty of Law, University of Tehran*, *50*(2), 100-125.

Nissenbaum, H. (2010). *Privacy in Context*. Stanford University Press.

Rezaeipour, N. (2021). A Comparative Analysis of Iranian Computer Crime Laws and the Budapest Convention. *Judiciary Law Journal*, *85*(116), 23-54.

Saberi, F. (2019). Legal Analysis of Disclosure of Personal Information on Social Networks. *Criminal Law Research Quarterly*, *8*(2), 123-146.

Salehi, M. (2022). A Comparative Study of Criminal Protection of Privacy in Iranian and American Law. *Quarterly Journal of Criminal Law and Criminology*, *9*(1), 79-105.

Solove, D. J. (2008). *Understanding Privacy*. Harvard University Press.

Unodc. (2013). *Comprehensive Study on Cybercrime*.
Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Polity.
Zweigert, K., & Kötz, H. (1998). *Introduction to Comparative Law* (3rd ed.). Oxford University Press.