Comparative Studies in Jurisprudence, Law, and Politics

The Role of Custom in Discovering the Rationales of Rulings: With an Emphasis on the Views of Prominent Shiite Jurists from the 11th to 13th Century CE

1. Haider Abbas Mohammad Al Saleh: PhD Student, Department of Criminal Law and Criminology, Isfahan (Khorasgan) Branch, Islamic Azad University, Isfahan, Iran
2. Mahmood Ashrafy*: Assistant Professor, Department of Law, Isfahan (Khorasgan) Branch, Islamic Azad University, Isfahan, Iran. Email: mahmood.ashrafy2000@gmail.com (Corresponding Author)
3. Mohammad Jabbar Jadoo Al- Abdali: Assistant Professor, Department of Law, University of Kufa, Kufa, Iraq
4. Masoud Heydari: Associate Professor, Department of Law, Isfahan (Khorasgan) Branch, Islamic Azad University, Isfahan, Iran

ABSTRACT

Shiite jurisprudence has long been efficient, dynamic, and responsive to societal issues and needs. This adaptability has enabled it to guide the Shiite community during various historical periods, such as times of marginalization or governance, while maintaining adherence to its jurisprudential principles. Among various factors, custom (*ʿurf*) is perhaps fundamental in this context. This study aims to address the question of how, from the perspective of Shiite jurists from the 11th to 13th century CE, custom has played a role in discovering the rationales (*milākāt*) of rulings. By relying on library resources and a descriptive-analytical method, the study seeks to explore this topic in a historical context. It will elucidate the views of jurists of this era, examine scholarly evolutions, and chart the fluctuations in related jurisprudential discussions. Furthermore, it seeks to identify opportunities and challenges in this domain. Key topics include the conditions for the realization of custom, the dynamics of customary transformations, the discovery of rationales of rulings through custom, the interrelation between the validity of custom and rational judgment, and the perspectives of prominent jurists such as Sheikh Mufid, Sayyid Murtada, Ibn Idris, Ibn Zuhra, Muhaqqiq al-Hilli, and Sayyid Ibn Tawus. The findings of this research indicate that the validity of custom extends beyond mere endorsement or proof of the absence of rejection. Certain jurists have regarded custom, along with the practices of rational individuals (*binaʾ al-ʿuqalāʾ*) or their collective conduct (*sirat al-ʿuqalāʾ*), as having equivalent significance. Moreover, some jurists have considered the validity of custom as intrinsic, equating it with rationality. In this context, custom can function as a source for discovering the rationales of rulings, much like reason.

How to cite: Al Saleh, H. A. M., Ashrafy, M., Al-Abdali, M. J. J., & Heydari, M. (2025). The Role of Custom in Discovering the Rationales of Rulings: With an Emphasis on the Views of Prominent Shiite Jurists from the 11th to 13th Century CE. *Comparative Studies in Jurisprudence, Law, and Politics*, *7*(2), 1-15.

Submit Date: 08 December 2024
Revise Date: 20 December 2024
Accept Date: 31 December 2024
Publish Date: 02 July 2025

Keywords: *Custom, role of custom, rationales of rulings, Shiite jurisprudence, practices of rational individuals*.

پژوهش‌های تطبیقی فقه، حقوق و سیاست

بررسی تطبیقی جرایم سایبری در حقوق و سیاست ایران وعراق

۱. حیدر عباس محمد الصالح: دانشجوی دکتری حقوق جزا و جرم شناسی، واحد اصفهان (خوراسگان)، دانشگاه آزاد اسلامی، اصفهان، ایران
۲. محمود اشرافی مهابادی*: استادیار گروه حقوق، واحد اصفهان (خوراسگان)، دانشگاه آزاد اسلامی، اصفهان، ایران. پست الکترونیک: mahmood.ashrafy2000@gmail.com (نویسنده مسئول)
۳. محمد جبار جدوع العبدلی: استادیار گروه حقوق، دانشگاه کوفه، کوفه، عراق
۴. مسعود حیدری: دانشیار گروه حقوق، واحد اصفهان (خوراسگان)، دانشگاه آزاد اسلامی، اصفهان، ایران

چکیده

معیارهای فقهی شورای نگهبان در تطبیق و اعلام عدم مغایرت قوانین با موازین اسلامی موضوع اصول ۴ و۹۴ قانون اساسی ایران موضوعی است که در این مقاله مورد بررسی قرار گرفته است. این تحقیق از نظر هدف کاربردی و با روش توصیفی- تحلیلی انجام شده است. به تبعیت از نظم کلنی در نظام حقوقی ایران تقدم قانون اساسی و شرع بر قوانین عادی مورد پذیرش قرار گرفته است که معیار فقهی مشخصی برای تطبیق و اعلام عدم مغایرت قوانین عادی با شرع پیش‌بینی نشده است و از این رو مجادلات و اختلاف نظرهای زیادی در این حوزه وجود دارد. نظریه غالب آن است که ارتباط منابع با مبانی در بسیاری از موارد رعایت نشده و شورای‌نگهبان به موضوعاتی در رد قوانین مجلس استناد نموده که یا مبانی شرعی نداشته یا اساساً با شرع ارتباطی نداشته است. گذشته از تفاوت دیدگاهی که در مسأله نظارت شورای نگهبان مطابق اصل چهارم قانون اساسی بر قوانین و مقررات سابق وجود دارد، به نظر می‌رسد این نظارت به طور تام و بدون دخالت مجلس نمی‌تواند انجام گیرد، اما قانون اساسی تمهیداتی را برای تشریفات این امر در نظر نگرفته است. اتخاذ نظر و بیان تمهیدات قانونی در این زمینه امری لازم و ضروری پیش‌بینی می‌شود. این در حالی است که در بسیاری از موارد که فقهای شورای نگهبان رأی به مغایرت چنین قوانینی داده‌اند، در برهه‌های زمانی متفاوت همان قوانین در قالب و شکل دیگری به تأیید شورا رسیده است.

واژگان کلیدی: شورای نگهبان، قوانین اسلامی، مغایرت، قانون اساسی، معیارهای فقهی.

نحوه استناددهی: عباس محمد الصالح، حیدر.، اشرافی مهابادی، محمود.، جبار جدوع العبدلی، محمد.، و حیدری، مسعود. (۱۴۰۴). بررسی تطبیقی جرایم سایبری در حقوق و سیاست ایران وعراق. *پژوهش‌های تطبیقی فقه، حقوق و سیاست*، *۷*(۲)، ۱۵-۱.

تاریخ ارسال: ۱۸ آذر ۱۴۰۳
تاریخ بازنگری: ۲۱ خرداد ۱۴۰۴
تاریخ پذیرش: ۳۰ آذر ۱۴۰۳
تاریخ چاپ: ۱۰ دی ۱۴۰۳

مقدمه

در دنیای امروز، پیشرفت‌های فناورانه نقش مهمی در ایجاد فرصت‌های اقتصادی، ارتباطات جهانی و توسعه زیرساخت‌ها ایفا کرده است. اما همزمان، این فناوری‌ها زمینه‌ساز گسترش جرایم سایبری شده‌اند. با رشد شبکه‌های ارتباطی و افزایش وابستگی به فضای مجازی، تهدیدات سایبری به یکی از بزرگ‌ترین چالش‌های امنیتی برای دولت‌ها تبدیل شده است (Ali & Ahmmad, 2023). این تهدیدات تنها به جرایم مالی محدود نمی‌شوند، بلکه حریم خصوصی، اطلاعات حساس و حتی زیرساخت‌های حیاتی کشورها را نیز در معرض خطر قرار می‌دهند. این شرایط، نیازمند بررسی تطبیقی سیاست‌ها و قوانین کشورها در مقابله با این جرایم است.

ایران و عراق به عنوان دو کشور هم‌مرز با زیرساخت‌های فناوری در حال توسعه، با چالش‌های جدی در زمینه جرایم سایبری مواجه هستند. ایران با اجرای قانون جرایم رایانه‌ای و تأسیس پلیس فتا، گام‌هایی مؤثر در مقابله با این تهدیدات برداشته است (مرکز پژوهش‌های مجلس، ۱۳۹۹). از سوی دیگر، عراق به دلیل عدم استقرار کامل زیرساخت‌های حقوقی و ضعف در توانمندی‌های سایبری، بیشتر در برابر حملات سایبری آسیب‌پذیر است (Bayancenter, 2022). این تفاوت‌ها نشان‌دهنده ضرورت تحلیل تطبیقی برای ارائه راهکارهای بهینه در سیاست‌گذاری این کشورها است.

جرایم سایبری فراتر از مرزهای ملی عمل می‌کنند و امنیت بین‌المللی را به چالش می‌کشند. حملات سایبری به زیرساخت‌های حیاتی مانند نیروگاه‌ها، سیستم‌های بانکی و بیمارستان‌ها، نمونه‌هایی از این تهدیدات هستند که به طور مستقیم امنیت ملی کشورها را تحت تأثیر قرار می‌دهند (Mokhtaripour, 2021). در این میان، ایران با بهره‌گیری از توانمندی‌های بومی در حوزه سایبری، سعی در کاهش تهدیدات دارد، اما همچنان نیازمند تعامل و همکاری بین‌المللی است. مطالعه تطبیقی قوانین و سیاست‌های سایبری ایران و عراق می‌تواند به درک بهتر این چالش‌ها کمک کند.

جرایم سایبری اغلب فراملی هستند و حل آن‌ها نیازمند همکاری منطقه‌ای و جهانی است. ایران و عراق به عنوان اعضای جامعه بین‌المللی، نیازمند هماهنگی با یکدیگر و سایر کشورها در زمینه مقابله با این جرایم هستند (Katman, 2021). همکاری‌های مشترک می‌تواند به تبادل دانش، بهبود ظرفیت‌های فنی و تقویت قوانین بینجامد. این موضوع به ویژه در زمینه‌هایی نظیر جرایم مرتبط با پول‌شویی، تروریسم سایبری و نقض حقوق دیجیتال اهمیت بیشتری پیدا می‌کند.

مطالعه تطبیقی قوانین سایبری ایران و عراق امکان شناسایی نقاط قوت و ضعف در سیاست‌گذاری هر کشور را فراهم می‌آورد. این تحلیل نه تنها به بهبود چارچوب‌های حقوقی در سطح ملی کمک می‌کند، بلکه می‌تواند به ارائه راهکارهایی برای مقابله با تهدیدات مشترک منطقه‌ای منجر شود. بررسی تجارب این دو کشور نشان می‌دهد که با وجود تفاوت‌ها، شباهت‌هایی نظیر نیاز به تقویت زیرساخت‌های سایبری و هماهنگی بین‌المللی وجود دارد که می‌تواند زمینه‌ساز تعاملات سازنده باشد (Eslami & Danesh, 2023).

هدف اصلی این پژوهش بررسی و شناسایی نقاط اشتراک و اختلاف میان قوانین سایبری ایران و عراق است. با توجه به موقعیت جغرافیایی، اشتراکات فرهنگی و روابط اقتصادی میان این دو کشور، تحلیل تطبیقی نظام حقوقی آن‌ها در حوزه جرایم سایبری می‌تواند به ارائه راهکارهای مؤثر برای مقابله با چالش‌های مشترک و ارتقاء سیاست‌گذاری کمک کند. این پژوهش همچنین در پی پیشنهاد اصلاحات و بهبودهایی برای چارچوب‌های حقوقی و اجرایی هر دو کشور است تا بتوانند پاسخگوی تهدیدات پیچیده سایبری در عصر حاضر باشند. لذا این پژوهش در پی رسیدن به پاسخ سؤالات زیر است:

۱. نظام حقوقی ایران و عراق چگونه با جرایم سایبری برخورد می‌کنند؟

۲. چه شباهت‌ها و تفاوت‌هایی میان سیاست‌گذاری دو کشور وجود دارد؟

پیشینه پژوهش

توسعه حقوق سایبری در ایران: ایران به عنوان یکی از کشورهای پیشرو در منطقه، تلاش‌های زیادی برای تنظیم و تدوین قوانین مرتبط با جرایم سایبری انجام داده است. قانون جرایم رایانه‌ای ایران که در سال ۱۳۸۸ تصویب شد، به عنوان چارچوب اصلی مبارزه با جرایم سایبری شناخته می‌شود. این قانون موضوعاتی مانند دسترسی غیرمجاز، جعل داده‌های رایانه‌ای و کلاهبرداری سایبری را پوشش می‌دهد. با این حال، مطالعات نشان می‌دهند که این قانون در زمینه‌های جدیدتر، از جمله حفاظت از داده‌های شخصی و امنیت سایبری در برابر تهدیدات فراملی، کاستی‌هایی دارد. محققانی مانند زرنشان و همکاران (۲۰۲۲) بر ضرورت عضویت ایران در کنوانسیون بوداپست تأکید کرده‌اند، زیرا این کنوانسیون می‌تواند ابزارهای اجرایی بین‌المللی و حمایت‌های قانونی بیشتری را فراهم آورد (Zarneshan et al., 2022).

چالش‌های حقوق سایبری در عراق: عراق به دلیل بحران‌های سیاسی و امنیتی چند دهه اخیر، در توسعه چارچوب حقوقی مرتبط با جرایم سایبری با چالش‌های جدی مواجه بوده است. قوانین سایبری عراق در مقایسه با ایران بسیار پراکنده و ناکافی هستند. به گفته عبدالامیر و همکاران (۲۰۲۲)، مهم‌ترین موانع اجرای قوانین سایبری در عراق عبارتند از ضعف زیرساخت‌های قانونی، کمبود نیروی انسانی متخصص و عدم هماهنگی میان نهادهای مجری قانون. این کشور همچنین فاقد یک قانون جامع برای مقابله با تهدیدات سایبری است، که این موضوع اجرای سیاست‌های کیفری مؤثر را دشوار کرده است. پژوهش‌ها نشان می‌دهند که عراق نیازمند همکاری‌های بین‌المللی برای تدوین و اجرای قوانین جامع‌تر است (AbdulAmeer et al., 2022).

مقایسه سیاست‌های کیفری ایران و عراق در حوزه جرایم سایبری: مقایسه سیاست‌های کیفری ایران و عراق نشان‌دهنده تفاوت‌های قابل توجه در رویکردهای این دو کشور است. ایران توانسته است با تصویب قوانین جامعی نظیر قانون جرایم رایانه‌ای و ایجاد واحدهای تخصصی در پلیس فتا، به طور قابل ملاحظه‌ای از جرایم سایبری جلوگیری کند. در مقابل، عراق به دلیل نبود قوانین جامع، با مشکلات جدی در پیشگیری و پیگیری جرایم سایبری مواجه است (Rahimi & Shaygan-Fard, 2023). علاوه بر این، ایران با وجود برخی ضعف‌ها، در سیاست‌گذاری برای حفاظت از داده‌های شخصی پیشرفت کرده است، اما عراق هنوز در این حوزه در مراحل اولیه قرار دارد.

همکاری‌های بین‌المللی در مقابله با جرایم سایبری: همکاری‌های بین‌المللی در مبارزه با جرایم سایبری از اهمیت بالایی برخوردار است. ایران به دلیل عدم عضویت در کنوانسیون بوداپست، از ابزارهای همکاری بین‌المللی محروم مانده است. این موضوع مانع از توانایی ایران در پیگرد مجرمان سایبری در سطح جهانی شده است (Rahimi & Shaygan-Fard, 2023). در مقابل، عراق به دلیل مشکلات داخلی و عدم توجه کافی به قوانین بین‌المللی مرتبط، نتوانسته از این ابزارها بهره‌مند شود. پژوهش‌ها تأکید دارند که عضویت در کنوانسیون‌های بین‌المللی و ایجاد ساختارهای همکاری منطقه‌ای می‌تواند توانایی هر دو کشور را در مقابله با تهدیدات سایبری افزایش دهد.

تحلیل تطبیقی جرم‌انگاری در قوانین سایبری: یران و عراق در جرم‌انگاری جرایم سایبری، مانند کلاهبرداری سایبری و دسترسی غیرمجاز، رویکردهای متفاوتی دارند. در حالی که قانون جرایم رایانه‌ای ایران این جرایم را به صورت جامع تعریف کرده است، عراق فاقد تعاریف قانونی مشخص برای بسیاری از این موارد است (Amiri-Moghadam & Zarei, 2022). این موضوع باعث شده است که عراق در

پیگرد قانونی مجرمان با مشکلات بیشتری مواجه شود. ایران نیز اگرچه از قوانین جامع‌تری برخوردار است، اما به دلیل ضعف در زیرساخت‌های فنی و نیروی انسانی متخصص، در برخی موارد مانند پیگیری هویت مجرمان سایبری با چالش‌هایی روبرو است.

نیاز به اصلاحات در سیاست‌های سایبری ایران و عراق: هر دو کشور ایران و عراق نیازمند اصلاحات اساسی در سیاست‌های سایبری خود هستند. در ایران، بهبود زیرساخت‌های فنی و تقویت همکاری‌های بین‌المللی از جمله مهم‌ترین پیشنهادات محققان است (Shahbazi, 2019). عراق نیز باید با ایجاد قوانین جامع و شفاف، توسعه زیرساخت‌های امنیتی و افزایش توان اجرایی نهادهای قانونی، گام‌های جدی در این زمینه بردارد. همچنین آموزش عمومی و افزایش آگاهی جامعه در خصوص جرایم سایبری می‌تواند به کاهش این تهدیدات کمک کند.

این تحلیل‌ها نشان می‌دهند که توسعه قوانین سایبری و سیاست‌های کیفری جامع در ایران و عراق از اهمیت ویژه‌ای برخوردار است و نیازمند توجه و همکاری‌های داخلی و بین‌المللی است.

جایگاه پژوهش حاضر در میان تحقیقات موجود :پژوهش حاضر، با تمرکز بر تحلیل تطبیقی جرایم سایبری در حقوق و سیاست ایران و عراق، گامی مؤثر در پر کردن شکاف مطالعاتی موجود در ادبیات حقوقی و سیاست‌گذاری سایبری است. با توجه به بررسی‌های پیشین، اگرچه مطالعات متعددی به ابعاد مختلف جرایم سایبری در ایران پرداخته‌اند (Shahbazi, 2019; Shahbazi & Shabani-Kolahi, 2024; Zarneshan et al., 2022) اما رویکرد تطبیقی با کشورهای منطقه، به‌ویژه عراق، کمتر مورد توجه قرار گرفته است. عراق به‌عنوان کشوری با ساختارهای حقوقی و امنیتی متفاوت و چالش‌های متمایز، بستری جذاب برای بررسی تطبیقی است. پژوهش‌های قبلی اغلب بر تحلیل قوانین داخلی ایران یا تطبیق این قوانین با استانداردهای بین‌المللی متمرکز بوده‌اند (Asgari et al., 2020; Rahimi & Shaygan-Fard, 2023). در مقابل، این مطالعه تلاش می‌کند با بررسی هم‌زمان دو کشور، الگوهای سیاست‌گذاری و ظرفیت‌های قانونی را برای مقابله با جرایم سایبری در محیطی منطقه‌ای مورد ارزیابی قرار دهد و از این منظر به دانش موجود افزوده و بسترهای بهبود قوانین را پیشنهاد دهد.

این پژوهش علاوه بر پرداختن به جنبه‌های قانونی و کیفری جرایم سایبری، ابعاد سیاست‌گذاری سایبری، به‌ویژه در زمینه حریم خصوصی، حفاظت از داده‌ها، و همکاری‌های بین‌المللی را نیز مورد بررسی قرار می‌دهد (Eslami & Danesh, 2023; Majidi, 2021). این ترکیب میان تحلیل‌های حقوقی و سیاست‌گذاری، جایگاه پژوهش را در میان مطالعات مشابه منحصر به فرد می‌سازد. همچنین، نتایج این تحقیق می‌تواند ابزار ارزشمندی برای سیاست‌گذاران و قانون‌گذاران در هر دو کشور باشد تا ضعف‌های موجود را شناسایی و رفع کنند. پژوهش حاضر نه‌تنها محدود به تحلیل و مقایسه نیست، بلکه پیشنهادات عملی برای بهبود سیستم‌های حقوقی و سیاست‌گذاری ایران و عراق ارائه می‌دهد که می‌تواند به ایجاد یک چارچوب قانونی مشترک و ارتقای همکاری‌های منطقه‌ای در مقابله با تهدیدات سایبری منجر شود.

چارچوب نظری

نظریات حقوق کیفری مرتبط با جرایم سایبری

نظریه‌های حقوق کیفری از جمله بازدارندگی، عدالت ترمیمی، و نظریه بازپروری در تحلیل جرایم سایبری مورد استفاده قرار می‌گیرند. نظریه بازدارندگی بر تدوین قوانین سخت‌گیرانه با هدف جلوگیری از وقوع جرم تأکید دارد و در ایران به‌ویژه در قانون جرایم رایانه‌ای این رویکرد مشهود است (قانون جرایم رایانه‌ای، ۱۳۸۸). نظریه عدالت ترمیمی، به‌جای مجازات صرف، به جبران خسارات وارده به قربانیان جرایم سایبری تأکید دارد که این مفهوم در کشورهای منطقه کمتر توسعه یافته است (Kshetri, 2005). از سوی دیگر، نظریه بازپروری نیز بر اصلاح رفتار مجرمان سایبری از طریق برنامه‌های آموزشی و بازپروری تمرکز دارد.

مفهوم جرایم سایبری

جرایم سایبری به تخلفات کیفری صورت‌گرفته در فضای مجازی گفته می‌شود که شامل کلاهبرداری دیجیتال، سرقت اطلاعات، و تخریب زیرساخت‌های الکترونیکی است (Gharaibeh & Al-Senussi, 2023). در ایران، این مفهوم در قانون جرایم رایانه‌ای به‌صورت جامع تعریف شده و جنبه‌های متعددی از جمله نقض حریم خصوصی و سرقت اطلاعات را در بر می‌گیرد (قانون جرایم رایانه‌ای، ۱۳۸۸). در عراق، با توجه به محدودیت‌های حقوقی و سیاسی، این تعریف کمتر شامل جنبه‌های دقیق حقوقی است و بیشتر بر موضوعات امنیت ملی تمرکز دارد (AbdulAmeer et al., 2022).

سیاست‌گذاری سایبری و امنیت دیجیتال

سیاست‌گذاری سایبری شامل تدوین استراتژی‌ها و چارچوب‌های حقوقی برای مدیریت جرایم سایبری و حفاظت از فضای دیجیتال است. ایران با تصویب راهبردهای ملی امنیت سایبری و قوانین جامع تلاش کرده است تا ساختار حقوقی خود را در برابر تهدیدات سایبری تقویت کند (Suleiman et al., 2023; Tarrad et al., 2022). در عراق، به دلیل فقدان سیستم منسجم، سیاست‌های سایبری بیشتر به اقدامات واکنشی محدود شده‌اند (Nehme, 2023). این تفاوت‌ها نشان‌دهنده سطح مختلف توسعه‌یافتگی سیاست‌گذاری سایبری در این دو کشور است.

حقوق تطبیقی و جایگاه آن در مطالعه جرایم سایبری

حقوق تطبیقی ابزار مهمی برای تحلیل تطابقات و تفاوت‌های نظام‌های حقوقی است. مطالعه تطبیقی قوانین ایران و عراق در زمینه جرایم سایبری نشان می‌دهد که ایران قوانین کامل‌تری برای جرایم سایبری تدوین کرده است (قانون جرایم رایانه‌ای، ۱۳۸۸). در عراق، این قوانین هنوز به سطح اجرایی کافی نرسیده و نیاز به پژوهش بیشتر برای شناسایی بهترین شیوه‌ها وجود دارد (Ali & Ahmmad, 2023). استفاده از حقوق تطبیقی می‌تواند به بهبود سیاست‌های حقوقی در منطقه کمک کند.

نظریه‌های اجتماعی مرتبط با جرایم سایبری

نظریات اجتماعی مانند نظریه کنترل اجتماعی و نظریه فشار اجتماعی به تحلیل رفتارهای مجرمانه در فضای سایبری کمک می‌کنند. نظریه کنترل اجتماعی توضیح می‌دهد که فقدان نظارت و قوانین محکم می‌تواند موجب افزایش رفتارهای مجرمانه در فضای مجازی شود (Afshari, 2019). این موضوع در ایران با اجرای سخت‌گیرانه‌تر قوانین سایبری تا حدودی کنترل شده است (قانون جرایم رایانه‌ای، ۱۳۸۸)، اما عراق به دلیل ضعف قوانین و ساختارهای نظارتی همچنان با چالش‌هایی روبه‌رو است.

ارتباط بین فرهنگ سایبری و جرایم دیجیتال

فرهنگ سایبری به تعاملات اجتماعی و رفتارهای کاربران در فضای مجازی اشاره دارد. در ایران، سیاست‌های فرهنگی سایبری با هدف ارتقای آگاهی کاربران و کاهش رفتارهای مجرمانه تنظیم شده است (Eslami & Danesh, 2023). در عراق، ضعف زیرساخت‌های آموزشی و نبود برنامه‌های فرهنگی سایبری موجب گسترش جرایم سایبری شده است (Nehme, 2023). این جنبه‌ها نشان می‌دهند که فرهنگ سایبری می‌تواند نقش مهمی در پیشگیری از جرایم داشته باشد.

نظریات سایبری در تحلیل جرایم دیجیتال

نظریات سایبری شامل تحلیل الگوهای رفتاری در فضای مجازی و روش‌های مقابله با جرایم دیجیتال می‌شود. نظریه اکوسیستم سایبری، که بر تعامل میان کاربران، فناوری، و سیاست‌گذاری تمرکز دارد، یکی از رویکردهای مهم در این زمینه است (Gharaibeh & Al-Senussi, 2023). ایران با ایجاد ساختارهایی مانند پلیس فضای تولید و تبادل اطلاعات (فتا) تلاش کرده است تا از این نظریه در سیاست‌گذاری استفاده کند (قانون جرایم رایانه‌ای، ۱۳۸۸). عراق نیز باید با بهره‌گیری از این نظریات، ساختارهای حقوقی و اجرایی خود را تقویت کند.

روش‌شناسی

این پژوهش از نوع تطبیقی-تحلیلی است که به بررسی شباهت‌ها و تفاوت‌های حقوقی میان دو نظام حقوقی ایران و عراق در زمینه جرایم سایبری می‌پردازد. این روش با هدف شناسایی نقاط قوت و ضعف قوانین سایبری و ارائه پیشنهادات بهبود طراحی شده است.

تحلیل تطبیقی قوانین سایبری در ایران و عراق

قانون جرایم رایانه‌ای ایران، تصویب شده در سال ۱۳۸۸، یکی از مهم‌ترین قوانین در زمینه مقابله با جرایم سایبری است. این قانون با هدف ایجاد شفافیت و کارآمدی در مواجهه با تخلفات سایبری تدوین شد. این قانون در پنج فصل، شامل جرایم علیه امنیت ملی، جرایم مالی، نقض حریم خصوصی، و سایر موارد، چارچوب قانونی جامعی برای مقابله با جرایم در فضای دیجیتال ارائه می‌دهد. یکی از نقاط قوت این قانون، تمرکز بر جنبه‌های پیشگیری و همچنین مجازات دقیق برای انواع تخلفات سایبری است (Golkhandan, 2024). با این حال، فقدان تطبیق کامل با تحولات سریع فناوری، چالش‌هایی را ایجاد کرده است.

یکی از نقاط تمرکز قانون جرایم رایانه‌ای، حفاظت از حریم خصوصی کاربران است. این قانون به‌طور ویژه به مواردی مانند دسترسی غیرمجاز به داده‌ها، سرقت اطلاعات شخصی، و انتشار غیرقانونی اطلاعات پرداخته است. در سال‌های اخیر، فشارهای بین‌المللی بر ایران برای تقویت حفاظت از داده‌ها افزایش یافته است، اما هنوز چالش‌هایی مانند عدم وجود قوانین جامع حفاظت از داده‌ها به چشم می‌خورد (Shahbazi & Shabani-Kolahi, 2024). به‌رغم این چالش‌ها، قوانین موجود نشان‌دهنده گام‌های اولیه مهمی در جهت حفاظت از حقوق دیجیتال کاربران است.

پلیس فضای تولید و تبادل اطلاعات (فتا) در ایران، بازوی اجرایی قوانین سایبری است که در سال ۱۳۹۰ تأسیس شد. این سازمان با هدف مقابله با جرایم رایانه‌ای، نظارت بر امنیت فضای مجازی، و ارائه خدمات پیشگیری و مشاوره‌ای فعالیت می‌کند. فتا موفق شده است در پرونده‌های متعددی، از جمله کلاهبرداری‌های آنلاین و نقض امنیت اطلاعات، به موفقیت دست یابد. با این حال، انتقاداتی از جمله ضعف در هماهنگی میان فتا و نهادهای قضایی و همچنین محدودیت‌های بودجه‌ای وجود دارد (Afshari, 2019).

ایران به عنوان یکی از اعضای کنوانسیون‌های بین‌المللی در حوزه جرایم سایبری مشارکتی نداشته است، اما قوانین داخلی آن تحت تأثیر استانداردهای جهانی تدوین شده‌اند. این موضوع باعث شده است که برخی از شکاف‌ها در قوانین داخلی، مانند نحوه برخورد با جرایم فرامرزی یا همکاری بین‌المللی، همچنان باقی بماند (Dehmardeh, 2020). تلاش‌هایی برای نزدیک‌تر کردن قوانین ایران به استانداردهای جهانی دیده می‌شود، اما محدودیت‌های سیاسی و اقتصادی مانع پیشرفت سریع در این زمینه است.

یکی از چالش‌های اساسی در اجرای قوانین جرایم رایانه‌ای، ضعف هماهنگی بین نهادهای قانون‌گذاری، اجرایی، و قضایی است. به علاوه، کمبود نیروی متخصص و فناوری پیشرفته، باعث می‌شود اجرای قوانین با موانع عملی روبه‌رو شود (Golkhandan, 2024). همچنین، در

برخی موارد، اختلاف نظرها بین نهادهای مختلف باعث کندی در فرآیندهای اجرایی شده است. با این حال، نیاز به بازنگری در قوانین برای انطباق با فناوری‌های نوین بیش از پیش احساس می‌شود.

با افزایش تهدیدات سایبری در ایران، تقاضا برای تقویت قوانین موجود و تدوین مقررات جدید افزایش یافته است. یکی از پیشنهادات اساسی، تدوین قانونی جامع‌تر با تأکید بر همکاری منطقه‌ای و بین‌المللی است. به علاوه، آموزش نیروی انسانی متخصص در زمینه سایبری و ایجاد زیرساخت‌های فناوری پیشرفته، می‌تواند به بهبود اجرای قوانین کمک کند (Javadi & Aghababayi, 2022; Manap & Taji, 2012). با توجه به تحولات اخیر، پیش‌بینی می‌شود که قوانین سایبری ایران در سال‌های آینده بهبود یافته و با نیازهای روز هماهنگ‌تر شود.

قوانین سایبری در عراق

قوانین مرتبط با جرایم سایبری در عراق به دلیل تغییرات گسترده در نظام سیاسی و اجتماعی این کشور، دارای چالش‌های عمده‌ای بوده است. پس از سقوط رژیم سابق در سال ۲۰۰۳، عراق با تهدیدات سایبری جدیدی مواجه شد که لزوم تدوین قوانین جامع در این حوزه را بیش از پیش آشکار کرد (AbdulAmeer et al., 2022). با این حال، این کشور همچنان فاقد یک قانون جامع جرایم سایبری است و اغلب به قوانین سنتی کیفری برای مقابله با این جرایم تکیه می‌کند (El Guindy & Hegazy, 2014). تلاش‌های صورت گرفته در این زمینه شامل پیش‌نویس قانون جرایم اطلاعاتی است که با انتقادات حقوق بشری روبرو شده است.

در سال‌های اخیر، عراق پیش‌نویس قانونی تحت عنوان «قانون جرایم اطلاعاتی» ارائه داده است. این قانون تلاش می‌کند تا چارچوبی برای مقابله با سوءاستفاده‌های اینترنتی و حفاظت از داده‌های حساس ایجاد کند. با این حال، این پیش‌نویس به دلیل مفاد مبهم و گسترده‌ای که ممکن است منجر به نقض آزادی بیان و محدود کردن حقوق کاربران شود، مورد انتقاد سازمان‌های حقوق بشری قرار گرفته است (Lebarmy.gov.lb, 2023). این پیش‌نویس همچنان در مرحله بررسی پارلمان قرار دارد و هنوز به تصویب نهایی نرسیده است.

عراق با چالش‌های عمده‌ای در اجرای قوانین سایبری مواجه است که شامل ضعف زیرساخت‌های فناوری اطلاعات، کمبود نیروی انسانی متخصص، و محدودیت‌های مالی است (Bayancenter, 2022). در کنار این مشکلات، نبود هماهنگی بین نهادهای دولتی و قضایی موجب شده است که بسیاری از جرایم سایبری گزارش نشده یا پیگیری نشوند (Ghareb & Sedeeq, 2018). این چالش‌ها نه تنها بر امنیت ملی تأثیر می‌گذارد بلکه موجب افزایش آسیب‌پذیری شهروندان نیز می‌شود.

سازمان‌های بین‌المللی مانند اتحادیه اروپا و سازمان ملل متحد تلاش کرده‌اند تا با ارائه مشاوره و کمک‌های فنی، به عراق در تدوین قوانین سایبری کمک کنند. با این حال، عدم ثبات سیاسی و وجود تنش‌های منطقه‌ای باعث شده است که این کمک‌ها به‌طور کامل به نتیجه نرسند (Nehme, 2023). همکاری‌های منطقه‌ای نیز به دلیل تفاوت‌های قانونی و اولویت‌های متناقض کشورها در حوزه سایبری، به کندی پیش می‌رود.

با وجود نبود قوانین جامع سایبری، دادگاه‌های عراق سعی کرده‌اند با استفاده از قوانین سنتی، به جرایم سایبری رسیدگی کنند. این رویه‌ها شامل استناد به قوانین ضد کلاهبرداری و استفاده غیرمجاز از فناوری است (Tarrad et al., 2022). با این حال، این روش‌ها به دلیل ناهماهنگی قانونی و عدم آگاهی قضات از جرایم سایبری، ناکارآمد بوده‌اند. تحلیل پرونده‌های موجود نشان می‌دهد که نیاز به آموزش قضایی در این حوزه به‌شدت احساس می‌شود.

با توجه به افزایش حملات سایبری و نیاز روزافزون به حفاظت از داده‌ها، عراق باید هرچه سریع‌تر قوانین جامعی در حوزه جرایم سایبری تصویب کند. تدوین این قوانین نیازمند مشارکت نهادهای داخلی و همکاری با سازمان‌های بین‌المللی است. علاوه بر این، سرمایه‌گذاری در زیرساخت‌های فناوری و تقویت آموزش‌های تخصصی می‌تواند به بهبود نظام حقوقی عراق کمک کند (Suleiman et al., 2023). تنها از طریق یک چارچوب قانونی جامع و کارآمد، عراق می‌تواند امنیت سایبری خود را تضمین کند.

تطبیق و مقایسه قوانین سایبری در ایران و عراق

هر دو کشور ایران و عراق با چالش‌های مشابهی در زمینه مقابله با جرایم سایبری روبه‌رو هستند، زیرا هر دو در یک منطقه ژئوپلیتیکی حساس قرار دارند. یکی از نقاط اشتراک قابل توجه، تمرکز بر حفظ امنیت ملی در برابر تهدیدات سایبری است. ایران و عراق هر دو قوانینی را برای مقابله با نفوذهای سایبری که امنیت اطلاعات حساس و دولتی را تهدید می‌کند تدوین کرده‌اند. در ایران، قانون جرایم رایانه‌ای (۱۳۸۸) به‌طور گسترده به جرایم علیه امنیت ملی پرداخته است (Golkhandan, 2024)، و در عراق نیز تلاش‌هایی برای تدوین چارچوب‌های مشابه دیده شده است، اگرچه به دلیل عدم تصویب نهایی پیش‌نویس قوانین سایبری، هنوز ساختار جامعی در این زمینه وجود ندارد (AbdulAmeer et al., 2022).

در زمینه حریم خصوصی، هر دو کشور اهمیت حفاظت از داده‌های کاربران را به رسمیت شناخته‌اند. در ایران، قوانین موجود از جمله قانون جرایم رایانه‌ای، به صراحت به حفاظت از اطلاعات شخصی پرداخته است (Shahbazi & Shabani-Kolahi, 2024)، و عراق نیز در پیش‌نویس قانون جرایم اطلاعاتی خود مفادی برای حفاظت از داده‌ها گنجانده است، هرچند اجرای این موارد با محدودیت‌هایی روبرو است (El Guindy & Hegazy, 2014).

تفاوت‌های عمده بین ایران و عراق در زمینه جرایم سایبری به توسعه زیرساخت‌های قانونی و اجرایی بازمی‌گردد. ایران از یک چارچوب قانونی منسجم برخوردار است که از طریق نهادهایی مانند پلیس فتا حمایت می‌شود. این نهاد با ایجاد سازوکارهایی برای پیشگیری و مقابله با جرایم سایبری، نقش کلیدی در اجرای قوانین ایفا می‌کند (Afshari, 2019). در مقابل، عراق با ضعف زیرساخت‌های فناوری و اجرایی روبه‌رو است و نهاد مشابهی که بتواند وظایفی مشابه پلیس فتا انجام دهد، وجود ندارد (Bayancenter, 2022).

در حوزه قوانین فرامرزی نیز ایران و عراق رویکردهای متفاوتی اتخاذ کرده‌اند. ایران، با وجود عدم عضویت در کنوانسیون‌های بین‌المللی، تلاش کرده است قوانین خود را با استانداردهای جهانی تطبیق دهد (Dehmardeh, 2020). اما در عراق، به دلیل ناهماهنگی میان نهادهای قضایی و اجرایی، حتی قوانین داخلی نیز به‌صورت کامل اجرا نمی‌شوند، چه رسد به همگرایی با استانداردهای بین‌المللی (Nehme, 2023).

تطبیق در سیاست‌گذاری سایبری

از نظر سیاست‌گذاری، ایران راهبردهای جامعی برای مدیریت امنیت سایبری و مقابله با تهدیدات دیجیتال تدوین کرده است. این راهبردها شامل تقویت همکاری‌های منطقه‌ای و تدوین مقررات جامع‌تر است (Javadi & Aghababayi, 2022; Manap & Taji, 2012). در مقابل، عراق به دلیل تغییرات سیاسی و محدودیت‌های مالی نتوانسته است سیاست‌گذاری جامعی در این زمینه ارائه دهد و بیشتر به اقدامات واکنشی و پروژه‌های موقتی بسنده کرده است (Suleiman et al., 2023).

تطبیق در حوزه جرایم مالی سایبری

هر دو کشور اهمیت مقابله با جرایم مالی سایبری را به رسمیت شناخته‌اند. در ایران، قوانینی برای مبارزه با کلاهبرداری‌های آنلاین و پولشویی سایبری تدوین شده است (Golkhandan, 2024). عراق نیز در پیش‌نویس قانون جرایم اطلاعاتی به موضوعاتی مانند سوءاستفاده مالی پرداخته است، اما این قوانین هنوز به مرحله اجرا نرسیده‌اند (Tarrad et al., 2022).

تفاوت‌های فرهنگی و اجتماعی در قوانین سایبری

فرهنگ سایبری نیز یکی از عوامل مهم در تفاوت میان ایران و عراق است. در ایران، فرهنگ استفاده از فضای مجازی تحت تأثیر سیاست‌های فرهنگی و دینی قرار دارد و قوانین نیز متناسب با این ارزش‌ها تنظیم شده‌اند (Eslami & Danesh, 2023). در مقابل، عراق به دلیل تنوع فرهنگی و ناهماهنگی در سیاست‌های فرهنگی، قوانین سایبری متناسب با تمامی اقشار جامعه تدوین نکرده است (Ghareb & Sedeeq, 2018).

تحلیل آینده‌نگر

با توجه به رشد سریع فناوری و افزایش تهدیدات سایبری، هر دو کشور نیاز به تقویت قوانین و سیاست‌های خود دارند. ایران با تکیه بر زیرساخت‌های موجود و تجربیات پلیس فتا می‌تواند به استانداردهای جهانی نزدیک‌تر شود. اما عراق برای رسیدن به این هدف نیازمند سرمایه‌گذاری در زیرساخت‌های فناوری، تقویت نهادهای اجرایی، و همکاری‌های بین‌المللی است (Bayancenter, 2022). تطبیق این دو کشور نشان‌دهنده نیاز به همکاری منطقه‌ای و بین‌المللی برای مقابله با تهدیدات مشترک در فضای سایبری است.

چالش‌ها و فرصت‌ها در مواجهه با جرایم سایبری

ایران و عراق، به‌رغم تفاوت‌های سیاسی و اقتصادی، با چالش‌های مشترکی در زمینه مقابله با جرایم سایبری روبه‌رو هستند. یکی از این چالش‌ها، محدودیت‌های فناوری است. در هر دو کشور، زیرساخت‌های فناوری اطلاعات و ارتباطات برای مقابله با تهدیدات پیچیده سایبری کافی نیستند. در ایران، اگرچه زیرساخت‌های فناوری نسبت به عراق پیشرفته‌تر است، اما تحریم‌های بین‌المللی دسترسی به فناوری‌های روز را محدود کرده‌اند (Afshari, 2019). در عراق نیز، ضعف سرمایه‌گذاری در حوزه فناوری اطلاعات و نبود برنامه‌های مدون توسعه، مانع از پیشرفت مؤثر در مقابله با جرایم سایبری شده است (AbdulAmeer et al., 2022).

ضعف همکاری‌های بین‌المللی یکی دیگر از چالش‌های کلیدی است. ایران، به دلیل مسائل سیاسی و عدم عضویت در کنوانسیون‌های بین‌المللی مانند کنوانسیون بوداپست، در هماهنگی با سایر کشورها برای مقابله با جرایم سایبری فرامرزی با مشکلاتی روبه‌رو است (Dehmardeh, 2020). در عراق، نهادهای قانونی و اجرایی به دلیل ناهماهنگی داخلی و عدم شفافیت در قوانین، قادر به ایجاد روابط مؤثر با سازمان‌های بین‌المللی نیستند (Nehme, 2023). این کمبود همکاری باعث می‌شود که توانایی هر دو کشور در مقابله با شبکه‌های مجرمانه بین‌المللی محدود شود.

کمبود نیروی متخصص نیز از مشکلات مشترک است. هر دو کشور با کمبود متخصصان سایبری روبه‌رو هستند که بتوانند به‌طور مؤثر با جرایم پیچیده سایبری مقابله کنند. این موضوع به‌ویژه در عراق، که زیرساخت‌های آموزشی سایبری مناسبی ندارد، بیشتر نمایان است (Ghareb & Sedeeq, 2018). در ایران نیز، اگرچه برنامه‌هایی برای تربیت نیروی انسانی متخصص در جریان است، اما مهاجرت نخبگان و محدودیت‌های اقتصادی، توسعه این حوزه را کند کرده است (Shahbazi & Shabani-Kolahi, 2024).

در کنار چالش‌ها، هر دو کشور فرصت‌هایی برای بهبود وضعیت خود در مقابله با جرایم سایبری دارند. یکی از مهم‌ترین فرصت‌ها، توسعه قوانین جامع‌تر و هماهنگ‌تر است. ایران می‌تواند با بازنگری در قانون جرایم رایانه‌ای و تطبیق آن با تحولات فناوری و استانداردهای بین‌المللی، چارچوب قانونی خود را تقویت کند (Golkhandan, 2024). عراق نیز می‌تواند با تصویب پیش‌نویس قانون جرایم اطلاعاتی و حذف مفاد مبهم آن، گام‌های مهمی در جهت مقابله با سوءاستفاده‌های سایبری بردارد (El Guindy & Hegazy, 2014).

تقویت همکاری‌های منطقه‌ای نیز از جمله فرصت‌های مهم است. هر دو کشور می‌توانند با ایجاد سازوکارهای همکاری مشترک در زمینه جرایم سایبری، از تجربه‌ها و منابع یکدیگر بهره‌مند شوند. این همکاری‌ها می‌تواند شامل تبادل اطلاعات، هماهنگی در مقابله با حملات سایبری فرامرزی، و برگزاری دوره‌های آموزشی مشترک باشد. سازمان‌هایی مانند اتحادیه کشورهای اسلامی و شورای همکاری‌های منطقه‌ای می‌توانند بستری مناسب برای این همکاری‌ها فراهم کنند (Javadi & Aghababayi, 2022; Manap & Taji, 2012).

سرمایه‌گذاری در آموزش و فناوری نیز می‌تواند نقشی کلیدی در تقویت توانایی‌های دو کشور داشته باشد. ایران با بهره‌گیری از دانشگاه‌ها و مؤسسات پژوهشی خود می‌تواند برنامه‌های آموزشی تخصصی برای مقابله با جرایم سایبری ارائه دهد (Eslami & Danesh, 2023). عراق نیز می‌تواند با حمایت از سازمان‌های بین‌المللی، برنامه‌های آموزشی برای تربیت نیروی متخصص را توسعه دهد (Bayancenter, 2022).

پتانسیل ارتقای همکاری‌های بین‌المللی یکی دیگر از فرصت‌هاست. ایران می‌تواند از طریق افزایش شفافیت در قوانین و سیاست‌های خود، به همکاری‌های بین‌المللی نزدیک‌تر شود (Dehmardeh, 2020). عراق نیز می‌تواند با بهبود ساختارهای داخلی و جلب حمایت نهادهای بین‌المللی، روابط خود را در حوزه مقابله با جرایم سایبری گسترش دهد (Nehme, 2023).

در نتیجه، چالش‌ها و فرصت‌های موجود نشان می‌دهد که مقابله با جرایم سایبری نیازمند اقدامات هماهنگ و سرمایه‌گذاری بلندمدت است. ایران و عراق می‌توانند با تمرکز بر توسعه قوانین، تقویت همکاری‌های منطقه‌ای و بین‌المللی، و آموزش نیروی متخصص، نه تنها با تهدیدات موجود مقابله کنند، بلکه به الگویی برای دیگر کشورهای منطقه در مدیریت فضای سایبری تبدیل شوند.

بحث و نتیجه‌گیری

این پژوهش نشان داد که جرایم سایبری به‌عنوان یکی از چالش‌های مهم عصر دیجیتال، نیازمند چارچوب‌های حقوقی و سیاست‌گذاری منسجم هستند. تحلیل تطبیقی قوانین ایران و عراق نشان داد که ایران با تدوین قانون جرایم رایانه‌ای و ایجاد نهادهایی نظیر پلیس فتا، زیرساخت‌های حقوقی و اجرایی قوی‌تری نسبت به عراق فراهم کرده است. در مقابل، عراق به دلیل فقدان قانون جامع جرایم سایبری، ضعف در نهادهای اجرایی تخصصی و محدودیت‌های سیاسی و اقتصادی، همچنان در مراحل ابتدایی مقابله با تهدیدات سایبری قرار دارد. هر دو کشور با چالش‌های مشترکی مانند ضعف همکاری‌های بین‌المللی و کمبود تخصص فنی روبرو هستند که تلاش‌های مشترک برای مقابله با جرایم سایبری را الزامی می‌کند.

ایران برای بهبود قوانین سایبری خود باید به‌روزرسانی قانون جرایم رایانه‌ای را در دستور کار قرار دهد تا با تحولات روز فناوری و جرایم سایبری نوظهور همگام شود. توسعه قوانین جامع حفاظت از داده‌ها، جرم‌انگاری رفتارهای جدید مانند حملات مبتنی بر هوش مصنوعی، و تدوین مقررات شفاف برای مقابله با جرایم فرامرزی از جمله اقدامات ضروری است. افزایش شفافیت در عملکرد نهادهای اجرایی مانند پلیس فتا و بهبود هماهنگی میان این نهادها و دستگاه قضایی نیز می‌تواند اجرای قوانین را کارآمدتر کند.

عراق باید تصویب قانون جامع جرایم سایبری را در اولویت قرار دهد. پیش‌نویس قانون جرایم اطلاعاتی باید با حذف مفاد مبهم و تقویت بخش‌های مرتبط با حقوق بنیادین شهروندان اصلاح شود. ایجاد نهاد اجرایی تخصصی برای نظارت و مقابله با تهدیدات سایبری، مشابه پلیس فتا در ایران، می‌تواند یکی از گام‌های اساسی در این مسیر باشد. همچنین، سرمایه‌گذاری در زیرساخت‌های فناوری و تربیت نیروی انسانی متخصص برای عراق ضروری است تا توانمندی‌های خود را در مقابله با جرایم سایبری ارتقا دهد.

همکاری‌های بین‌المللی برای مقابله با جرایم سایبری اهمیت بسیاری دارد. ایران می‌تواند با افزایش شفافیت در سیاست‌های خود و عضویت در کنوانسیون‌های بین‌المللی مانند کنوانسیون بوداپست، تعاملات خود را با جامعه جهانی تقویت کند. در مقابل، عراق نیز باید از حمایت‌های نهادهای بین‌المللی برای تدوین و اجرای قوانین سایبری بهره‌مند شود. ایجاد یک نهاد منطقه‌ای برای هماهنگی در مقابله با جرایم سایبری، که شامل ایران، عراق و سایر کشورهای منطقه باشد، می‌تواند به تبادل اطلاعات، هماهنگی در پیگرد مجرمان فرامرزی و برگزاری دوره‌های آموزشی مشترک منجر شود.

آموزش عمومی و تخصصی در زمینه جرایم سایبری از دیگر اولویت‌ها است. طراحی دوره‌های آموزشی در دانشگاه‌ها و مؤسسات تخصصی، برگزاری کمپین‌های آگاهی‌بخشی عمومی برای افزایش دانش کاربران فضای مجازی، و آموزش نیروهای اجرایی و قضایی می‌تواند به پیشگیری از جرایم سایبری کمک کند. سرمایه‌گذاری در فناوری‌های پیشرفته نظیر هوش مصنوعی برای پیش‌بینی و شناسایی تهدیدات سایبری نیز باید در دستور کار هر دو کشور قرار گیرد.

تقویت هماهنگی میان نهادهای داخلی نیز از اقدامات ضروری است. ایران می‌تواند با ایجاد یک کمیته دائمی برای نظارت بر اجرای قوانین سایبری، تعامل میان پلیس فتا و دستگاه قضایی را بهبود بخشد. عراق نیز نیازمند ایجاد رویه‌های شفاف برای پیگیری پرونده‌های سایبری و تقویت هماهنگی میان نهادهای دولتی و قضایی است. همچنین، تشکیل بانک اطلاعاتی مشترک میان نهادهای مختلف در هر کشور می‌تواند سرعت و کارآمدی فرایندهای قضایی و اجرایی را افزایش دهد.

چشم‌انداز آینده همکاری‌های سایبری ایران و عراق باید بر تقویت روابط منطقه‌ای و بهره‌گیری از ظرفیت‌های مشترک متمرکز باشد. ایجاد یک کنسرسیوم منطقه‌ای برای امنیت سایبری می‌تواند بستری برای تبادل دانش و همکاری در مقابله با تهدیدات سایبری فراهم کند. تدوین پروتکل‌های مشترک امنیتی و بهره‌گیری از فناوری‌های پیشرفته در سطح منطقه‌ای می‌تواند توانایی دو کشور را در مقابله با تهدیدات فرامرزی افزایش دهد.

با توجه به پیچیدگی روزافزون جرایم سایبری، ایران و عراق باید برنامه‌های بلندمدتی برای مقابله با این تهدیدات تدوین کنند. تقویت همکاری‌های بین‌المللی، بهبود زیرساخت‌های فنی، تدوین قوانین پیشرفته، و آموزش نیروی انسانی می‌تواند امنیت سایبری پایدار را در این دو کشور تضمین کند. اقدامات هماهنگ و بهره‌گیری از تجربیات جهانی می‌تواند ایران و عراق را به الگویی برای مدیریت فضای سایبری در منطقه خاورمیانه تبدیل کند.

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

In recent decades, the unprecedented growth of digital technologies has transformed social, economic, and legal landscapes. This rapid evolution has brought numerous opportunities while also exposing nations to escalating cybersecurity threats. Cybercrimes have transcended geographical boundaries, becoming a formidable challenge for international governance. Addressing these issues demands a comparative understanding of national legal frameworks and policies. This study critically analyzes the approaches adopted by Iran and Iraq—two neighboring countries with shared cultural and geopolitical dynamics—to address cybercrimes. The study explores the strengths and limitations of their respective legal systems, policies, and international collaborations while drawing insights from scholarly perspectives.

The legal system in Iran is notable for its structured and progressive approach to cybercrime. The cornerstone of Iran's cybersecurity governance is the Computer Crimes Act of 2009, which provides comprehensive definitions and penalties for cyber offenses such as unauthorized access, data theft, and online fraud (Golkhandan, 2024). This act also addresses the protection of personal data, an area of growing concern in the digital age (Shahbazi & Shabani-Kolahi, 2024). However, the lack of alignment with international standards, such as the Budapest Convention, remains a significant limitation, impeding cross-border collaboration (Dehmardeh, 2020). Policymakers in Iran face the dual challenge of modernizing existing laws while navigating political constraints that limit international cooperation. The role of Iran’s cyber police, FATA, has been instrumental in enforcing these laws, though its efforts are hindered by resource limitations and technological barriers (Afshari, 2019).

Conversely, Iraq’s cybersecurity framework remains underdeveloped due to years of political instability and economic challenges. The absence of a comprehensive cybercrime law has resulted in fragmented policies that fail to address the complexity of digital threats (Bayancenter, 2022). While a draft law on cybercrime has been proposed, it has faced criticism for potential overreach and ambiguities that could suppress freedom of expression (El Guindy & Hegazy, 2014). Iraq’s reliance on traditional criminal laws to address cybercrimes highlights a critical gap in its governance structure. Moreover, the lack of specialized enforcement agencies akin to Iran’s FATA further exacerbates Iraq’s vulnerability to cyber threats (Ghareb & Sedeeq, 2018).

The comparative analysis underscores key similarities and differences in the cybercrime policies of Iran and Iraq. Both countries emphasize national security in their legal frameworks, reflecting their geopolitical sensitivities. However, Iran’s approach is relatively proactive, incorporating dedicated laws and enforcement mechanisms. In contrast, Iraq’s strategy is largely reactive, constrained by limited resources and institutional weaknesses (AbdulAmeer et al., 2022). Despite these differences, both nations face common challenges, including insufficient international collaboration and inadequate technical expertise (AbdulAmeer et al., 2022). Enhancing regional cooperation could offer a viable solution to these shared challenges, fostering mutual support in policy development and enforcement.

Cultural and social factors play a significant role in shaping the cyber policies of both countries. In Iran, the integration of cultural and religious values into cybersecurity policies has led to a unique regulatory framework that emphasizes moral considerations (Eslami & Danesh, 2023). Conversely,

Iraq's diverse cultural fabric and lack of cohesive policy orientation have contributed to inconsistencies in its approach to digital governance (Nehme, 2023). These cultural dimensions highlight the need for localized solutions that resonate with societal values while aligning with global standards.

International collaboration emerges as a pivotal factor in combating cybercrime. Iran's limited engagement with global frameworks, such as the Budapest Convention, has restricted its ability to address transnational cyber threats effectively (Dehmardeh, 2020). Iraq, despite receiving technical support from international organizations, has struggled to implement these recommendations due to domestic challenges (Bayancenter, 2022). Both countries would benefit from enhanced participation in international forums and regional initiatives, which could facilitate knowledge sharing and capacity building.

Policy recommendations for Iran and Iraq focus on three key areas: legislative reform, institutional strengthening, and international cooperation. For Iran, aligning domestic laws with international standards and expanding the mandate of FATA to include advanced cyber forensics could significantly improve its cybersecurity posture (Shahbazi & Shabani-Kolahi, 2024). For Iraq, the immediate priority should be the enactment of a comprehensive cybercrime law that balances security needs with human rights considerations (El Guindy & Hegazy, 2014). Additionally, establishing a specialized cyber enforcement agency and investing in technical infrastructure are critical steps for Iraq to mitigate its vulnerabilities (AbdulAmeer et al., 2022).

In conclusion, the evolving nature of cybercrime demands adaptive and collaborative governance strategies. The comparative insights from Iran and Iraq underscore the importance of integrating legal, technical, and cultural dimensions into cybersecurity policies. By addressing their respective weaknesses and leveraging regional and international partnerships, both countries can enhance their resilience against digital threats. This study contributes to the broader discourse on cybersecurity governance by highlighting the interplay between national policies and global challenges, offering a roadmap for other nations grappling with similar issues.

References

AbdulAmeer, S. A., Saleh, W. R., & Hussam, R. (2022). Cyber Security Readiness in Iraq: Role of the Human Rights Activists. *Journal of Cybercrime Studies*. https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/86

Afshari, M. (2019). Comparative study of cyber-crime in Iran and international law. *Journal of Comparative Law*. https://lps.journals.umz.ac.ir/article_2566_783e7bca98a9dedadefe9404b701cfec.pdf

Ali, W. W., & Ahmmad, Y. K. (2023). The emergence of cybersecurity and its roles in developing contemporary international law. https://www.researchgate.net/publication/378769830

Amiri-Moghadam, E., & Zarei, S. (2022). Comparative Analysis of Laws in Iran and Iraq Against Internet Fraud. *Defense Law Studies*, *17*(5), 58-75. https://sds.sndu.ac.ir/article_1653.html

Asgari, M., Moravat, H., & Alipour, H. (2020). Comparative Analysis of Iran's Criminal Policy in Combating Cyber Theft. *Criminal Law Research*, *12*(4), 34-50. https://jclr.atu.ac.ir/article_12123_0.html

Bayancenter. (2022). *Constructing an interinstitutional effort on cyber security in Iraq*. https://www.bayancenter.org/en/wp-content/uploads/2022/03/87tr6tdf.pdf

Dehmardeh, S. (2020). A Study of the Legal System of New Technologies in Iran. *Blue-Ap.com*. https://blue-ap.com/J/List/8/iss/volume%2009%20(2020)/issue%2002/2.pdf

El Guindy, M. N., & Hegazy, F. (2014). Cybercrime Legislation in the Middle East. https://www.researchgate.net/publication/259583247_Cybercrime_Legislation_in_the_Middle_East

Eslami, R., & Danesh, A. (2023). Critical analysis of representation in cyberspace; case study of Iran. *Springer*. https://doi.org/10.1007/s10708-022-10675-8

Gharaibeh, A., & Al-Senussi, M. (2023). Administrative Obligations for Diplomatic Missions in the Context of International and National Law: Implications and Challenges for Cybercrime. *Journal of Cybercrime Studies*. https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/207

Ghareb, M. I., & Sedeeq, F. M. (2018). Electronic Crimes and the International Community Legislation: Comparative Analytical Study. https://www.researchgate.net/profile/Mazen-Ghareb-2/publication/327159884_Electronic_Crimes_And_The_International_Community_Legislation_Comparative_Analytical_Study/links/5b7d5d0092851c1e12273c11/Electronic-Crimes-And-The-International-Community-Legislation-Comparative-Analytical-Study.pdf

Golkhandan, S. (2024). The Extent of Using the Control Theory to Deal with Computer Crimes in Iran's Criminal Policy. *Journal of Comparative Criminal Justice*. https://www.jccj.ir/article_200467.html?lang=en

Javadi, M., & Aghababayi, R. (2022). Developing Cyber Criminal Policies in Iran to Combat Hacking. *Scientific Quarterly of Opinions*, *11*(4), 90-112. https://doi.org/10.25007/ajnu.v11n4a1246

Katman, F. (2021). *The Islamic Republic of Iran's cyber security strategy*. Routledge. https://doi.org/10.4324/9780429399718-37

Kshetri, N. (2005). Pattern of global cyber war and crime: A conceptual framework. *Journal of International Management*. https://doi.org/10.1016/j.intman.2005.09.009

Majidi, S. (2021). Analysis of Iran's Criminal Policy Against Phishing. *Criminal Studies*, *8*(3), 29-50. https://nashr.majles.ir/m/article_442.html?lang=fa

Manap, N. A., & Taji, H. (2012). Cyber crimes: Lessons from the legal position of Malaysia and Iran. *International Journal of Information and Electronics Engineering*. https://doi.org/10.7763/IJIEE.2012.V2.125

Mokhtaripour, M. (2021). A comparative study of Internet police on combating computer crimes. https://www.researchgate.net/publication/280977819

Nehme, T. (2023). *Impasse of Cyber laws: Iraqi Case*. https://www.lebarmy.gov.lb/en/content/impasse-cyber-laws-iraqi-case

Rahimi, M., & Shaygan-Fard, A. (2023). Iran's Criminal Law Approach to Privacy Protection in Cyberspace. *Justice Legal Journal*, *10*(2), 45-67. https://www.jlj.ir/mobile/article_707463.html

Shahbazi, A. (2019). Technological developments in cyberspace and commission of crimes in international law and Iran. *Journal of Legal Ethical & Regulatory Issues*.

Shahbazi, A., & Shabani-Kolahi, F. (2024). Legal Challenges in Protecting Personal Data in Iran's Cyberspace. *Modern Technology Law Journal*, *19*(1), 80-97. https://mtlj.usc.ac.ir/article_190516.html

Suleiman, N. M., Hatim, A., & Alseidi, M. A. (2023). Cybercrime Laws in Iraq: Addressing Limitations for Effective Governance.

Tarrad, K. M., Al-Hareeri, H., & Alghazali, T. (2022). Cybercrime Challenges in Iraqi Academia: Creating Digital Awareness for Preventing Cybercrimes. *Journal of Cybercrime Studies*. https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/download/87/24

Zarneshan, S., Kheyrani, R., & Soleimanian, M. (2022). Evaluation of Iran's Status Regarding International Regulations on Cybercrimes. *Legal Research Journal*, *15*(3), 56-78. https://jlr.sdil.ac.ir/article_148310.html?lang=fa