Comparative Studies on Islamic and Western Law
Print ISSN : 2476 - 4213 Online ISSN : 2476 - 4221
Homepage : https://csiw.qom.ac.ir

A Comparative Study of the Legal Systems of Iran and Pakistan in Response to Digital Crimes with an Approach to International Documents on the Digital Space

Peyman Namamian [1]

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

Received: 2024/10/04
Revised: 2025/01/06
Accepted: 2025/02/23
Published online: 2025/12/22

Abstract

Digital crimes, which originate from digital space technology, can only be observed. They are controlled and prevented through digital laws. Countries face the dangers of digital crimes for many reasons, from poor technology, inability and lack of standards to financial constraints, lack of cooperation with international law and implementing organizations. In order to combat digital crimes to the maximum extent, the Iranian legislator is trying to establish numerous and diverse regulations and documents that aim to strengthen the legal capacities for discovering and prosecuting the perpetrators of such crimes. However, despite the legislator's knowledge of the possibility of committing various crimes on digital platforms, the type of legal provisions has not been established according to the circumstances and situation of the perpetrator and the type of crime, which will somehow cause the expansion of the perpetrators' activism in such a space. In addition, in recent decades, the Pakistani legislator has attempted to adopt various regulations in order to protect the digital space and combat threats and crimes committed in it, and has established centers in this regard, which have provided the means to prevent and suppress the commission of digital crimes. Of course, the established standards have not been able to provide the digital space with legal and legal protection to the maximum extent. Therefore, the question of "Given the technical and technological developments in the global community, what capacity is there in the legislative sphere of Iran and Pakistan in responding to digital crimes?" has been the main focus of this article, the answer to which is the ultimate goal of writing the article.

Keywords: Digital Space, Digital Crimes, Digital Security, Digital Rights of Iran and Pakistan, International Digital Rights.

How To Cite: Namamian, p (2025). A Comparative Study of the Legal Systems of Iran and Pakistan in Response to Digital Crimes with an Approach to International Documents on the Digital Space, *Comparative studies on Islamic and Western Law*, 12(4), 259-285. http://www.doi.org/10.22091/csiw.2025.11430.2593

Published by: University of Qom **Article type: Research**

پژوهش تطبیقی حقوق اسلام و غرب
شاپا الکترونیکی: ۲۴۷۶-۴۲۲۱ شاپا چاپی: ۲۴۷۶-۴۲۱۳
Homepage : https://csiw.qom.ac.ir

مطالعه تطبیقی نظام حقوقی ایران و پاکستان در پاسخ به جرائم دیجیتالی با رویکردی به اسناد بین‌المللی فضای دیجیتالی

پیمان نمامیان[1]

۱. دانشیار حقوق کیفری و جرم‌شناسی، دانشکده علوم اداری و اقتصاد دانشگاه اراک، اراک، ایران، رایانامه: p-namamian@araku.ac.ir

چکیده

جرائم دیجیتالی که منشأ فناوری فضای دیجیتالی است تنها قابل رصد است. از طریق حقوق دیجیتالی کنترل و پیشگیری می‌شود. کشورها به دلایل متعددی از فناوری ضعیف و ناتوانی و فقدان موازین گرفته تا محدودیت‌های مالی، عدم همکاری با حقوق بین‌المللی و سازمان‌های مجری با خطرات جرائم دیجیتالی مواجه هستند. قانون‌گذار ایران در راستای مقابله حداکثری با جرائم دیجیتالی ضمن مبادرت به وضع مقرره‌ها و اسناد متعدد و گوناگونی می‌کند که هدف تقویت ظرفیت‌های حقوقی ناظر به کشف و تعقیب مرتکبان این‌گونه جرائم ارتکابی است، لکن قانون‌گذار به‌رغم اشراف اطلاعاتی به امکان ارتکاب جرائم متنوع در سکوهای دیجیتالی، اما نوع گذاره‌های قانونی وفق شرایط و موقعیت مرتکب و نوع جرم وضع نشده است که این امر به‌نحوی موجبات توسعه کُنشگری مرتکبان را در چنین فضایی را رقم خواهد زد. قانون‌گذار پاکستان طی دهه‌های اخیر در راستای حفاظت از فضای دیجیتالی و مقابله با تهدیدها و جرائم ارتکابی در آن ضمن مبادرت به تصویب مقرراتی گوناگون، نسبت به تشکیل مراکزی دراین‌باره نموده است که موجبات پیشگیری و سرکوب ارتکاب جرائم دیجیتالی را فراهم آورده است. موازین مقرر به نحو حداکثری نتوانسته است فضای دیجیتالی را مورد حمایت قانونی و حقوقی قرار دهد. بنابراین پرسش اینکه «با توجه به تحولات فنی و فناورانه در جامعه جهانی، چه ظرفیتی در قلمرو قانون‌گذاری ایران و پاکستان در پاسخ به جرائم دیجیتالی وجود دارد؟» به‌عنوان محور اصلی این مقاله بوده که پاسخ بدان، هدف غایی تقریر مقاله است.

کلیدواژه‌ها: فضای دیجیتالی، جرائم دیجیتالی، امنیت دیجیتالی، حقوق دیجیتالی ایران و پاکستان، حقوق بین‌المللی دیجیتالی.

تاریخ دریافت: ۱۴۰۳/۰۷/۱۳
تاریخ اصلاح: ۱۴۰۳/۱۰/۱۷
تاریخ پذیرش: ۱۴۰۳/۱۲/۰۵
تاریخ انتشار برخط: ۱۴۰۴/۱۰/۰۱

استناد: نمامیان، پیمان (۱۴۰۴). مطالعه تطبیقی نظام حقوقی ایران و پاکستان در پاسخ به جرائم دیجیتالی با رویکردی به اسناد بین‌المللی فضای دیجیتالی، پژوهش تطبیقی حقوق اسلام و غرب، ۱۲(۴)، ۲۸۵-۲۵۹. http://www.doi.org/ 10.22091/csiw.2025.11430.2593

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

مقدمه

در کنار توسعه سریع فناوری اطلاعات و ارتباطات و شیوع فزاینده اینترنت، این فعالیت‌های مجرمانه به‌طور قابل توجهی اقتصاد جهانی، امنیت ملی، ثبات اجتماعی و علایق فردی را مختل می‌کند؛ اگرچه تخمین هزینه دقیق مالی جرائم دیجیتال دشوار است. توسعه اینترنت و فناوری‌های دیجیتال، فرصتی بزرگ برای بشریت در تبدیل کسب‌وکارها و ارائه ابزارهای جدید برای ارتباطات روزمره است. بر این اساس، اشکال جدید جرائم دیجیتالی چالش‌های نوینی را برای قانون‌گذاران، سازمان‌های مجری قانون و نهادهای بین‌المللی ایجاد می‌کند. این امر مستلزم وجود سازوکارهای فراملی و داخلی مؤثر است که بر استفاده از فناوری اطلاعات و ارتباطات برای فعالیت‌های مجرمانه در فضای مجازی نظارت می‌کند.

با رشد اینترنت، شبکه‌های سیمی و بی‌سیم، دوربین‌های تحت وب و دسترسی آسان به اطلاعات، تلفن‌های هوشمند و تبلت‌ها، فرصت‌های جرائم رایانه‌ای در حال افزایش است و مجریان قانون منابع فزاینده‌ای را به این موارد اختصاص می‌دهند.[۱] افزون بر این، جرائم دیجیتالی یک نگرانی عمده برای جامعه جهانی است؛ زیرا معرفی، رشد و بهره‌گیری از فناوری‌های اطلاعات و ارتباطات باعث افزایش فعالیت‌های مجرمانه شده است. جرائم دیجیتالی، گونه‌ای آشکار از جرائم بین‌المللی است که تحت تأثیر انقلاب جهانی در فناوری اطلاعات و ارتباطات قرار گرفته است. بر این اساس، اشکال جدید جرائم دیجیتالی چالش‌های نوینی را برای قانون‌گذاران، سازمان‌های مجری قانون و نهادهای بین‌المللی ایجاد می‌کند. این امر مستلزم وجود سازوکارهای فراملی و داخلی مؤثر است که بر استفاده از فناوری اطلاعات و ارتباطات برای فعالیت‌های مجرمانه در فضای مجازی نظارت می‌کند.

فضای بی‌مرز دیجیتال، جهانی موازی با جهان حقیقی را به وجود آورده است که درواقع کنترل و ادارهٔ حقوقی آن از حیطهٔ اِعمال قدرت یک حاکمیت برنمی‌آید. برای حاکمیت بر این فضا و مقابله با جرائم روزافزون و پیچیدهٔ ارتکابی در آن، همکاری و معاضدت جامعهٔ بین‌المللی برای قاعده‌سازی ضرورت دارد،

---

۱ به آدرس زیر مراجعه شود:

https://hamzaandhamza.com/cyber-crime/

به‌گونه‌ای که هیچ مجرمی بدون کیفر نماند نیل به این امر با تدوین مقررات هماهنگ و متحدالشکل امکان‌پذیر است؛ زیرا جرائم ارتکابی در فضای دیجیتال مرزهای جغرافیایی و سنتی را پشت سر می‌گذارند و به سبب ویژگی‌هایی که دارند، می‌توان برخی از این‌گونه جرائم را در زمرهٔ آن دسته جرائمی به شمار آورد که برای مقابله با آن‌ها اعمال صلاحیت جهانی ضرورت دارد (جلالی و توسلی‌اردکانی، ۱۳۹۸: ۱۳۵۱). جرائم ارتکابی در بستر این فناوری، آنگاه که به ارزش‌های بنیادین جوامع بشری، به‌ویژه کرامت انسانی آسیب برسانند، از طریق جرم‌انگاری‌های متناسب سرکوب می‌شوند (کردعلیوند و میرزایی، ۱۳۹۷: ۱۹۲).

مرتکبان جرائم دیجیتالی به‌طور مداوم درحال‌توسعه فنون پیشرفته با جابه‌جایی اهداف خود هستند که به‌طور عمده کمتر بر سرقت اطلاعات مالی و بیشتر بر جاسوسی تجاری و دسترسی به اطلاعات دولتی تمرکز دارند. درزمینهٔ جرائم دیجیتالی که به سرعت گسترش می‌یابد، دولت‌های کشورهای درحال‌توسعه باید در سطح جهانی همکاری کنند تا بتوان یک مدل مؤثر برای کنترل تهدیدها ایجاد کرد.

کشورهای درحال‌توسعه به دلیل توسعه و پیشرفت در فناوری رایانه و مخابرات، قادر به توسعه و گسترش شبکه‌های ارتباطی خود با ایجاد امکان شبکه‌سازی و تبادل اطلاعات سریع و آسان هستند. جرائم دیجیتالی طی سال‌های اخیر در سطح جهان افزایش یافته است که این سناریو را به طرز چشم‌گیری تغییر داده است، اکنون مجرمان از ابزارهای پیچیده‌ای برای شکستن امنیت دیجیتالی استفاده می‌کنند. علاوه‌بر این، اخیراً بدافزارها، ایمیل‌های هرزنامه، هکِ وبگاه‌های نهادها و سازمان‌ها و سایر حملاتی از این دست، کار نابغه‌های رایانه‌ای است که استعداد آن‌ها را آشکار می‌کند. این حملات نادر بدخواهانه به‌تدریج به سندیکای جرائم دیجیتالی تبدیل شده‌اند که از طریق سکوهای دیجیتالی غیرقانونی پول جمع‌آوری می‌کنند.

با در نظر گرفتن ماهیت بین‌المللی جرائم دیجیتالی، ممکن است نه‌تنها در مناطقی که از آنجا منشأ می‌گیرد، بلکه سایر کشورها یا مناطق را نیز درگیر کند. جرائم دیجیتالی نه‌تنها به اقدام‌های کنترلی هماهنگ شده بین‌المللی نیز نیاز دارد. به همین ترتیب، سازوکار تحقیق و گزارش این جرائم باید منابع فشرده باشد. اگرچه دولت‌های کشورهای توسعه‌یافته و درحال‌توسعه مصمم و فعالانه بر مبارزه و پیشگیری از مرتکبان جرائم دیجیتالی برای پیشگیری از آسیب به زیرساخت‌های دیجیتالی خود تمرکز می‌کنند، اما ماهیت فضای

دیجیتالی چالش‌های متعدد در اجرای مقررات دیجیتالی ایجاد می‌کند. علاوه‌بر این، مرتکبان جرائم دیجیتالی و فنون آن‌ها به‌طور مداوم در حال تغییر هستند و همین امر، همگام شدن با سازوکارهای در حال تغییر مورد استفاده توسط مرتکبان جرائم دیجیتالی را برای دولت‌ها و کسب‌وکارها دشوارتر می‌کند.

در چارچوب سیاست جنایی تقنینی ایران، قانون‌گذار مبادرت به وضع مقررات بسیاری نظیر قانون جرائم رایانه‌ای (۱۳۸۸) نموده است که مبنی بر مقابله آشکار و مؤثر در مقابله با جرائم دیجیتالی را دارند. قانون‌گذار در این فرایند ضمن شناسایی گونه‌های متنوع جرائم ارتکابی در سکوهای دیجیتالی، مبادرت به پاسخ‌دهی به آن‌ها نموده است. آنچه در این فرایند مورد اهمیت قانون‌گذار در شناسایی مرتکبان و کنشگری آن‌ها در سکوهای دیجیتالی در ارتکاب جرائمی بوده، امکان مقابله با نقض امنیت آن‌ها است. قانون‌گذار با توجه به تحولات ناظر به تنوع جرائم ارتکابی نسبت به هدف و غایت جرم ارتکابی و کیفیت مؤثر و مطلوب پاسخ‌دهی به آن غفلت ورزیده و امکان مقابله متناسب به آن‌ها را نتوانسته در چارچوب سیاست جنایی مدنظر قرار دهد.

افزون بر این، پاکستان تلاش‌هایی را برای دیجیتالی کردن نه‌تنها بخش عمومی انجام داده است، بلکه چندین اقدام برای تسهیل رونق دیجیتال در بخش خصوصی نیز آغاز شده است. سیاست فناوری اطلاعات برای ایجاد فرهنگ دیجیتال در جامعه در کنار سیاست پهنای باند معرفی شد. سرعت و اتصال به اینترنت در گذشته دو برابر شده است (Chaudhy, 2012: 89-91). پاکستان به‌عنوان کشوری با میزان جرائم دیجیتالی بالاتر از سایر کشورها شناخته شده است. این شامل تهدیدها و جرائم دیجیتالی گوناگون نظیر هک، سرقت هویت، کلاهبرداری مالی، کلاهبرداری‌های فیشینگ و حملات باج افزار است. این روند را می‌توان به عدم آگاهی در مورد امنیت دیجیتالی، اجرای ضعیف مقررات دیجیتالی، منابع محدود برای اجرای قانون و افزایش استفاده از فناوری در کشور نسبت داد (Magalla, 2013: 64-65). هیچ‌قانون مناسبی برای پیشگیری از جرائم دیجیتالی برای محافظت از کاربران در قبال کلاهبرداری‌های الکترونیکی و... که مانع بزرگی در برابر اعتماد و اطمینان کاربران است، وضع نشده است؛ اگرچه فرمان جرائم الکترونیکی پاکستان مصوب ۲۰۰۲[۱] و اصلاحی ۲۰۰۸ (Pakistan Electronic Crimes Ordinance, 2002) ابلاغ شد، اما این قانون پس از

---

۱ به آدرس زیر مراجعه شود:
https://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-apaUY2Fta5Y%3D-sg-jj

شش هفته در قانون اساسی ۱۹۷۳ لغو شد. علاوه‌بر این، قانون جرائم الکترونیکی پاکستان مصوب ۲۰۰۷[۱] (Pakistan Electronic Crimes Act, 2007) و قانون جرائم الکترونیکی پاکستان مصوب ۲۰۱۶[۲] (Pakistan Electronic Crimes Act, 2016) آغاز شده است.

روش مطالعه در این مقاله از نوع توصیفی‌تحلیلی و بر پایه اسناد و منابع مکتوب به‌وسیله مطالعه کتابخانه‌ای (با اهدافی نظیر رویارویی با توسعه فزاینده جرائم دیجیتالی، روزآمدسازی سازوکارهای مقابله و پیشگیری مؤثر در قبال جرائم دیجیتالی و سنجش مقررات مصوب در نظام حقوقی ایران و پاکستان در مقابله حداکثری با جرائم دیجیتالی) بوده که برای جمع‌آوری اطلاعات از ابزار فیش‌برداری استفاده شده است.

۱. مفهوم جرم دیجیتالی و شناخت آن

از زمان پیدایش اولین جرم فناوری اطلاعات تاکنون اصطلاحات متعددی برای نام‌گذاری این پدیده مورد استعمال قرار گرفته است که مهم‌ترین آن‌ها شامل «جرم رایانه‌ای»، «جرم مرتبط با رایانه»، «جرم اینترنتی»، «جرم شبکه»، «جرم رایانه‌ای و اینترنت»، «جرم سایبر»، «جرم رایانه‌ای‌سایبر»، «جرم مرتبط با رایانه و فناوری برتر»، هستند.

راجع‌به تعریف «جرم فناوری اطلاعات» نیز مباحث زیادی بین صاحب‌نظران علم حقوق در جریان بوده و تعاریف متعددی از سوی آن‌ها ارائه شده است، اما درنهایت به این نتیجه رسیده‌اند که نمی‌توان تعریفی کلی از جرم رایانه‌ای ارائه کرد که برای کلیه شاخه‌ها و اهداف حقوق کیفری و علوم جنایی قابل استفاده باشد. در یک تقسیم‌بندی کلی می‌توان جرائم فناوری اطلاعات را ازلحاظ فلسفه قانون‌گذاری و قوانین حاکم بر آن‌ها، به دو گروه تقسیم کرد. گروه نخست، شامل طیفی از جرائم رایانه‌ای است که با مقررات مربوط به جرائم سنتی قابل تعقیب و کیفر هستند و نیازها به قانون‌گذاری جدید ندارند. این گروه خود شامل انواع گوناگونی از جرائم است و می‌توان آن‌ها را به جرائم علیه اشخاص، اموال، امنیت و آسایش عمومی، اخلاق

---

۱ به آدرس زیر مراجعه شود:
http://pklegal.org/pdf/Prevention-of-Electronic-Crimes-Ordinance-2007-(PECO2007).pdf

۲ به آدرس زیر مراجعه شود:
https://www.na.gov.pk/uploads/documents/1470910659_707.pdf

و عفت عمومی و خانواده دسته‌بندی نمود. گروه دوم، شامل طیفی از جرائم رایانه‌ای است که نیاز به قانون خاص دارند. این طبقه از جرائم را نیز می‌توان به سه دسته تقسیم نمود: دسته اول جرائم جدیدی هستند که ارتکاب آن‌ها قبل از پیدایش فناوری اطلاعات به‌هیچ‌وجه امکان‌پذیر نبوده است. مانند دستیابی غیرمجاز، شنود غیرمجاز، اخلال در داده و اخلال در سامانه؛ دسته دوم شامل تعدادی از جرائم سنتی است که رایانه ماهیت آن‌ها را تغییر داده و به لحاظ تفاوت ماهیتی بین نوع رایانه‌ای و نوع سنتی آن‌ها، نیاز به قانون خاص دارند. جعل و کلاهبرداری رایانه‌ای ازجمله این جرائم هستند؛ دسته سوم شامل جرائمی است که ارتکاب آن‌ها از طریق شبکه‌های رایانه‌ای موجب خطرناک‌تر شدن آن‌ها نسبت به نوع غیر رایانه‌ای آن‌ها شده است و به همین جهت نیاز به قانون خاص دارند. جرائم مرتبط با محتوا جزء این دسته هستند. بر اساس اهداف تحقیقاتی مختلف طبقه‌بندی‌های گوناگونی از جرائم رایانه‌ای به عمل آمده است (خرم‌آبادی، ۱۳۸۴: ۵).

فناوری دیجیتال به‌عنوان ابزاری بسیار پویا برای ارتباطات دارای کاربرد قابل ملاحظه‌ای است. به‌نحوی که این فناوری نیروی محرکه‌ای برای بازیگران غیردولتی و حامیان آن‌ها برای طیف وسیعی از اهداف است (Buresh, 2020: 71-72). اینترنت به دلیل مزایای بسیاری که ارائه می‌کند، به ابزار مورد علاقه مرتکبان جرائم دیجیتالی تبدیل شده است، ازجمله دسترسی آسان، مقررات اندک یا بدون محدودیت، سانسور ضعیف یا بدون آن یا سایر اشکال کنترل دولتی، مخاطبان بالقوه عظیمی که در سراسر جهان منتشر می‌شوند (Sander, 2022: 295). ناشناس بودن ارتباطات، جریان سریع اطلاعات، تعامل، توسعه و نگهداری ارزان یک حضور وب، یک محیط چندرسانه‌ای و توانایی تأثیرگذاری بر پوشش در رسانه‌های جمعی سنتی (Odhiambo, Ochara and Kadymatimba, 2018: 149-151). عصر دیجیتال و گسترش سکوهای موجود در فضای مجازی، ظهور جرائم دیجیتالی را تسهیل کرد.

به هر روی، می‌توان در اندیشه صاحب‌نظران جرائم دیجیتال را در تعاریف گوناگون ملاحظه کرد که با توجه به تحولات فزاینده این نوع جرم، زوایای این اندیشه‌ها در دو محور مورد مطالعه قرار می‌گیرد:

الف. جرائم دیجیتال، جرائمی هستند که با استفاده از دستگاه‌های دیجیتال، رایانه، تلفن همراه و موارد دیگر مرتبط هستند. جرم دیجیتال به‌عنوان جرمی تعریف می‌شود که داده‌های رایانه‌ای و سامانه‌های دیجیتال

مرتبط با آن را هدف قرار می‌دهد که در آن دسترسی، سرقت، تغییر، فساد یا اختلال غیرمجاز انجام می‌شود. یک جرم دیجیتال تنها زمانی رخ می‌دهد که یک آسیب‌پذیری در سامانه یا برنامه مورد نظر شناسایی و مورد سوءاستفاده قرار گیرد (ملکوتی و خلیل‌زاده، ۱۴۰۱: ۸۳-۸۱). آسیب‌پذیری به‌عنوان ضعفی تعریف می‌شود که در دستگاه‌ها یا گروهی از دستگاه‌ها (منابع) وجود دارد که می‌تواند توسط یک تهدید مورد سوءاستفاده قرار گیرد. آسیب‌پذیری‌ها منابع را در معرض خطر بزرگی قرار می‌دهند. خطر به‌عنوان امکانی برای داده‌ها یا یک سامانه تعریف می‌شود که دچار فساد، از دست دادن، سرقت، آسیب، اختلال یا تخریب شود. این دسته از جرائم در گونه‌ها و اَشکالی نظیر کلاهبرداری و سرقت هویت، جنگ اطلاعاتی، کلاهبرداری‌های فیشینگ و هرزنامه قابل ملاحظه است (Taylor, 2014: 48-50).

ب. جرائم دیجیتالی، جرائم نوظهوری هستند که به‌طور غیرقانونی از طریق اینترنت انجام می‌شود، مانند شکستن اوراق بهادار اینترنتی، جعل یا تجاوز به حساب‌های الکترونیکی، شکستن رمزهای عبور حساب‌های بانکی، حملات جاسوسی دیجیتالی و... جرائم دیجیتالی بسیار قابل کیفر هستند. جرائم دیجیتال ازجمله جرائمی است که مولود جامعه فناور و مدرن بوده و به همین دلیل، ابهامات زیادی در باب ماهیت و پیشینه این‌گونه جرائم از یک سو و ویژگی‌های این جرائم و مرتکبان آن‌ها از سوی دیگر وجود دارد. با عنایت به این ابهامات و نیز تفاوت‌های موجود بین جرائم دیجیتال و سایر جرائم، پیشگیری و مقابله با جرائم دیجیتال اقدام‌های تهاجمی خاصی را می‌طلبد (موسوی و همکاران، ۱۴۰۱: ۳۲۳). جرم دیجیتالی زمانی شروع می‌شود که فعالیت غیرقانونی وجود داشته باشد. این فعالیت‌ها برای داده‌ها یا اطلاعات موجود در رایانه‌ها یا شبکه‌ها انجام می‌شود.[۱]

اصطلاح جرائم رایانه‌ای برای اشاره به هرگونه فعالیت مجرمانه‌ای که علیه رایانه‌ها و شبکه‌ها یا استفاده از رایانه به‌عنوان ابزاری برای انجام آن فعالیت انجام می‌شود استفاده می‌شود. اما طی سال‌های اخیر این جرائم به سایر دستگاه‌های دیجیتال نظیر تلفن همراه نیز گسترش یافته است، این اصطلاح به جرائم دیجیتال نیز تعمیم داده شد (دشتی و افشاری، ۱۳۹۸: ۸۳). تاکنون تعریف واحدی برای جرائم دیجیتالی ارائه نشده و

۱ به آدرس زیر مراجعه شود:
https://www.igi-global.com/dictionary/digital-forensics-and-data-mining/7591

شکل‌گیری استاندارد آن دشوار است (Dupont and Holt, 2022)، اما آنچه می‌توان ابراز داشت اینکه جرائم دیجیتالی علیه داده‌ها یا سامانه‌های رایانه‌ای، دسترسی غیرمجاز، تغییر یا آسیب به یک رایانه یا سامانه دیجیتال متمرکز است.

با جمع اندیشه‌های صاحب‌نظران می‌توان اذعان داشت رفتارهای مجرمانه در فضای دیجیتال که به «جرم یا جرائم دیجیتالی» اطلاق می‌شوند، درواقع زمانی شروع می‌شود که فعالیت غیرقانونی وجود داشته باشد. این فعالیت‌ها برای داده‌ها یا اطلاعات موجود در رایانه‌ها یا شبکه‌ها صورت می‌پذیرد. جرائم دیجیتال برخلاف جرائم سنتی، دارای ویژگی‌های منحصربه‌فردی هستند. در عین حال، این دسته از جرائم فاقد هرگونه قلمرو جغرافیایی است و می‌تواند در یک کشور یا منطقه علیه کشور یا منطقه دیگر مرتکب شد.

تعریف جدید از سنجش دقیق تعاریف موجود در ادبیات قابل دسترس عموم قابل ملاحظه است که مشتمل بر کلیه اشتراکات کلیدی شناسایی شده وفق طبقه‌بندی جدید پیشنهادی (یعنی بازیگر، انگیزه، قصد، وسیله، اثر و هدف) است. این رویکرد نوین برای تعریف جرائم دیجیتالی درک مشترکی از تهدید گسترده‌تر برای استانداردسازی سیاست، همکاری جهانی و تحقیقات ارائه می‌کند (Plotnek and Slay, 2021: 136-137)، در حالی که اجازه می‌دهد زیرمجموعه‌های منحصربه‌فردی از این شاخه از جرائم دیجیتالی برای کاربردهای قانونی یا تخصصی خاص تعریف شود.

۲. پاسخ‌های ملی در چارچوب ظرفیت‌های قانون‌گذاری

۲-۱. جرم‌انگاری‌ها

با توجه به شرایط حاکم در نظام قانون‌گذاری ایران و پاکستان و جرم‌انگاری رفتارها وفق ظرفیت‌های قانون‌گذاری در قبال جرائم دیجیتالی، در مقابله با جرائم موصوف در قلمرو نظام حقوقی هر دو کشور، شاخص‌های قانون‌گذار مورد مداقه قرار می‌گیرند.

۲-۱-۱. ایران

وجود مقرره‌های قانونی نظیر «قانون مجازات انتشار و افشای اسناد محرمانه و سری دولتی، مصوب ۱۳۵۳»، «قانون مجازات تبلیغ نژادی، مصوب ۱۳۵٦»، ماده ۲۳ تا ۳۴ «قانون مطبوعات، مصوب ۱۳٦۴»، مواد ۱۲ و ۱۳ «قانون حمایت از پدیدآورندگان نرم‌افزارهای رایانه‌ای، مصوب ۱۳۷۹»، مواد ۶۷ تا ۷۷ «قانون تجارت الکترونیکی، مصوب ۱۳۸۲»، «قانون مجازات جرائم نیروهای مسلح، مصوب ۱۳۸۲»، «لایحه حمایت از حریم خصوصی، مصوب ۱۳۸۴»، «قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیت‌های غیرمجاز می‌نمایند، مصوب ۱۳۸۶»، ماده ۲۲ «قانون انتشار و دسترسی آزاد به اطلاعات، مصوب ۱۳۸۸» و «قانون جرائم رایانه‌ای، مصوب ۱۳۸۸»، امکان مقابله با جرائم را در فضای دیجیتالی را فراهم می‌آورد.

اگرچه نحوه اجرای مبانی جرم‌انگاری در قلمرو قانون‌گذاری ارتباطی مستقیم با چارچوب سیاست کیفری دارد، اما دیدگاه‌های مبنایی دایر به سیاست جنایی، میزان اهمیت و تأثیر ارزش‌های اخلاقی و شرایط اجتماعی، سیاسی و اقتصادی در بیان مبانی محوریِ جرم‌انگاری در این چارچوب اثرگذار هستند. هر چه جرم‌انگاری وفق مطالعات و اندیشه‌های عمیق متکی باشد، نظام کیفری را کارآمدتر خواهد کرد و این امر مستلزم این است که گستره فرهنگی و اجتماعی این رویکرد در نظام قانون‌گذاری ایران ایجاد شود (علمداری، فرجی‌ها، ۱۳۹۶: ۱٦۵- ۱۸۷). آنچه در این بین مورد اهتمام قانون‌گذار جهت رویارویی با جرائم ارتکابی در فضای دیجیتالی است اینکه در نظام حقوقی ایران و منطبق بر «قانون جرائم رایانه‌ای، مصوب ۱۳۸۸» مصادیقی نظیر جعل، جاسوسی، سرقت نرم‌افزار، نشر اکاذیب و هتک حیثیت، شنود غیرمجاز محتوای ارتباطات غیرعمومی، انتشار، تولید و یا در دسترس قرار دادن غیرقانونی گذرواژه یا داده‌ها، سرقت خدمات، مزاحمت اینترنتی، توهین به مقدسات مذهبی در فضای مجازی، انتشار محتویات غیراخلاقی، خراب‌کاری، دسترسی غیرمجاز به دستگاه‌های پردازش داده و...، به‌عنوان جرائم قابل ارتکاب مورد تقریر قرار گرفته است. این در حالی است که قانون‌گذار ایران در چارچوب قانون جرائم رایانه‌ای، مبادرت ایجاد و توسعه مسئولیت کیفری از طریق جرم‌انگاری اقدام‌های ناهنجار در فضای دیجیتالی می‌کند.

بهره‌گیری از سازوکارهای حل اختلاف و حتی بهره‌گیری از کیفرهای نوین به‌عنوان اقدامی مؤثر در احراز و تفکیک مسئولیت کیفری میان اشخاص حقیقی و حقوقی به شمار می‌رود. لازم به ذکر است قانون‌گذار ماده ۱۹ و ۲۰ در فصل ششم از قانون اخیرالذکر و ماده ۱۴۳ قانون مجازات اسلامی مصوب ۱۳۹۲ را به موضوع مسئولیت کیفری اختصاص داده است که به‌عنوان مهم‌ترین تغییری که این قانون در خصوص مسئولیت کیفری ایجاد نموده است. نکته حائز اهمیت، آیا رویه قانون‌گذار ایران بر این بوده که اصل را بر مسئولیت کیفری اشخاص حقوقی قرار دهد؟ یا به دنبال نفی مسئولیت کیفری اشخاص حقیقی در محیط دیجیتالی بوده است؟ در پاسخ باید اذعان داشت نظر به تبصره دوم از ماده ۱۹، موضوع به معنای نفی مسئولیت کیفری اشخاص حقیقی نیست. قانون‌گذار ایران در قانون جرائم رایانه‌ای اشاره‌ای به عوامل رافع مسئولیت کیفری ننموده است بند «ب» ماده ۱۹ اشاره به دستور مدیر و نقش این دستور در ارتکاب جرم دارد که این امر اشاره به علل موجه جرم دارد، نه عوامل رافع مسئولیت کیفری (رضوی‌فرد، موسوی، ۱۳۹۵: ۳۲).

لازم به ذکر است برای رسیدگی به جرائم دیجیتال در قلمرو حاکمیتی ایران ضرورت دارد تا صلاحیت کیفری محاکم را وفق مقررات کیفری ماهوی و شکلی در دو معیار قواعد معمول مشتمل بر صلاحیت سرزمینی (مواد ۶۴۴ و ۶۵۵ قانون آیین دادرسی کیفری (مصوب ۱۳۹۲)، صلاحیت حمایتی (ماده ۵ قانون مجازات اسلامی، مصوب ۱۳۹۵ و بند «پ» ماده ۶۴۴ قانون آیین دادرسی کیفری)، صلاحیت جهانی (ماده ۹ قانون مجازات اسلامی) و صلاحیت دائر به تابعیت متهم و بزه‌دیده (مواد ۷ و ۸ قانون مجازات اسلامی و بند «ت» «ماده ۶۴۴ قانون آیین دادرسی کیفری) و معیار کیفی جرم مشتمل بر صلاحیت مرجع محل بارگذاری و یا پیاده‌سازی وفق بند «ب» ماده ۶۴۴ قانون آیین دادرسی کیفری، مورد مداقه قرار داد. برآیند اینکه گرچه با توجه به معیارهای مورد بحث تعیین مرجع ذیصلاح قضایی در رسیدگیِ جرائم دیجیتال به‌نحوی قابل تحقق است، اما همچنان در مواردی نظیر عدم دسترسی به متهم در قلمرو حاکمیتی یا ارتکاب جرم خارج از قلمرو حاکمیتی وجود دارند که در این زمینه‌ها باید از همکاری‌های بین‌المللی میان ایران و سایر کشورها بهره گرفت (همان: ۹۴-۸۸).

۲-۱-۲. پاکستان

پاکستان تلاش‌هایی را برای دیجیتالی کردن نه‌تنها بخش عمومی انجام داده است، بلکه چندین اقدام برای تسهیل رونق دیجیتال در بخش خصوصی نیز آغاز شده است. این در حالی است که قانون‌گذار پاکستان با توجه به شرایط فراسرزمینی ارتکاب جرائم دیجیتالی در قلمرو سرزمینی و نیز عنایت به مقررات داخلی که بخشی از آن برگرفته از اسناد بین‌المللی است این امکان را در جهت پاسخ‌گذاری و واکنش به این نوع از جرائم در سطوح گوناگون ملی و بین‌المللی دارد؛ علی‌رغم اینکه وضعیت کنونی پاکستان در خصوص مقابله با جرائم دیجیتالی با چالش‌های جدید مواجه است.

به‌منظور پیشگیری و مقابله با این جنایتکاران، پاکستان مرکز ملی واکنش به جرائم دیجیتالی[۱] (National Response Center for Cyber Crime) را برای نظارت، ردیابی و دستگیری مرتکبان جرائم دیجیتالی ایجاد کرد. مرکز ملی واکنش به جرائم دیجیتالی نقطه تماس واحدی را برای همه سازمان‌های داخلی و خارجی برای جرائم دیجیتالی در پاکستان فراهم می‌کند. در کنار برگزاری نشست‌ها و کارگاه‌های آموزشی به‌منظور آموزش کاربران در برابر حملات دیجیتالی به منابع اطلاعاتی، نفوذ اطلاعات و ایمن‌سازی سامانه‌ها در قبال این‌گونه تهدیدها، آموزش‌ها و آموزش‌های امنیتی مرتبط را به سازمان‌های دولتی و غیردولتی و بخش خصوصی می‌دهد (Jamil, 2006: 32-33). با ادامه پیشرفت فناوری، نیاز به قوانین و مقررات حاکم بر فعالیت‌های دیجیتالی اهمیت فزاینده‌ای پیدا می‌کند. حقوق دیجیتالی یک جزء حیاتی از چارچوب‌های قانونی است که هدف آن پیشگیری از جرائم دیجیتالی و تنظیم فعالیت‌های برخط با استفاده از منابع رایانه‌ای است. در پاکستان، دولت گام‌های مهمی برای رفع این نگرانی‌ها با وضع مقررات دیجیتالی ضروری برای تضمین ایمنی و امنیت شهروندانش در حین انجام فعالیت‌های برخط برداشته است.

---

۱. به آدرس زیر مراجعه شود: https://www.nr3c.gov.pk

اولین قانون در پاکستان برای کنترل و پیشگیری از این‌گونه جنایات به‌عنوان «قانون معاملات الکترونیکی» (Electronic Transaction Act in 1996)[۱] در سال ۱۹۹۶ به تصویب رسید.[۲] «فرمان معاملات الکترونیکی» (Electronic Transactions Ordinance, 2002)[۳] در سال ۲۰۰۲ به اجرا درآمد؛ این اقدام نقش اساسی در ایجاد یک پایه قانونی محکم برای امضاها و سوابق الکترونیکی داشت. علاوه‌بر این، دولت فدرال باید حفاظت از داده‌ها و دستورالعمل‌های حریم خصوصی کاربر را مشخص کند «قانون جرائم الکترونیکی»، در سال ۲۰۰۴ با رعایت مفاد آیین‌نامه معاملات الکترونیکی به تصویب رساند. در این قانون، جرائم مختلف در فضای مجازی به‌عنوان جرائم دیجیتالی معرفی شد. طبق قانون جرائم الکترونیکی سال ۲۰۰۴، جرائم دیجیتالی طیف گسترده‌ای از فعالیت‌های غیرمجاز مانند رهگیری، ردیابی دیجیتالی، هرزنامه، جعل و دسترسی غیرمجاز را تحت شمول قرار داد. «مقررات پیشگیری از جرائم الکترونیکی» (Prevention of Electronic Crimes Ordinance, 2007)[٤] طی سال ۲۰۰۷ تصویب شد، اما در سال ۲۰۱۰ لغو شد. وفق این قانون، پرونده‌ها توسط آژانس تحقیقات فدرال پاکستان با اشاره به جعل حساب‌ها، کلاهبرداری دیجیتالی بررسی می‌شد.

---

۱ به آدرس زیر مراجعه شود:

https://www.na.gov.pk/uploads/documents/1329727963_180.pdf

۲ لازم به‌ذکر است که قانون تلگراف (Telegraph Act, 1885) باید برای در نظر گرفتن آخرین پیشرفت‌های فناوری بازنگری شود. دولت به نام منافع عمومی و بدون دخالت دادگاه‌ها اختیارات نامحدودی را اعمال می‌کند .در صورت وضعیت اضطراری ملی یا به خاطر امنیت عمومی، دولت می‌تواند کنترل تلگراف را به دست گیرد. علاوه بر این، ورود به دفاتر تلگراف بدون مجوز قانونی و تداخل در پیام‌های تلگراف، جرمی جدی است که کیفر قانونی دارد. «قانون مخابرات پاکستان (Pakistan Telecommunications "Re-Organization" Act, 1996)» ضروری است که هرگونه ارتباط غیرمجاز به سرعت از طریق اداره مخابرات یا هیأت تخصیص فرکانس طبق مفاد این قانون به دادگاه گزارش شود. دادگاه دارای صلاحیت صدور حکم تفتیش است که امکان جستجوی مکان‌هایی را که گمان می‌رود جنایات در آنها رخ داده است را فراهم می‌کند .مقامات مجری قانون قدرت توقیف تجهیزات مورد استفاده برای فعالیت‌های مجرمانه و انجام تحقیقات کامل را دارند (Saleem, Junaid Jan, Areej, 2022: 7).

۳ به آدرس زیر مراجعه شود:

https://khalidzafar.com/laws-of-pakistan/electronic-transaction-ordinance-2002/

٤ به آدرس زیر مراجعه شود:

http://pklegal.org/pdf/Prevention-of-Electronic-Crimes-Ordinance-2007-(PECO2007).pdf

علاوه‌بر مقررات فوق‌الذکر، کابینه فدرال در ۱۷ ژانویه ۲۰۰۷ لایحه پیشگیری از جرائم الکترونیکی (Prevention of Electronic Crimes Bill, 2007)[1] را تصویب کرد. قانون پیشنهادی با عنوان لایحه پیشگیری از جرائم الکترونیکی ۲۰۰۷ کیفرهای از شش ماه حبس تا کیفر اعدام را برای هفده نوع جرم دیجیتالی ارائه می‌کند؛ ازجمله جرائم دیجیتالی، هک وب‌گاه‌ها و دسترسی مجرمانه به داده‌های امن (Jamil, 2006: 39-40). با جرائم دیجیتالی، دسترسی مجرمانه، دسترسی به داده‌های مجرمانه، تقلب الکترونیکی آسیب به داده‌ها، جعل الکترونیکی، سوءاستفاده از سامانه الکترونیکی، دسترسی غیرمجاز به کد، سوءاستفاده از رمزگذاری، سوءاستفاده از کد، تعقیب دیجیتالی سروکار دارد و کیفر سختی را برای این افراد پیشنهاد می‌کند (Kundi et al, 2012: 51-53).

می‌توان به قانون جدیدی را با عنوان «قانون پیشگیری از جرائم الکترونیکی» که در سال ۲۰۱۴ برای تصویب به دولت وقت ارائه شده بود، اشاره داشت که کیفرهای تهاجمی و سرکوب‌گرانه‌ای را برای جرائم دیجیتالی پیشنهاد می‌کرد. مقررات مزبور شامل جرائم دیجیتالی، شنود غیرمجاز، دسترسی غیرقانونی به سامانه و برنامه یا داده‌های اطلاعاتی، مداخله غیرقانونی در برنامه یا داده‌ها، جعل الکترونیکی، جرم هویت و حمایت از زنان و غیره می‌شود.

قانون‌گذار پاکستان طی سال ۲۰۱۶ مبادرت به تصویب «قانون پیشگیری از جرائم الکترونیکی» (The Prevention of Electronic Crimes Act, 2016)[2] نمود. این قانون مشتمل بر طیف گسترده‌ای از جرائم نظیر جعل دیجیتالی، جعل دیجیتالی، فیشینگ، آزار و اذیت دیجیتالی، دسترسی غیرقانونی به سامانه‌های اطلاعاتی، دسترسی غیرقانونی به داده‌ها یا اطلاعات، مداخله غیرقانونی با داده‌ها یا سامانه‌های اطلاعاتی، جرائم دیجیتالی، توهین به مقدسات و جعل دیجیتالی است (Saleem, Junaid Jan, Areej, 2022: 8). قانون اخیر به استفاده دفاعی از فضای دیجیتالی درزمینهٔ «جنگ ترکیبی»[3] اشاره دارد. این در حالی است که

---

۱ به آدرس زیر مراجعه شود:
http://pklegal.org/pdf/Prevention-of-Electronic-Crimes-Ordinance-2007-(PECO2007).pdf

۲ به آدرس زیر مراجعه شود:
https://www.na.gov.pk/uploads/documents/1470910659_707.pdf

3 Hybrid Warfare

«سیاست امنیت ملی ۲۰۲۶-۲۰۲۲» (National Security Policy (NSP) 2022-2026)[۱] بر اهمیت دفاع در جنگ ترکیبی درزمینهٔ انتشار اطلاعات نادرست یا اطلاعات علیه منافع دولت تأکید دارد.[۲]

طی سال ۲۰۰۰، دولت پاکستان «سیاست ملی فناوری اطلاعات و برنامه اقدام» (National Information Technology Policy and Action Plan, 2000)[۳] را تصویب و اجرا کرد.[٤] هدف از سیاست مزبور ایجاد قوانینی برای مقابله با جرائم دیجیتالی بود. پس از بررسی چارچوب‌های حقوقی کشورهای مختلف حقوق عمومی و قانون مدنی، این سیاست بر اساس مقررات نمونه آنسیترال تدوین شد. ضمن تضمین توسعه سیاست‌ها و برنامه‌های اقدام فناوری اطلاعات، ایمنی داده‌های فردی، از یکپارچگی تجارت الکترونیک محافظت می‌کند. اذعان می‌شود این قانون سیاستی متناسب و مؤثر در تأمین امنیت فضای دیجیتالی بود. این در حالی است که با توجه به تحولات فزاینده در فضای دیجیتالی و ضرورت پاسخ به جرائم ارتکابی در این فضا و وجود چالش‌های امنیتی در سکوهای دیجیتالی در فضای حکمرانی دیجیتالی پاکستان، «سیاست ملی امنیت سایبری» (National Cybersecurity Policy 2021)[٥] را در سال ۲۰۲۱ تصویب کرد. با کمک این سیاست یک چارچوب ملی واکنش امنیت دیجیتالی ایجاد می‌شود. دولت کمیته «سیاست حکمرانی سایبری» را برای اجرای این سیاست تشکیل داده است (Asif Khan, 2023: 14-16). طبق این سیاست هرگونه حمله سایبری به هر یک از سازمان‌های پاکستانی یک اقدام تهاجمی علیه دولت به حساب می‌آید و کلیه سازوکارهای لازم برای مقابله با آن اتخاذ می‌شود. کمیته «سیاست‌های حکمرانی سایبری»

---

۱ به آدرس زیر مراجعه شود:
https://nsd.gov.pk/SiteImage/Misc/files/NSP%20summary.pdf

۲ اصطلاح جنگ ترکیبی به مداخله در سامانه‌های اطلاعاتی برای تضعیف و هدف قرار دادن امنیت ملی از طریق ترویج اطلاعات ضد دولتی اطلاق می‌شود.

۳ برای اطلاع از محتوای این سیاست به آدرس زیر مراجعه شود:
https://lgkp.gov.pk/wp-content/uploads/2014/03/National-IT-Policy.pdf

٤ به آدرس زیر مراجعه شود:
https://moib.gov.pk/Downloads/Policy/DIGITAL_PAKISTAN_POLICY%2822-05-2018%29.pdf

٥ به آدرس زیر مراجعه شود:
https://issra.pk/images/issra/01-Insight-Cyber-Security.pdf

موظف است سیاست مذکور را در سطح ملی اجرا و راهبرد مناسب را تعیین کند و اقدام لازم را در زمان مناسب انجام دهد.

۲-۲. پاسخ‌گذاری‌ها

آنچه در این بخش مورد مداقه قرار خواهد گرفت مطالعه پاسخ‌های حقوقی و فنی قابل اجرا در پاسخ به جرائم دیجیتالی در قلمرو مقررات مصوب ایران و پاکستان است که با اتخاذ ظرفیت‌های حقوقی امکان مقابله با چنین جرائمی فراهم می‌گردد؛ هرچند با وجود وضع مقررات متنوع و کثیر، چالش‌ها و تهدیدهای ناشی از ارتکاب جرائم در فضای دیجیتالی به‌مثابه امری گریزناپذیر قابل ملاحظه است.

۲-۲-۱. ایران

نظام حقوقی در راستای شناسایی و راهبردی مطلوب بسترهای موجود در فضای دیجیتالی و برای مقابله مطلوب با جرائم ارتکابی در فضای دیجیتالی افزون بر مقررات مصوب، درصدد ایجاد ساختار و سازوکارهایی برآمد. بر این اساس، می‌توان به «سند راهبردی جامع فناوری اطلاعات جمهوری اسلامی ایران، مصوب ۱۳۸۸» اشاره نمود که به نحوی مبادرت به ارائه تعریفی از فناوری اطلاعات نموده است. پس از این شورای عالی فضای مجازی کشور مصوبه‌ای را با موضوع «توسعه فضای مجازی سالم، مفید و ایمن» در سال ۱۳۹۴ ابلاغ کرد که هدف آن ایجاد و توسعه داوطلبانه، مشارکتی و قابل مدیریت «فضای مجازی سالم، مفید و ایمن» در راستای «تولید و توزیع محتوا و خدمات سالم، مفید و ایمن مورد نیاز»، «ممانعت از نشر محتوا و خدمات مضر و ناسالم و ناایمن» و «طرح جامع توسعه فضای مجازی سالم، مفید و ایمن» بود. در این راستا باید اظهار داشت که تعریف ارائه شده از فضای ایمن در مصوبه اخیر، مقصود فضای ایمن محتوایی منطبق بر ساختار مبانی اسلامی بوده است. شورا در راستای انسجام‌بخش به فضای دیجیتالی در سال‌های متمادی مبادرت ابلاغ مصوبه‌هایی نظیر «طرح‌های کلان مرکز ملی فضای مجازی کشور جهت تدوین لایحه بودجه، مصوب ۱۳۹۲»، «سیاست‌های ساماندهی خدمات پیامکی ارزش‌افزوده و پیامک انبوه در شبکه‌های ارتباطی، مصوب ۱۳۹۳» و «سیاست‌ها و اقدامات ساماندهی پیام‌رسان‌های اجتماعی، مصوب ۱۳۹۶» نمود (وطنی و اسدی، ۱۳۹۵: ۱۲۱-۱۱۱).

افزون بر مصوبه‌های شورای عالی فضای مجازی، شورای عالی انقلاب فرهنگی، «مقررات و ضوابط شبکه‌های اطلاع‌رسانی رایانه‌ای، مصوب ۱۳۸۰» پیرو تصویب و ابلاغ «سیاست‌های کلی شبکه‌های اطلاع‌رسانی رایانه‌ای» طی سال ۱۳۸۰، ابلاغ کرد. لازم به ذکر است که «آیین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیکی» در اجرای ماده ۵۴ قانون جرائم رایانه‌ای، به پیشنهاد وزیر دادگستری از سوی قوه قضائیه در سال ۱۳۹۳ به تصویب رسید. به‌رغم وجود ظرفیت‌ها، پاسخ‌های متعدد قابل اتخاذ در نیل به اهداف سالم‌سازی، فضای حاکم در سکوهای دیجیتالی از محتواهای مجرمانه مورد غفلت جدی قرار گرفته است که در راستای اصلاح چنین وضعیتی ضرورت دارد تا با احصای معیارهای مقرر در بستر این سکوها به‌عنوان یک رسانه، الزامات سالم‌سازی آن‌ها و انواع سازوکارهای عملیاتی که امکان هماهنگی با تحولات موجود را دارند با کمک جوامع مدنی و سازمان‌های مردم‌نهاد چارچوب‌بندی کرد (نظری و همکاران، ۱۴۰۰: ۱۷۲).

ساختار نظام حقوقی ایران برای پیشگیری از جرائم دیجیتالی، برخی سازوکارها را نظیر «پالایش محتوا» و «تدابیر نظارتی» به‌عنوان پیشگیری وضعی و برخی را نظیر «تدابیر آموزشی-آگاهی‌بخش» و «تدابیر تربیتی‌پرورشی» به‌عنوان پیشگیری اجتماعی، مقرر ساخته است. یافته‌های حاصل از مطالعات پژوهشگران مؤید آن است که پالایش محتوا به شیوه جاری، به‌عنوان رایج‌ترین سازوکار در چارچوب پیشگیری از جرم، «غیرعادلانه»، «غیرعلمی» و «غیراقتصادی» است؛ چه آنکه با حق‌های بنیادین شهروندان ازجمله حق آزادی، حق برابری و حق امنیت مغایرت دارد و با رهیافت‌های دانش جرم‌شناسی نیز انطباق ندارد و علی‌رغم صرف هزینه‌های فراوان، کارایی و اثربخشی لازم را ندارد. فراتر از این، کاربستِ روبه تزاید پالایش محتوا به شیوه جاری، موجب «عمومی شدن جرم» «بزه‌کاری مضاعف نوجوانان» و «افزایش احتمال بزه‌دیدگی» شده است. با توجه به اشکالات و نواقص پیشگیری از جرائم ارتکابی در ایران، پژوهشگران سازوکارهای پیشنهادی قابل اتکایی را در مقابله با این نوع از جرائم ارائه کرده‌اند که بر این اساس با تعدیل سیاست فیلترینگ به شیوه جاری و ارتقای «سواد امنیت دیجیتالی» شهروندان، تدابیر اجرایی پیشگیری از جرم در یک الگوی «علت‌مدار»، «حق‌مدار»، «جامعه‌مدار»، «ایجابی» و «ریزومیک» تنظیم شود تا شهروندان

فضای مجازی، متناسب با علل و عوامل جرم، به صورت افقی، موضوع پیشگیری را به مثابه یک حق (حقِ مشارکتِ فرهنگی) دنبال نمایند (سلیمی، ۱۳۹۷: ۵).

۲-۲-۲. پاکستان

با توجه به این‌که پاکستان هنوز با مشکلات متعددی نظیر فساد، فقر، فقدان رشد فناورانه و ساختار حاکمیتی ناامن، دست‌وپنجه نرم می‌کند، این امر موجب شده تا مشکلات متعددی را برای امنیت داخلی سازمان ایجاد کند. سازمان‌های مجری قانون پاکستان با موانع متعدد و پیچیده‌ای در مقابله با جرائم دیجیتالی روبه‌رو هستند (Zia UL Islam et al, 2019). در پاکستان تلاش‌های متعددی در سطح داخلی و بین‌المللی صورت پذیرفت، اما این مقررات مصوب همچنان دارای نواقصی است. آنچه در پاکستان جرم محسوب می‌شود ممکن است در سایر کشورها جرم تلقی نشود. این امر همیشه آزادی مرتکبان جرائم دیجیتالی را پس از دستگیری تسهیل بخشیده و رسیدگی و پیشگیری از جرائم و مرتکبان را برای دیگری دشوار کرده است. در پاکستان، ظاهراً قانونی که برای محافظت از جامعه برخط در قبال جرائم دیجیتالی در نظر گرفته شده است، نمی‌تواند از مسائل غیرتجاری ازجمله ارتباطات و عقیدتی افراطی که در فضای دیجیتالی ایجاد می‌شوند، محافظت کند. در پاکستان فعالیت‌های افراطی در رسانه‌های اجتماعی برای برهم زدن حاکمیت، یکپارچگی و اعتبار افراد و نهادها ارتکاب می‌یابد، این امر مستلزم قانون‌گذاری فشرده علیه افراط‌گرایی دیجیتالی و سایر رفتارهای خشونت‌آمیز و ارتباط آن با جامعه بین‌المللی است (نمامیان، ۱۴۰۳: ۲۲۲-۲۲۱).

آموزش و سواد رسانه‌ای می‌تواند از جرائم دیجیتالی به نحو مطلوبی پیشگیری کند. آموزش نحوه بهره‌گیری از سامانه‌های اطلاعاتی و نحوه پیشگیری یا محافظت از مرتکبان جرائم در فضای دیجیتالی ضرورتی است که کاربران باید رایج‌ترین هک را درک کنند. افزون بر این، آموزش و آگاهی کاربران برخط در سراسر کشور باید راه طولانی را برای محافظت از آن‌ها در قبال بسیاری از انواع جرائم دیجیتالی انجام دهد؛ زیرا معرفی فناوری جدید نه‌تنها در مورد استفاده از سامانه‌های جدید بلکه به حقوق، وظایف و مسئولیت‌های مرتبط با ماشین‌های جدید نیاز به آموزش و آگاهی دارد.

به‌طور مشابه، مقررات حاکم بر سامانه‌های الکترونیکی باید به‌طور گسترده منتشر شوند تا کاربر از مقررات و اقدام‌های تنظیم‌کننده جرائم دیجیتالی و اقدام‌هایی که توسط دولت‌های خود در سطح بین‌المللی معرفی شده است، آگاه شود. نظام تحقیقاتی ضعیف و محافظه‌کارانه نیز مانعی در برابر امنیت الکترونیکی است؛ زیرا عدم صلاحیت حرفه‌ای و مداخله سیاسی در ثبت پرونده‌های حقوقی، نظام تحقیق و اطاله دادرسی و تشریفات دست و پاگیر در نظام قضایی پاکستان، اجرای عدالت را به تأخیر می‌اندازد و درنتیجه اجرای صحیح مقررات را با چالش مواجه می‌کند.

یکی دیگر از ابزارهای سرکوب جرائم دیجیتالی، هماهنگی در همکاری‌ها در چارچوب حقوق بین‌المللی است. این برای مرتکبان جرائم دیجیتالی و با انگیزه طمع صدق می‌کند. تنها با آموزش نمی‌توان با آن‌ها مبارزه کرد؛ زیرا آن‌ها از پیش مجرمانی شناخته شده هستند. تنها راه مناسب برای مبارزه، تصویب مقررات جدید، هماهنگی در همکاری‌ها در چارچوب حقوق بین‌المللی و تشویق هماهنگی و همکاری بین سازمان‌های مجری مقررات ملی و جامعه بین‌المللی است؛ اگرچه حقوق دیجیتالی تا حدودی در قلمرو حاکمیتی پاکستان وجود دارد، اما عدم تطابق و عدم هماهنگی آن‌ها با نهادهای بین‌المللی مجری حقوق دیجیتالی بزرگ‌ترین چالش برای پیشگیری از وقوع جرائم دیجیتالی است؛ زیرا در اکثر موارد مجرمان مرتکب این جرائم می‌شوند.

۳. ظرفیت‌سنجی اسناد بین‌المللی فضای دیجیتالی در قلمرو قانون‌گذاری ایران و پاکستان

در تلاقی فناوری و بشریت، مفهوم «حقوق دیجیتال» پدیدار می‌شود. این حقوق در عصر دیجیتال به‌عنوان حافظ آزادی‌های بشر در فضای وسیع دیجیتالی عمل می‌کند. حقوق دیجیتال به‌مثابه سازوکاری است که حقوق بشر سنتی را با پیچیدگی‌های فضای برخط پیوند می‌دهد و تضمین می‌کند که تعاملات دیجیتالی، تصمیم‌گیری‌ها و هویت‌های بشر با همان احترام و حمایتی که در دنیای فیزیکی وجود دارد، رفتار می‌شود. این شاخه از حقوق نه‌تنها حفاظت از حریم خصوصی و امنیت را تضمین می‌کند، بلکه آزادی بیان، دسترسی

برابر به فناوری و عدم تبعیض را ارتقا می‌دهد (ر.ک: فضائلی و همکاران، ۱۳۹۸: ۸۷). در چارچوب یک جامعه دیجیتالی فزاینده، شناسایی و حمایت از این حقوق ضرورتی انکارناپذیر است.[۱]

لازم به ذکر است ماده نخست کنوانسیون مونترال (کنوانسیون در مورد سرکوب اعمال غیرقانونی علیه ایمنی هواپیمایی کشوری) جرائم را در چارچوب اجرای کنوانسیون تعریف کرده است. برخی کشورها طی ژرف‌اندیشی در مورد پیش‌نویس کنوانسیون، رویکرد برشمردن را ترجیح می‌دادند که تعداد محدودی از جرائم خاص را فهرست می‌کرد؛ در حالی که سایرین طرفدار یک تعریف عمومی بودند. در سال ۲۰۰۱ شورای اروپا «کنوانسیون جرم سایبری» را تصویب کرد. هدف اصلی کنوانسیون جرم سایبری، پیگیری یک سیاست کیفری هماهنگ و مشترک با هدف حفاظت از جامعه در برابر جرم سایبری، به ویژه با به‌کارگیری قانون‌گذاری مناسب و تقویت همکاری بین‌المللی است.

با توسعه و گسترش سریع اینترنت در آغاز این قرن، قانون‌گذاران در سراسر جهان در قبال خلأ قانونی که با مقررات قانونی موجود قابل رفع نبود، لازم بود حوزه دیجیتال را با حقوق و مقررات ملی خاص تنظیم کنند. به‌عنوان نمونه، «قانون اجرای شبکه»[۲] در آلمان و «قانون مبارزه با نفرت در اینترنت»[۳] در فرانسه به تصویب رسید که هر دو وظیفه بحث‌برانگیز سکوهای برخط برای حذف محتوای غیرقانونی خاص را تدوین می‌کنند. در عین حال، اتحادیه اروپا در حال کار بر روی یک قانون خدمات دیجیتال پس از تصویب «مقررات عمومی حفاظت از داده‌ها»[٤] است و از سال ۲۰۱۸ اجرا شده است. در یک اقدام مهم، در ژانویه ۲۰۲۲، پارلمان و شورای اتحادیه اروپا در مورد «اعلامیه اروپایی حقوق دیجیتال و اصول برای دهه دیجیتال»[٥] به توافق رسیدند.

---

۱ به آدرس زیر مراجعه شود:

https://www.un.org/techenvoy/content/digital-human-rights

۲ به آدرس زیر مراجعه شود:

Netzwerkdurchsetzungsgesetz of 1 September 2017 (BGBl.I p. 3352), which was changed by Article 274 of the Decree of 19 June 2020 (BGBl.I p. 1328).

۳ به آدرس زیر مراجعه شود:

Assemblée nationale, proposition de loi visant à lutter contre les contenus haineux sur internet, loi n° 2020–766 de 24 juin 2020.

٤ به آدرس زیر مراجعه شود:

https://dig ital-strategy.ec.europa.eu/.

٥ به آدرس زیر مراجعه شود:

این بیانیه نشان دهنده تعهد مشترک نهادهای اروپایی برای ایجاد چارچوبی است که از حقوق دیجیتالی شهروندان اتحادیه اروپا حمایت و ترویج می‌کند.[۱] در ۲۹ آوریل ۲۰۲۱، اتحادیه اروپا مقررات ۲۰۲۱/۷۸۴ را در خصوص رسیدگی به انتشار محتوای تروریستی برخط به‌عنوان یکی از مصادیق «آسیب‌های برخط» تصویب کرد.[۲]

طی سال‌های اخیر مجمع عمومی سازمان ملل متحد طی سال ۲۰۲۱، برای تدوین کنوانسیون بین‌المللی جامع مبارزه با بهره‌گیری از فناوری اطلاعات و ارتباطات برای اهداف مجرمانه اولین جلسه سازمانی خود را برگزار کرد. هدف از تهیه پیش‌نویس مزبور «تقویت همکاری‌های بین‌المللی برای مبارزه با برخی جرائم ارتکابی از طریق سامانه‌های فناوری اطلاعات و ارتباطات و به اشتراک‌گذاری مدارک به‌صورت الکترونیکی جرائم جدی» و با هدف نهایی تهیه «پیش‌نویس کنوانسیون سازمان ملل متحد علیه جرائم سایبری» (Draft United Nations Convention against Cybercrime)[۳] بود که درنهایت به دلایل فنی و حقوقی تاکنون سند مزبور به لحاظ تقریر متن نهایی و تصویب نشده است. پیش‌نویس کنوانسیون سازمان ملل متحد علیه جرائم سایبری که با هدف پیشگیری و مقابله با جرائم سایبری پایه‌ریزی شده و برای آینده اینترنت، حقوق بشر، آزادی‌های دیجیتال و مسیر آتی همکاری بین‌المللی و چندجانبه‌گرایی اهمیت اساسی دارد؛ به دیگر تعبیر، پیش‌نویس پیشنهادی که در اصل، هدف آن بهبود همکاری بین‌المللی برای پیشگیری و مقابله با جرائم

---

https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles

۱ در حال حاضر، فناوری‌های دیجیتالی حیات بشر را به شدت تغییر داده است. به‌طور تقریبی هر حوزه از روابط اجتماعی در حال حاضر هم در سطح ملی و هم در سطح بین‌المللی در حال دیجیتالی شدن است. شورای امنیت سازمان ملل متحد در قطعنامه‌های ۲۴۱۹ (۲۰۱۸)، ۲۴۶۲ (۲۰۱۹) و ۲۴۹۰ (۲۰۱۹) اذعان دارد که فعالیت افراد و نهادهای غیردولتی در حوزه دیجیتال ممکن است تهدیدی برای صلح بین‌المللی و نیز موجبات نقض امنیت را در حملات دیجیتال به زیرساخت‌های حیاتی؛ عدم امکان استفاده از نظام‌های پرداخت برخط، انسداد دسترسی به اینترنت، حساب‌های توییتر و اینستاگرام فراهم نماید.

۲ به آدرس زیر مراجعه شود:

Defined in: Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on Addressing the Dissemination of Terrorist Content Online (O.J. L 172, 17 March 2021, p. 79) [hereinafter 'Regulation (EU) 2021/784'], Article 2 (1).

۳ به آدرس زیر مراجعه شود:

UN General Assembly, A/AC.291/L.16, New York, 29 July–9 August 2024, 7 August 2024, https://documents.un.org/doc/undoc/gen/v24/055/48/pdf/v2405548.pdf

ارتکابی در سکوهای دیجیتالی بود، اکنون به یک ابزار برای اعمال نظارت‌های گسترده، تضعیف آزادی بیان، نقض حریم خصوصی و سایر استانداردهای حقوق بشر تبدیل شده و تهدیدهایی برای تحقیقات ملی و بین‌المللی را ایجاد کرده است (Falchetta, 2024: 1).[1]

نشست اخیر مذاکرات در ۹ فوریه ۲۰۲۴ راجع‌به پیش‌نویس در حالی به پایان رسید که دولت‌های عضو نتوانستند در خصوص ابعاد اساسی آن به اجماع برسند و روند مذاکرات به ژوئیه ۲۰۲۴ موکول شد.[2] شایسته است که دولت‌های مذاکره‌کننده پیش از تصویب متن پیش‌نویس، اطمینان حاصل کنند که متن پیشنهادی، صرفاً بر مقابله با جرائم دیجیتالی متمرکز است و پادمان‌های حقوق بشری را تهدید نمی‌کند. مادام که در کاستی‌های متن، تغییرات معناداری صورت نپذیرد، کنوانسیون مزبور نتیجه‌ای جز نقض حقوق بشر را به دنبال نخواهد داشت؛ هرچند مقابله با چنین جرائمی نباید منجر به تهدید یا نقض حقوق بشر شود (Ibid).

شورای امنیت سازمان ملل متحد در قطعنامه‌های ۲۴۱۹ (۲۰۱۸)، ۲۴۶۲ (۲۰۱۹) و ۲۴۹۰ (۲۰۱۹) اذعان دارد که فعالیت افراد و نهادهای غیردولتی در حوزه دیجیتال ممکن است تهدیدی برای صلح بین‌المللی و نیز موجبات نقض امنیت را در حملات دیجیتال به زیرساخت‌های حیاتی، عدم امکان استفاده از نظام‌های پرداخت برخط، انسداد دسترسی به اینترنت، حساب‌های توییتر و اینستاگرام فراهم نماید.

قانون‌گذار ایران و حتی پاکستان نسبت به اتخاذ رویکردی که امکان مقابله حداکثری با جرائم دیجیتالی را در قلمرو جامعه بین‌المللی با الحاق به اسناد و معاهدات جهانی ناظر به این پدیده فراهم آورد، غفلت ورزیده و تعلل قانون‌گذاران امکان ایجاد تهدید و چالش‌های موجود در فضای دیجیتالی را توسعه داده‌اند. این در حالی است که قانون‌گذار ایران و پاکستان در الحاق به برخی از اسناد معاهدات جهانی عامی که امکان مقابله با جرائم دیجیتالی در قلمرو حاکمیتی دولت‌های عضو را فراهم می‌کند، اقدام نموده‌اند. باید

---

۱ متن پیش‌نویس جرایمی نظیرسرقت یا کلاهبرداری مرتبط با رایانه (ماده ۱۲)، پول‌شویی عواید ناشی از جرم (ماده ۱۶) و مقرره‌ای با گستره بی‌پایان راجع‌به جرائم مقرردر سایر کنوانسیون‌های بین المللی و پروتکل‌های الحاقی قابل اجرا (ماده ۱۷) را مطرح کرده که دامنه این کنوانسیون را برخلاف اصول جرم‌انگاری، بسیار گسترش پیدا کرده است.

۲ به آدرس زیر مراجعه شود:

https://cpj.org/2024/02/as-negotiations-continue-the-proposed-un-cybercrime-convention-must-not-become-a-tool-to-undermine-press-freedom/amp/

تأکید داشت که در قلمرو قانون‌گذاری ایران و پاکستان به‌رغم وجود مقرره‌های قانونی متعدد و متکثر که امکان جرم‌انگاری را در ابعاد متنوع جرائم دیجیتالی را فراهم آورده است، اما نظریه تحولات فزاینده اطلاعات و فناوری‌های نوین در عرصه فضای دیجیتالی، امکان مقابله مطلوب و متناسب از طریق مقررات مصوب تاکنون حاصل نشده است که برای رفع شکاف‌های حقوقی ناشی از وجود چنین امری، الحاق به اسناد خاص در حوزه فضای دیجیتال ضرورتی انکارناپذیر است؛ چراکه پاسخ به جرمی جهانی از طریق معیارها و مقرره‌های داخلی، امکان سرکوب و پیشگیری را در ابعاد گوناگون دولت‌ها را با چالش‌هایی غیرقابل پیش‌بینی در قلمرو سرزمینی مواجه خواهد ساخت.[۱]

نتیجه‌گیری

جرائم دیجیتال و جرائم سنتی تسهیل شده توسط اینترنت یک پدیده مجرمانه جهانی است که تمایز متعارف بین تهدیدهای امنیت داخلی و خارجی نظیر جرائم، فعالیت‌های نظامی و امنیتی را مخدوش می‌کند. مسئولیت‌پذیری شبکه‌های برخط برای فعالیت برای اهداف مختلف و توانایی انتقال افراد از یک نوع فعالیت غیرقانونی به نوع دیگر، نشان می‌دهد که سرزمین‌گرایی مانع از تلاش‌ها برای مبارزه مؤثر با استفاده نادرست از فناوری می‌شود. اگرچه قانون‌گذار در ایران و پاکستان چندین گام را برای کنترل جرائم در فضای دیجیتالی آغاز کرده است، اما هنوز جای پیشرفت زیادی وجود دارد. نظام‌های حقوقی ایران و پاکستان تمایل حقوقی خود را به یافتن سازوکارهایی برای شناسایی فعالیت‌های فناورانه در بستر فضای دیجیتالی و جرم‌انگاری جرائم دیجیتالی با تصویب قوانینی در این منظر نشان داده‌اند.

علاوه‌بر این، برخی راهبردها و اقدام‌های عملی نیز برای مقابله با جرائم دیجیتالی در سیاست‌های اتخاذ شده در قلمرو نظام حقوقی هر دو کشور قابل ملاحظه است، اما ضرورت اتخاذ رویکردی پیشگیرانه در قبال

---

۱ دولت‌های ایران و پاکستان در راستای اهمیت توسعه همکاری‌های دو جانبه و بین‌المللی در زمینه مسائل امنیتی و مبارزه با جرائم سازمان یافته فراملی وافزایش نگرانی‌های ناشی از آن‌ها، در چارچوب بند هشتم ماده نخست از موافقتنامه همکاری‌های امنیتی بین دولت جمهوری اسلامی ایران و دولت جمهوری اسلامی پاکستان» مبادرت به همکاری درزمینه پیشگیری و مقابله با جرائم رایانه‌ای و سایر جرائمی که با سوءاستفاده از وسایل مخابراتی و ارتباطی صورت می‌گیرد، نمودند. لازم به ذکر است موافقتنامه مزبور از سوی مجلس شورای اسلامی در سال ۱۳۹۳ به‌تصویب رسید.

چنین جرائمی قابل ملاحظه است. به‌عنوان نمونه، قانون‌گذار ایران وفق قانون جرائم رایانه‌ای مبادرت به اتخاذ رویکردی تهاجمی و پیشگیرانه در سطور گوناگون قانونی در قبال ارتکاب جرائم دیجیتالی در ابعاد و گونه‌های متنوع آن شده است که با توجه به تحولات فزاینده فناوری‌ها تمرکز قانون‌گذار تنها معطوف به پاسخ‌گذاری در این چارچوب است که مقابله و پیشگیری متناسب به‌عنوان حلقه مفقوده در این فرایند قابل ملاحظه است. در پاکستان اجرای قانون نگهداری از داده‌های الکترونیکی ترافیک، یکی از ابعادی است که نیاز به توجه ویژه دارد؛ چراکه بیشتر بررسی‌ها به دلیل کمبود داده‌ها به بن‌بست می‌رسد و بررسی‌ها دچار نقصان می‌شود.

از آنجایی که نظام عدالت کیفری دیجیتالی در ایران و پاکستان مبتنی بر مقررات حاکم در فضای مجازی استوار است، تصمیمات دادگاه‌ها تنها می‌تواند برای تفسیر و روشن کردن ماهیت قانون مفید باشد. انتظار می‌رود کاربرد عملی قانون و تحقیقات بیشتر برای توسعه ساختار حقوقی و رفع ایرادات نظام حقوقی هر دو کشور قابل توجه باشد. به هر روی، افزون بر وضع قوانین و اقدام‌های مربوطه، قانون‌گذار ایران و پاکستان باید روابط چندجانبه با سایر کشورها را برای مقابله با تهدید برآمده از ارتکاب جرائم دیجیتالی را تقویت کند و در اینترنت جهت مقابله با هرگونه تهدید، احساس امنیت و مصونیت به کاربران فضای مجازی دهند. به همین ترتیب، یکی دیگر از موانع مهم در روند تحقیقات، موضوع صلاحیت قضایی و همکاری بین‌المللی است. تا مادمی که این مسائل در سطح بین‌المللی حل‌وفصل نشود، به نظر می‌رسد چالش‌ها همچنان مانع مبارزه با جرائم دیجیتالی باشد.

فهرست منابع

فضائلی، مصطفی؛ شکیب‌نژاد، احسان و کرمی، موسی (۱۳۹۸). «آزادی دینی در فضای مجازی و تأثیر آن بر صلح و امنیت بین‌المللی: با نگاهی به آموزه‌های اسلامی». **پژوهش تطبیقی حقوق اسلام و غرب**، شماره ۴.

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

دشتی، بیتا و افشاری، مریم (۱۳۹۸). «مطالعه تطبیقی جرائم سایبری در ایران و حقوق بین‌الملل». **پژوهشنامه حقوق تطبیقی**، شماره ۴.

رضوی‌فرد، بهزاد و موسوی، سید نعمت‌اله (۱۳۹۵). «مسئولیت کیفری در فضای سایبر در حقوق ایران». **پژوهش حقوق کیفری**، شماره ۱۶.

سلیمی، احسان (۱۳۹۷). **آسیب‌شناسی پیشگیری از جرائم سایبری در ایران**. رساله دوره دکتری حقوق جزا و جرم‌شناسی، دانشکده حقوق دانشگاه قم.

خرم‌آبادی، عبدالصمد (۱۳۸۴). **جرائم فناوری اطلاعات**. رساله دوره دکتری حقوق جزا و جرم‌شناسی، دانشکده حقوق و علوم سیاسی دانشگاه تهران.

علمداری، علی و فرجی‌ها، محمد (۱۳۹۶). «مطالعه تطبیقی مبانی جرم‌انگاری جرائم سایبر در نظام کیفری ایران و آلمان». **پژوهش‌های حقوق تطبیقی**، شماره ۴.

کردعلیوند، روح‌الدین و میرزایی، محمد (۱۳۹۷). «گونه‌شناسی جرائم سایبری با نگاهی به قانون جرائم رایانه‌ای و آمار پلیس فتا». **مجله حقوقی دادگستری**، شماره ۱۰۲.

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

نظری، سید غنی؛ جعفرزاده؛ سیامک و نیک‌خواه‌سرنقی، رضا (۱۴۰۰). «نقش سیاست جنایی مشارکتی در پیشگیری از جرائم سایبری در ایران». **پژوهش‌های سیاسی جهان اسلام**، شماره ۴.

نمامیان، پیمان (۱۴۰۳). «مقابله و پیشگیری از ارتکاب جرائم تروریستی در شبکه‌های اجتماعی مجازی». **حقوق فناوری‌های نوین**، شماره ۱۰.

وطنی، امیر و اسدی، حمید (۱۳۹۵). «سیاست جمهوری اسلامی ایران در جرائم سایبری با تأکید بر ویژگی‌های خاص این جرائم». **پژوهشنامه حقوق اسلامی**، شماره ۲.

References

Kundi, G.M, Bartoli, A, & Baile. S (2012), E-local Government: Implementation Barriers in Pakistan, (Germany: Lap-Lambert Academic Publishing)

Odhiambo, N. A, Ochara, N. M, and Kadymatimba, A (2018), "Structuring of the Terrorism Problem in the Digital Age: A Systems Perspective", in: 2018 Open Innovations Conference, OI 2018 (Johannesburg: IEEE)

Taylor, R.W, Eric J. Fritsch, J.L (2014), Digital Crime and Digital Terrorism, (Prentice Hall Press)

Asif Khan, M (2023), "Legal Analysis of the Pakistan's National Cyber Security Policy in the Context of Cyber Warfare" Journal of Law & Social Studies, Vol. 5

Barrie, S (2022), "International Law in the Age of Digital Media: Reflections on History, the Neoliberal Communication Sphere, and Race" London Review of International Law, Vol. 10

Buresh, D.L (2020), "Does Digital Terrorism Really Exist?" Journal of Advanced Forensic Sciences, Vol. 1

Chaudhy, Y (2011). "A country without cyber-law: Pakistan" [Online] available at: http://propakistani.pk/2011/01/10/a-country-without-cyber-law-pakistan/10,june 2011/

Dupont B, Holt T (2022), "The Human Factor of Cybercrime" Social Science Computer Review Vol. 40

Jamil, Z (2006). "Cyber Law" Presented at the 50th Anniversary Celebrations of the Supreme Court of Pakistan International Judicial Conference on 11-14 August, 2006, Jamil and Jamil Law Associates, Islamabad, Pakistan, [Online] available at: http://jamilandjamil.com/wpcontent/uploads/2010/11/article_for_scp_50_anniv_v5.0.pdf, (March 26, 2014).

Falchetta, T (2024), "The Draft UN Cybercrime Treaty Is Overbroad and Falls Short On Human Rights Protection" Just Security: Reiss Center on Law and Security at New York University School of Law, January 22, https://www.justsecurity.org/91318/the-draft-un-cybercrime-treaty-is-overbroad-and-falls-short-on-human-rights-protection/

Magalla, A (2013). "Security, prevention and detection of cyber-crimes in Tanzania, Doctoral Thesis" Tumaini University Iringa University College, [Online] available at: http://www.academia.edu/3471542/the_introduction_to_cybercrime_security_prevention_and_detection_of _cybercrime_in_tanzania

Plotnek, J. and Jill S (2021), "Cyber Terrorism: A Homogenized Taxonomy and Definition" Computers & Security, Vol. 102

Saleem, H, Junaid J, Azzalfa A (2022), "Cyber Crimes Trends in Pakistan: Analyzing the Legal Framework and Enforcement Challenges" Society, Law and Policy Review, Vol. 1

Zia UL Islam, Khan, M. A, & Zubair, M (2019). "Cybercrime and Pakistan" Global Political Review, Vol. 5

In Persian

Alamdari, Ali; Farajiha, Mohammad (2017), A Comparative Study of the Basis of Criminalization of Cybercrimes in the Penal System of Iran and Germany, Comparative Law Research, Volume 8, Issue 2, Pages 637-653

Dashti, Bita; Afshari, Maryam (2019), A Comparative Study of Cybercrimes in Iran and International Law, Comparative Law Research, Volume 3, Issue 1, Serial Number 4, Pages 83-110

Nazari, Seyyed Ghani; Jafarzadeh; Siamak; Nikkhah Sarnaghi, Reza (2021), The Role of Participatory Criminal Policy in Preventing Cybercrimes in Iran, Political Researches of the Islamic World, Volume 11, Issue 4, Pages 151-174

Namamian, Peyman (2024), Combating and Preventing the Committing of Terrorist Crimes in Virtual Social Networks, Law of New Technologies, Volume 5, Issue 10, Pages 215-233

Mousavi, Seyyed Jamal; Rouhani-Moghaddam, Mohammad; Aghaei-Bajestani, Maryam (2022), Cybercrime Prevention Measures with Emphasis on Police Actions with a Jurisprudential Approach, Islamic Jurisprudence and Law Studies, Volume 14, Issue 26, Pages 323-358

Jalali, Mahmoud; Tavassoli-Ardakani, Saeideh (2019), The Necessity of Establishing a Harmonized International Legal System to Combat Crimes in Cyberspace, Public Law Studies, Volume 49, Issue 4, Pages 1351-1372

Razavifard, Behzad; Mousavi, Seyed Nematollah (2016), Criminal Liability in Cyberspace in Iranian Law, Criminal Law Research, Volume 5, Issue 16, Pages 29-45

Salimi, Ehsan (2018), Pathology of Cybercrime Prevention in Iran, Doctoral Thesis, Criminal Law and Criminology, Faculty of Law, Qom University.

Khorramabadi, Abdolsamad (2005), Information Technology Crimes, Doctoral Thesis, Criminal Law and Criminology, Faculty of Law and Political Science, University of Tehran.

Kordalivand, Ruhuddin; Mirzaei, Mohammad (2018), Typology of Cybercrimes with a Look at the Computer Crimes Law and FATA Police Statistics, Justice Legal Journal, Volume 82, Issue 102, Pages 191-207

Fazaeli, Mustafa; Shakibnejad, Ehsan; Karami, Musa (2020), Religious Freedom in Cyberspace and Its Impact on International Peace and Security: With a Look at Islamic Teachings, Comparative Research on Islamic and Western Law, Volume 6, Issue 4, Serial Number 22, February 2020, Pages 87-110

Vatani, Amir; Asadi, Hamid (2016), The Policy of the Islamic Republic of Iran on Cybercrimes with Emphasis on the Specific Characteristics of These Crimes, Islamic Law Research Journal, Volume 17, Issue 2, Serial Number 44, Pages 99-126