Comparative Studies in Jurisprudence, Law, and Politics

Challenges and Strategies for Safeguarding the Principles of Criminal Law in Electronic Criminal Proceedings During the Crime Detection and Preliminary Investigation Stages

1. Sirus Nazari: Department of Law, Qo.C., Islamic Azad University, Qom, Iran
2. Ali Arman*: Department of Law, Bo.C., Islamic Azad University, Borujerd, Iran. Email: 5579145802@iau.ir (Corresponding Author)
3. Soheila Ebrahimzadeh: Department of Law, Shahab Danesh University, Qom, Iran

ABSTRACT

The integration of information technology into criminal proceedings has transformed the nature of preliminary investigations and crime detection from traditional investigative practices into "digital forensics." Although this transformation has substantially enhanced the capacity to uncover the truth, it has also exposed fundamental principles of a fair trial, including the presumption of innocence, the right to privacy, and the accused's right to defense, to serious and unprecedented challenges. Using a descriptive-analytical method, the present article examines the challenges and strategies associated with safeguarding the principles of criminal law in electronic criminal proceedings during the stages of crime detection and preliminary investigation. The findings indicate that, in electronic criminal proceedings, managing massive volumes of data, distinguishing private information from evidence of criminal conduct, and preserving the integrity and chain of custody of digital evidence have become major challenges. Furthermore, the virtualization of judicial processes, including ineffective electronic service of process and restrictions on confidential consultation with legal counsel during online interrogations, has shifted the balance of power in favor of prosecutorial authorities. To address these challenges, the study highlights the necessity of recognizing emerging legal concepts, including the "right to digital silence," ensuring the accused's access to legal counsel and technical experts during cyber investigations, and complying with documented scientific standards in the collection of evidence. It is therefore concluded that the realization of fair electronic criminal proceedings depends on establishing an appropriate balance between the technological efficiency of crime detection and the rigorous protection of the accused's defense rights through the contextualization of international standards.

Keywords: *electronic criminal proceedings, preliminary investigations, digital evidence, defense rights of the accused, principles of criminal law.*

How to cite: Nazari, S., Arman, A., & Ebrahimzadeh, S. (2026). Challenges and Strategies for Safeguarding the Principles of Criminal Law in Electronic Criminal Proceedings During the Crime Detection and Preliminary Investigation Stages. *Comparative Studies in Jurisprudence, Law, and Politics*, *8*(6), 1-30.

© 2026 the authors. This is an open access article under the terms of the Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

Submit Date: 21 February 2026
Revise Date: 14 July 2026
Accept Date: 21 July 2026
Initial Publish Date: 01 September 2026
Final Publish Date: 20 February 2027

پژوهش‌های تطبیقی فقه،
حقوق و سیاست

چالش‌ها و راهکارهای تضمین اصول حقوق جزا در دادرسی کیفری الکترونیکی در مرحله کشف جرم و تحقیقات مقدماتی

۱. سیروس نظری: گروه حقوق، واحد قم، دانشگاه آزاد اسلامی، قم، ایران
۲. علی آرمان*: گروه حقوق، واحد بروجرد، دانشگاه آزاد اسلامی، بروجرد، ایران. پست الکترونیک: 5579145802@iau.ir (نویسنده مسئول)
۳. سهیلا ابراهیم زاده: گروه حقوق، دانشگاه شهاب دانش، قم، ایران

چکیده

ورود فناوری اطلاعات به عرصه دادرسی کیفری، ماهیت تحقیقات مقدماتی و کشف جرم را از کارآگاهی سنتی به «جرم‌یابی دیجیتال» تغییر داده است. این دگردیسی، اگرچه قدرت کشف حقیقت را به طرز چشمگیری افزایش داده، اما اصول بنیادین دادرسی منصفانه مانند اصل برائت، حریم خصوصی و حق دفاع متهم را با چالش‌هایی جدی و بی‌سابقه مواجه ساخته است. مقاله حاضر با هدف بررسی «چالش‌ها و راهکارهای تضمین اصول حقوق جزا در دادرسی کیفری الکترونیکی در مرحله کشف جرم و تحقیقات مقدماتی» و با بهره‌گیری از روش توصیفی-تحلیلی تدوین شده است. یافته‌های پژوهش نشان می‌دهد که در دادرسی الکترونیکی، مدیریت حجم انبوه داده‌ها، تفکیک حریم خصوصی از ادله جرم، و حفظ یکپارچگی و زنجیره حفاظتی ادله دیجیتال به چالش‌های اصلی تبدیل شده‌اند. همچنین، مجازی شدن فرآیندها مانند ابلاغ‌های الکترونیکی نامؤثر و محدودیت در مشاوره محرمانه با وکیل در بازجویی‌های آنلاین، توازن قوا را به نفع سیستم تعقیب تغییر داده است. برای عبور از این چالش‌ها، مطالعه حاکی از لزوم پذیرش مفاهیم حقوقی نوین از جمله «حق سکوت دیجیتال»، تضمین دسترسی متهم به وکیل و مشاور فنی در تحقیقات سایبری، و رعایت استانداردهای علمی مستند در جمع‌آوری ادله است. در نتیجه، تحقق دادرسی الکترونیکی عادلانه منوط به ایجاد توازن میان کارآمدی فناوری در کشف جرم و رعایت دقیق تضمینات حقوق دفاعی متهم از طریق بومی‌سازی استانداردهای بین‌المللی است.

واژگان کلیدی: *دادرسی کیفری الکترونیکی، تحقیقات مقدماتی، ادله دیجیتال، حقوق دفاعی متهم، اصول حقوق جزا.*

نحوه استناددهی: نظری، سیروس.، آرمان، علی.، و ابراهیم زاده، سهیلا. (۱۴۰۵). چالش‌ها و راهکارهای تضمین اصول حقوق جزا در دادرسی کیفری الکترونیکی در مرحله کشف جرم و تحقیقات مقدماتی. *پژوهش‌های تطبیقی فقه، حقوق و سیاست*، ۸(۶)، ۳۰-۱.

© ۱۴۰۵ تمامی حقوق انتشار این مقاله متعلق به نویسنده است. انتشار این مقاله به‌صورت دسترسی آزاد مطابق با گواهی (CC BY-NC 4.0) صورت گرفته است.

تاریخ ارسال: ۲ اسفند ۱۴۰۴
تاریخ بازنگری: ۲۳ تیر ۱۴۰۵
تاریخ پذیرش: ۳۰ تیر ۱۴۰۵
تاریخ چاپ اولیه: ۱۰ شهریور ۱۴۰۵
تاریخ چاپ نهایی: ۱ اسفند ۱۴۰۵

مقدمه

مرحله کشف جرم و تحقیقات مقدماتی، سنگ‌بنای پرونده کیفری و حساس‌ترین مقطع دادرسی است. در این مرحله است که تقابل میان «اقتدار دولت برای تأمین امنیت» و «حقوق و آزادی‌های فردی» به اوج خود می‌رسد (Khaleghi, 2024). با ورود فناوری اطلاعات به این عرصه، ماهیت تحقیقات از «کارآگاهی سنتی» به «جرم‌یابی دیجیتال» و «تحلیل داده‌ها» تغییر یافته است. این دگردیسی، اگرچه قدرت کشف حقیقت را به‌طرز چشمگیری افزایش داده، اما هم‌زمان، اصول بنیادین دادرسی منصفانه را با مخاطراتی بی‌سابقه و پیچیده مواجه ساخته است. در دادرسی سنتی، چالش اصلی، پیدا کردن سرنخ فیزیکی مانند اثر انگشت بود؛ اما در دادرسی الکترونیکی، چالش اصلی، مدیریت حجم انبوهی از داده‌ها و تفکیک حریم خصوصی از ادله جرم است. امروز، گوشی هوشمند یک متهم، مخزن اسرار زندگی اوست و تفتیش آن توسط ضابطین، دیگر شباهتی به بازرسی بدنی ساده ندارد، بلکه به‌مثابه ورود به ذهن و روح متهم است. اینجاست که اصول کلاسیک حقوق جزا، مانند «اصل برائت»، «حرمت حریم خصوصی» و «حق سکوت»، در برابر قدرت ابزارهای شنود و بازیابی اطلاعات، شکننده به نظر می‌رسند (Soni, 2024). علاوه بر این، «مجازی‌شدن» فرآیندهای دادسرا، حقوق دفاعی متهم را نیز تحت‌الشعاع قرار داده است. ابلاغ‌های الکترونیکی که گاهی به رؤیت واقعی متهم نمی‌رسند، بازجویی‌های آنلاینی که در آن وکیل امکان مشاوره محرمانه با موکل را ندارد، و بازداشت‌های موقتی که جای خود را به نظارت‌های الکترونیکی دائمی داده‌اند، همگی نشان‌دهنده تغییر توازن قوا به نفع سیستم تعقیب است (Hayat Poursefli, 2021). از سوی دیگر، ماهیت فنی و فرّار ادله دیجیتال، چالش‌های جدیدی را در باب «تمامیت ادله» و «زنجیره حفاظتی» ایجاد کرده است. یک تغییر کوچک در کد هش یک فایل، می‌تواند کل استدلال قضایی را فرو بریزد. همچنین، ماهیت بدون مرز فضای سایبر، قواعد سنتی «صلاحیت محلی» و «نیابت قضایی» را با بحران مواجه کرده و موجب سرگردانی ارباب‌رجوع و اطاله دادرسی شده است (Koulaei, 2025). در نتیجه و برخلاف تصور اولیه، دادرسی کیفری الکترونیکی در مرحله کشف جرم و تحقیقات مقدماتی، در عین سرعت‌بخشی به فرآیند رسیدگی و تسهیل فرآیندها، با چالش‌ها و آسیب‌های زیادی می‌تواند همراه باشد که این مقاله درصدد بررسی آن‌ها و ارائه راهکارهایی در جهت عبور از این چالش‌ها می‌باشد.

این مقاله با روش توصیفی و تحلیلی به بررسی موضوع پرداخته و از دو قسمت تشکیل شده است. در قسمت اول، به بررسی و تحلیل چالش‌ها پرداخته می‌شود و در قسمت دوم، راهکارهای گذر از این چالش‌ها مطرح می‌گردد.

چالش‌های تضمین اصول حقوق جزا در کشف جرم و تحقیقات مقدماتی

مرحله تحقیقات مقدماتی، بنیادین‌ترین و در عین حال حساس‌ترین مقطع در فرآیند دادرسی کیفری است. در دادرسی کیفری الکترونیکی، ماهیت تحقیقات مقدماتی از «جست‌وجوی فیزیکی» به «کاوش دیجیتال» تغییر یافته است. اگر در گذشته، دغدغه اصلی ضابطین، بازرسی از منزل یا مخفیگاه متهم بود، امروزه تمرکز بر تفتیش داده‌های رایانه‌ای، رهگیری ارتباطات و واکاوی حافظه‌های ابری است. این تغییر ماهیت، چالش‌های عمیقی را در برابر اصول دادرسی منصفانه قرار داده است.

نقض حریم خصوصی و اصل برائت در تحصیل دلیل

با ظهور عصر اطلاعات، مفهوم «دلیل» و «مکان» دگرگون شده است. امروزه، زندگی انسان‌ها به دیتای صفر و یک تبدیل شده و در ابزارهایی مانند تلفن همراه یا در سرورهایی نامرئی و فضای ابری ذخیره می‌شود. این تغییر ماهیت، چالش‌های حقوق بشری سهمگینی را در مرحله تحقیقات مقدماتی پدید آورده است.

چالش‌های تفتیش و توقیف داده‌های رایانه‌ای و حریم خصوصی

اگرچه قانون‌گذار در ماده ۶۶۹ ق.آ.د.ک، تفتیش را منوط به «ظن قوی» به کشف جرم کرده، اما ابهام در مصادیق فنی و اختیارات گسترده ضابطان در دسترسی به محتوای «داده‌های در حال انتقال»، موضوع ماده ۶۷۳، عملاً مرزهای حریم خصوصی موضوع اصل ۲۵ قانون اساسی را مخدوش می‌سازد (Akbari, 2022). چالش اصلی آنجاست که ماهیت سیال داده‌ها، امکان تفکیک داده‌های مرتبط با جرم از اطلاعات شخصی بی‌ارتباط را دشوار کرده و خطر نقض اصل «ممنوعیت تحصیل دلیل از طریق نامشروع» را افزایش می‌دهد. همچنین، با وجود تأکید ماده ۴ ق.آ.د.ک بر رعایت حریم خصوصی، فقدان سازوکار نظارتی دقیق بر نحوه نگهداری و امحای داده‌های توقیف‌شده و احتمال افشای آن‌ها، موضوع ماده ۵۵ قانون تجارت الکترونیکی، امنیت قضایی متهمان را تهدید کرده و با استانداردهای دادرسی منصفانه در تعارض است.

در عمل، ضابطین با توقیف یک کیس کامپیوتر یا لپ‌تاپ، به اقیانوسی از داده‌ها دسترسی پیدا می‌کنند که شاید تنها یک درصد آن مرتبط با جرم باشد. این دسترسی نامحدود، مصداق بارز «تفتیش عام» است که در حقوق مدرن مردود شناخته می‌شود. بر اساس دکترین «مشاهده در نمای آشکار» و انحراف آن: در حقوق سنتی، اگر پلیس برای یافتن مواد مخدر وارد خانه‌ای شود و به‌طور اتفاقی یک اسلحه غیرمجاز روی میز ببیند، می‌تواند آن را ضبط کند (Ehmann, 1990). در فضای دیجیتال، این دکترین به‌شدت خطرناک می‌شود. ضابط برای یافتن یک فایل متنی، مثلاً سند کلاهبرداری، مجبور است هزاران فایل را بازبینی کند. در این حین، ممکن است به عکس‌های خصوصی، چت‌های خانوادگی یا اسناد غیرمرتبط برخورد کند. چون ماهیت تفتیش دیجیتال نیازمند «اسکن‌کردن همه‌چیز» است، عملاً حریم خصوصی متهم در تمام ابعاد نقض می‌شود تا شاید دلیلی پیدا شود. این فرآیند، اصل «تناسب در تفتیش» را زیر سؤال می‌برد.

یکی از چالش‌های حقوقی، اصرار ضابطین بر «توقیف سخت‌افزار» است. توقیف موبایل یا لپ‌تاپ یک دانشجو یا تاجر برای ماه‌ها، می‌تواند زندگی تحصیلی و شغلی او را فلج کند؛ درحالی‌که طبق استانداردهای نوین و ماده ۶۷۱ قانون آیین دادرسی کیفری، اصل باید بر «کپی‌برداری از داده‌ها» و استرداد تجهیزات باشد. نقض این رویه و نگهداری طولانی‌مدت تجهیزات، نوعی «مجازات پیش از حکم» است که برخلاف اصل برائت اعمال می‌شود. علاوه بر این، در زمان توقیف، خطر «کاشت ادله» یا تغییر در داده‌ها توسط ضابطین غیرمتخصص وجود دارد که زنجیره بازداشت ادله را مخدوش می‌کند. همچنین، تلفن همراه متهم، تنها حاوی اطلاعات او نیست، بلکه حاوی اطلاعات صدها نفر دیگر، شامل مخاطبین، طرفین چت و عکس‌های دوستان است. تفتیش موبایل متهم، عملاً تجاوز به حریم خصوصی تمام کسانی است که با او در ارتباط بوده‌اند، بدون آنکه آن اشخاص جرمی مرتکب شده باشند. نظام حقوقی ایران هنوز پروتکل دقیقی برای حفاظت از داده‌های اشخاص ثالث در جریان تفتیش رایانه‌ای ندارد.

شنود و رهگیری ارتباطات و نقض اصل مصونیت مکالمات

قانون‌گذار در ماده ۷۳۰ قانون مجازات اسلامی، شنود غیرمجاز داده‌های در حال انتقال را جرم‌انگاری کرده و در ماده ۶۸۳ قانون آیین دادرسی کیفری، دسترسی به محتوای ارتباطات را منوط به دستور مقام قضایی دانسته، اما ساختار فنی دادرسی الکترونیکی، چالش‌برانگیز است.

الزام ارائه‌دهندگان خدمات اینترنتی به «نگهداری داده‌های ترافیک» طبق مواد ۶۶۷ و ۶۶۸ قانون آیین دادرسی کیفری، عملاً بستری برای «نظارت فراگیر» ایجاد کرده که با روح ماده ۱۵۰ همان قانون، یعنی محدودیت شدید کنترل ارتباطات، در تضاد است (Zadeh-Hossein Aliaei, 2017). آسیب اصلی آنجاست که تفکیک فنی میان «داده ترافیک» و «محتوای پیام» دشوار بوده و سهولت دسترسی ضابطان به این داده‌ها، خطر نقض حریم خصوصی و اصل «تفسیر مضیق محدودیت‌ها» را افزایش می‌دهد. بنابراین، علی‌رغم تأکید ماده ۵۸ قانون تجارت

الکترونیکی بر امنیت رمزنگاری، ظرفیت‌های فنی شبکه ملی عدالت، پتانسیل تبدیل «استثنای شنود» به «قاعده نظارت» را داراست که تهدیدی جدی برای امنیت قضایی شهروندان محسوب می‌شود. با گسترش پیام‌رسان‌های دارای رمزنگاری سرتاسری، شنود کلاسیک بی‌اثر شده است. این امر نهادهای امنیتی و انتظامی را به سمت روش‌های خطرناک‌تری، مانند «نصب بدافزار و تروجان‌های دولتی»، سوق داده است: در این روش، ضابط به‌جای شنود مسیر، خود دستگاه نهایی را هک می‌کند. این کار عملاً تبدیل گوشی شهروند به یک «میکروفون و دوربین جاسوسی» است. این سطح از نفوذ، بسیار فراتر از شنود مکالمات است و تمامی فعالیت‌های آفلاین و آنلاین فرد را رصد می‌کند که نقض فاحش حریم خصوصی محسوب می‌شود.

یکی از چالش‌های جهانی که در ایران نیز مصداق دارد، نظارت‌های توده‌ای بر ترافیک اینترنت است. سیستم‌های فیلترینگ و مانیتورینگ شبکه، گاهی تمام بسته‌های اطلاعاتی عبوری را اسکن می‌کنند تا کلمات کلیدی خاصی را بیابند. این رویکرد، اصل «شخصی‌بودن تعقیب» و «ظن خاص» را نقض می‌کند. در اینجا همه شهروندان در مظان اتهام هستند، مگر اینکه خلافش ثابت شود؛ که دقیقاً برعکس اصل برائت است (Zare, 2020).

شنود مکالمات میان متهم و وکیل، یکی از خطوط قرمز اصول حقوق جزا است. اما در شنودهای الکترونیکی و هک‌کردن گوشی‌ها، معمولاً تفکیکی صورت نمی‌گیرد و استراتژی‌های دفاعی متهم که باید محرمانه بماند، در اختیار مقام تعقیب قرار می‌گیرد. این امر «تساوی سلاح‌ها» را به نفع دادستان برهم می‌زند.

دسترسی ضابطین به داده‌های انبوه و نقض حریم خصوصی

تکلیف ارائه‌دهندگان خدمات دسترسی به «نگهداری داده‌های ترافیک و محتوا»، موضوع مواد ۶۶۷ و ۶۶۸ قانون آیین دادرسی کیفری، عملاً زیرساخت «نظارت فراگیر» را مهیا ساخته است (Sayadi, 2022). چالش حقوقی آنجاست که صدور دستورات کلی برای دسترسی به این مخازن داده توسط ضابطین، با استناد به تفاسیر موسع از ماده ۱۵۰ و ماده ۶۷۳ قانون آیین دادرسی کیفری، اصل «شخصی‌بودن تعقیب» و قاعده «ضرورت و تناسب در تفتیش» را مخدوش می‌سازد. فقدان ضوابط دقیق در قانون جرایم رایانه‌ای، مواد ۷۲۹ تا ۷۵۵ تعزیرات، برای تفکیک داده‌های مجرمانه از اطلاعات شخصی شهروندان عادی در زمان پالایش داده‌های انبوه، خطر نقض اصل ۲۵ قانون اساسی را تشدید کرده و دادرسی الکترونیکی را از مسیر عدالت قضایی به سمت «کنترل امنیتی نامحدود» منحرف می‌نماید.

چالش تفکیک داده‌های شخصی از ادله جرم در تجهیزات توقیفی

شاید عملیاتی‌ترین و ملموس‌ترین چالش در دادسراها و پلیس فتا، همین بند باشد. در نظام‌های حقوقی پیشرفته، نهادی به نام «تیم فیلتر» وجود دارد؛ گروهی مستقل از تیم تحقیق که داده‌ها را بررسی کرده و موارد خصوصی یا دارای مصونیت، مثل نامه به وکیل، را جدا می‌کنند و فقط داده‌های مرتبط با جرم را به بازپرس می‌دهند. در ایران، چنین سازوکاری نهادینه نشده است. همان ضابطی که دنبال دلیل است، به همه‌چیز دسترسی دارد. این امر خطر «اخاذی» یا «سوءاستفاده از اطلاعات شخصی» متهم را افزایش می‌دهد. استفاده از هوش مصنوعی در جست‌وجوی داده‌ها، در عین کمک به ضابطین، با آسیب‌های جدیدی در حوزه نقض حریم خصوصی همراه است (Rahnama & Zafari Kouretash, 2025). چالش دیگر، بازیابی اطلاعات پاک‌شده است. ممکن است متهم سال‌ها پیش عکسی داشته و پاک کرده باشد. بازگرداندن این اطلاعات توسط ضابطین، نبش قبر زندگی گذشته فرد است که ارتباطی با جرم فعلی ندارد؛ اما می‌تواند آبروی او را ببرد و ذهنیت قاضی را علیه او مخدوش کند.

آسیب‌شناسی چالش «تفکیک داده‌های شخصی از ادله جرم» در تجهیزات توقیفی، بیانگر تعارضی جدی میان الزامات فنی کشف جرم و اصل حرمت حریم خصوصی مستفاد از اصل ۲۵ قانون اساسی و ماده ۴ قانون آیین دادرسی کیفری است. اگرچه قانون‌گذار در ماده ۶۶۹ قانون آیین دادرسی کیفری، دامنه تفتیش و توقیف را مقید به «داده‌های مرتبط با جرم» نموده و در ماده ۶۷۱ همان قانون، اصل را بر «کپی‌برداری از داده» به‌جای «توقیف فیزیکی سامانه» نهاده است تا از تعرض به داده‌های غیرمرتبط جلوگیری شود؛ اما در مقام اجرا، ماهیت درهم‌تنیده اطلاعات در تجهیزات هوشمند، عملاً تفکیک داده‌های مجرمانه از حریم خصوصی افراد را در لحظه تفتیش ناممکن می‌سازد.

چالش‌های حقوق دفاعی متهم در دادسرا

مرحله تحقیقات مقدماتی در دادسرا، ذاتاً مرحله‌ای است که در آن کفه ترازوی عدالت به نفع «اقتدار عمومی» (دادستان و بازپرس) سنگینی می‌کند و «حقوق دفاعی متهم» در آسیب‌پذیرترین وضعیت خود قرار دارد. ویژگی‌های سنتی این مرحله، یعنی «غیرعلنی‌بودن»، «کتبی‌بودن» و «محرمانه‌بودن» (Akhoundi, 2015)، همواره چالش‌هایی را برای اعمال کامل حقوق دفاعی ایجاد می‌کردند. حال، با ورود فناوری اطلاعات و استقرار دادرسی الکترونیکی، لایه جدیدی از پیچیدگی بر این وضعیت افزوده شده است. تسریع در تحقیقات مقدماتی نباید به قیمت ذبح حق «آگاه‌شدن» و «پاسخ‌دادن» تمام شود (Ashouri, 2023). در این خصوص، چند چالش مهم مطرح است.

نقص در ابلاغ الکترونیک و عدم اطلاع واقعی متهم (چالش سامانه ثنا)

«حق آگاهی»، دروازه ورود به سایر حقوق دفاعی است (Naude, 2009). تا متهم نداند که تحت تعقیب است و چه اتهامی متوجه اوست، نمی‌تواند وکیل بگیرد، تدارک دفاع ببیند یا در جلسه حاضر شود. در نظام دادرسی کیفری ایران، نهاد «ابلاغ» ضامن این حق است. با تصویب ماده ۱۷۵ قانون آیین دادرسی کیفری ۱۳۹۲ و راه‌اندازی «سامانه ابلاغ الکترونیک» (ثنا)، انقلابی در این حوزه رخ داد که منجر به حذف مأمور ابلاغ و جایگزینی آن با «حساب کاربری» شد. اما این تغییر، مفهوم «ابلاغ» را از یک «امر واقعی» به یک «فرض قانونی» تغییر داد و چالش‌های عظیمی را برای حقوق دفاعی متهم ایجاد کرد.

چالش عدم اطلاع واقعی متهم در بستر سامانه ابلاغ الکترونیک، یکی از جدی‌ترین آسیب‌های دادرسی کیفری نوین است که با اصل «حق دفاع» و «لزوم تفهیم اتهام»، موضوع ماده ۵ قانون آیین دادرسی کیفری، در تعارض قرار می‌گیرد. اگرچه ماده ۱۷۵ قانون آیین دادرسی کیفری، ابلاغ الکترونیکی را کافی و معتبر دانسته و ماده ۶۵۵ آن را هم‌تراز ابلاغ فیزیکی فرض کرده است، اما تکیه صرف بر «مشاهده سامانه» به‌جای «رؤیت واقعی»، منجر به صدور آرای غیابی ناخواسته و تضییع حق واخواهی می‌شود (Loveymi & Janadeleh, 2023). این رویه، با ماده ۲ قانون آیین دادرسی کیفری که بر تضمین حقوق طرفین دعوی تأکید دارد، مغایر است؛ زیرا متهمی که به دلایل فنی، مانند قطع اینترنت یا عدم سواد دیجیتال، به حساب کاربری خود دسترسی ندارد، عملاً از جریان دادرسی حذف می‌شود. همچنین، فرض قانونی «ابلاغ واقعی» صرفاً با ارسال پیامک، موضوع تبصره ماده ۶۸۰، بدون اطمینان از وصول آن به مخاطب اصلی، نقض اصل «ترافعی‌بودن» دادرسی است و امنیت قضایی شهروندان را در برابر تکنولوژی قربانی می‌کند.

در دادرسی الکترونیکی، طبق ماده ۶۵۵ قانون آیین دادرسی کیفری و آیین‌نامه نحوه استفاده از سامانه‌های رایانه‌ای، به‌محض اینکه اوراق قضایی در حساب کاربری متهم در سامانه ثنا بارگذاری شود، ابلاغ «قانونی» محسوب می‌شود و اگر متهم آن را مشاهده کند (کلیک کند)، ابلاغ «واقعی» است (Rahimi et al., 2021). قانون‌گذار با این مصوبه، بار اثبات «اطلاع» را از دوش دادسرا برداشته و بار «کسب اطلاع» را بر دوش شهروند گذاشته است. در واقع، یک «فرض آگاهی» ایجاد شده است: فرض بر این است که همه شهروندان هر روز حساب کاربری

خود را چک می‌کنند. این فرض در جامعه‌ای که هنوز بخش بزرگی از آن با اینترنت بیگانه‌اند، فرضی خلاف واقع است. نتیجه عملی این تغییر چیست؟ اگر دادسرا احضاریه‌ای صادر کند و در سامانه قرار دهد و پیامک اطلاع‌رسانی به دلیل اختلال مخابراتی یا خاموش‌بودن گوشی به متهم نرسد، متهم از احضاریه مطلع نمی‌شود. اما از نظر قانونی، او «ابلاغ‌شده» محسوب می‌شود. در نتیجه، بازپرس می‌تواند پس از عدم حضور، دستور جلب صادر کند. این وضعیت، «غافلگیری دادرسی» است. در جرایم مهم کیفری، اکتفا به ابلاغ الکترونیکی بدون حصول اطمینان از رؤیت واقعی، نقض اصل «ترافع» است. متهمی که ناگهان با حکم جلب مواجه می‌شود، درحالی‌که روحش از پرونده خبر نداشته، قربانی «کارآمدی تکنولوژیک» سیستم شده است.

پاشنه آشیل سامانه ثنا، وابستگی آن به «پیامک» به‌عنوان ابزار هشداردهنده است. اگرچه قانون می‌گوید «اصل ابلاغ، بارگذاری در حساب کاربری است»، اما در عمل، هیچ شهروند عاقلی هر روز صبح سامانه عدل‌ایران را چک نمی‌کند تا ببیند پرونده‌ای دارد یا خیر. همه منتظر پیامک هستند. لیست سیاه مخابراتی که پیامک‌های تبلیغاتی را مسدود می‌کند و گاهی پیامک‌های قضایی را نیز فیلتر می‌کند، تغییر شماره تلفن همراه توسط متهم و فراموشی به‌روزرسانی آن در ثنا، و اختلالات سراسری اینترنت؛ در تمام این موارد، «پل ارتباطی» قطع می‌شود (Hosseini, 2023). در رویه قضایی، وقتی وکیل متهم اعتراض می‌کند که «موکل من پیامک دریافت نکرده»، پاسخ قضات معمولاً این است: «طبق قانون، ارسال به حساب کاربری ملاک است، نه پیامک». این استدلال، شکل‌گرایی محض و مغایر با عدالت کیفری است. در امور کیفری که پای آبرو و آزادی در میان است، سیستم نباید به «احتمالات فنی» تکیه کند. مسئولیت دولت در اطلاع‌رسانی، تعهد به نتیجه است و نه تعهد به وسیله و باید منجر به ابلاغ شود (Rahmdel, 2015).

سامانه ثنا برای «شهروند دیجیتال» طراحی شده است؛ فردی باسواد، دارای گوشی هوشمند و اینترنت پایدار؛ اما متهمان دادسرا لزوماً چنین افرادی نیستند. بسیاری از متهمان از اقشار فرودست، روستاییان دورافتاده، سالمندان یا افراد کم‌سواد هستند. اجبار به ثبت‌نام در ثنا، که اکنون پیش‌شرط هرگونه خدمات قضایی است، برای این گروه‌ها تبدیل به یک «مانع دسترسی به عدالت» شده است (Bastami, 2019). این وضعیت، مصداق «تبعیض ساختاری» است. سیستم دادرسی الکترونیکی، ناخواسته طبقات پایین جامعه را که بیشترین درگیری را با سیستم کیفری دارند، از چرخه اطلاع‌رسانی حذف می‌کند (Beiki Shouraki & Fallah, 2023).

صدور آرای غیابی متعدد علیه این افراد و از دست رفتن مهلت‌های واخواهی و تجدیدنظر، هزینه‌های سنگینی است که «فقر دیجیتال» بر آن‌ها تحمیل می‌کند.

اگرچه هدف سامانه ثنا حفظ حریم خصوصی و حذف مأمور ابلاغ از درِ منزل بود، اما چالش‌های جدیدی ایجاد کرده است. در بسیاری از موارد، افراد برای ثبت‌نام یا چک‌کردن ابلاغیه، مجبورند به کافی‌نت‌ها یا دفاتر خدمات قضایی مراجعه کنند. وقتی متهم رمز عبور خود را به متصدی کافی‌نت می‌دهد تا ابلاغیه را برایش پرینت بگیرد، عملاً محرمانه‌بودن اتهام نقض می‌شود. متصدی کافی‌نت متوجه می‌شود که مشتری‌اش متهم به «رابطه نامشروع» یا «سرقت» است (Beiki Shouraki & Fallah, 2024). در شهرهای کوچک، این موضوع می‌تواند به‌سرعت باعث ریختن آبروی فرد شود. در سیستم سنتی، برگه‌ها درون پاکت دربسته بود؛ اما در سیستم الکترونیکی، مشاهده ابلاغیه در اماکن عمومی، حریم خصوصی را در معرض خطر قرار می‌دهد.

موانع دسترسی محرمانه وکیل به موکل در بازجویی‌های آنلاین

در بستر الکترونیک، زیرساخت‌های فنی برای تحقق «ارتباط محرمانه» در حین جلسه رسیدگی مغفول مانده است. چالش اصلی آنجاست که در سامانه‌های ویدئوکنفرانس قضایی، موضوع دستورالعمل هوشمندسازی و الکترونیکی‌شدن فرآیندها، تمامی تعاملات صوتی و تصویری ضبط و پایش می‌شود و فقدان «اتاق‌های گفت‌وگوی خصوصی» برای مشورت آنی وکیل و موکل، عملاً حق دفاع را عقیم می‌سازد. این وضعیت، وکیل را از یک «مدافع فعال» به یک «ناظر صامت» تقلیل داده و با افشای استراتژی دفاعی نزد مقام تحقیق، اصل «ترافعی‌بودن دادرسی» و «تساوی سلاح‌ها» را نقض می‌کند.

در بازجویی سنتی، وکیل در اتاق بازپرس، کنار موکلش می‌نشیند. این «هم‌جواری فیزیکی» اثرات روانی و حقوقی دارد. وکیل با زبان بدن، نگاه و حضور خود، به موکل اعتمادبه‌نفس می‌دهد و به بازپرس یادآوری می‌کند که قانون ناظر است (Koushki, 2024). اما در بازجویی آنلاین، وکیل تبدیل به یک تصویر کوچک در گوشه مانیتور می‌شود. قانون‌گذار حضور وکیل را برای «نظارت بر تحقیقات» خواسته است. در ویدئوکنفرانس، زاویه دید وکیل محدود به کادر دوربین است. او نمی‌تواند ببیند که آیا در اتاق بازجویی، پشت دوربین، شخص دیگری متهم را تهدید می‌کند؟ یا آیا بازپرس برگه‌هایی را جلوی متهم می‌گذارد که وکیل نمی‌بیند؟ این «کوری بصری»، کارآمدی وکیل را در تضمین حقوق موکل به‌شدت کاهش می‌دهد.

بزرگ‌ترین چالش در بازجویی‌های آنلاین، عدم امکان «مشاوره محرمانه» است. استانداردهای بین‌المللی ایجاب می‌کنند که نرم‌افزارهای دادگاه مجازی باید دارای «اتاق‌های گفت‌وگو» باشند که قاضی یا بازپرس نتواند صدای آن را بشنود (Neira-Pena, 2023). فقدان این قابلیت فنی در سامانه‌های ایران، نقض آشکار تبصره ماده ۴۸ و استانداردهای دادرسی منصفانه است.

تبصره ماده ۴۸ آ.د.ک که حق انتخاب وکیل را در جرایم امنیتی محدود به وکلای مورد تأیید رئیس قوه قضاییه کرده است، خود چالشی بزرگ است؛ اما در فضای مجازی، این محدودیت تشدید می‌شود.

چالش تفهیم اتهام و اخذ آخرین دفاع به‌صورت غیرحضوری

«تفهیم اتهام» و «اخذ آخرین دفاع»، دو رکن مهم دادرسی کیفری و به‌مثابه «الف» و «ی» در الفبای تحقیقات مقدماتی هستند. تفهیم اتهام، لحظه‌ای است که متهم درمی‌یابد چرا در برابر عدالت قرار گرفته است (ماده ۱۹۵ آ.د.ک) و آخرین دفاع، آخرین فرصت او برای رد اتهامات پیش از صدور کیفرخواست است (ماده ۲۶۲ آ.د.ک). با الکترونیکی‌شدن دادرسی و استفاده از ویدئوکنفرانس یا حتی فرم‌های الکترونیکی، «کیفیت» و «ماهیت» این مراحل دستخوش تغییرات نگران‌کننده‌ای شده است. اگرچه قانون‌گذار در ماده ۶۵۹ قانون آیین دادرسی کیفری، بهره‌گیری از ویدئوکنفرانس برای بازجویی و رسیدگی را مجاز شمرده، اما ماهیت حقوقی «تفهیم اتهام»، موضوع مواد ۵ و ۱۹۵ قانون آیین دادرسی کیفری، فرآیندی فراتر از قرائت صرف عناوین مجرمانه است و مستلزم «تفهیم تفهیم» و اطمینان از درک کامل متهم نسبت به ماهیت اتهام و ادله آن است (Haddadzadeh Nairi et al., 2023).

واژه «تفهیم»، از ریشه فهم، بار معنایی خاصی دارد. اتهام، صرفاً قرائت متن قانون نیست؛ بلکه «تشریح و تبیین» اتهام به زبان ساده برای متهم است، به‌گونه‌ای که او ارکان مادی و معنوی جرم انتسابی را درک کند. این امر نیازمند تعامل چهره‌به‌چهره، مشاهده واکنش متهم و اطمینان از هوشیاری و درک اوست (Ashouri, 2023). در دادرسی الکترونیکی، این فرآیند مکانیکی می‌شود. بازپرس متن اتهام را از روی مانیتور می‌خواند و متهم در آن سوی خط، شاید با کیفیت صدای پایین، می‌شنود. در این فضا، تفهیم اتهام به «اعلام اتهام» تقلیل می‌یابد.

اخذ آخرین دفاع، زمانی مشروع است که متهم و وکیل او به «تمام محتویات پرونده» دسترسی داشته باشند. در دادرسی الکترونیکی، چالش «نابرابری اطلاعاتی» رخ می‌دهد. در بسیاری از موارد، دسترسی وکیل به سامانه مدیریت پرونده (*CMS*) محدود است. ممکن است برخی گزارش‌های ضابطین یا اسناد محرمانه در کارتابل وکیل بارگذاری نشده باشد، درحالی‌که بازپرس آن‌ها را در مانیتور خود می‌بیند. اخذ آخرین دفاع در شرایطی که متهم آنلاین به تمام ادله دسترسی ندارد، تبدیل به یک «دام» می‌شود. این وضعیت، نقض قاعده «منع تحصیل دلیل با فریب» است. اگر بازپرس در جلسه آنلاین سندی را رو کند که وکیل قبلاً ندیده و فرصت بررسی اصالت آن را نداشته، اصل غافلگیری رخ داده که مغایر با دادرسی منصفانه است (Ghane & Zarei, 2022).

جلسه تفهیم اتهام و آخرین دفاع، دارای یک جنبه «آیینی» است که به متهم جدیت موضوع را منتقل می‌کند. «فضای دادسرا» خود بخشی از فرآیند تأدیب و هوشیارسازی متهم است. اما در دادرسی الکترونیکی، متهم ممکن است با لباس راحتی در خانه خود نشسته باشد و از طریق موبایل تفهیم اتهام شود. این پدیده، «عادی‌سازی اتهام» است. وقتی مرز میان «تماس تصویری با دوست» و «تماس تصویری با بازپرس» کم‌رنگ شود، متهم ممکن است ناخواسته مطالبی را بیان کند که در فضای رسمی دادگاه نمی‌گفت (Ray, 2025). این کاهش ابهت، نه‌تنها بازدارندگی را کم می‌کند، بلکه باعث می‌شود متهم خطرات حقوقی کلمات خود را دست‌کم بگیرد.

بازداشت موقت و نظارت الکترونیکی پیش از محاکمه

بازداشت موقت، شدیدترین تصمیم در تحقیقات مقدماتی است که آزادی متهم را پیش از اثبات جرم سلب می‌کند (Khaleghi, 2024). مراقبت الکترونیکی، به پدیده خطرناک «تورگستری» منجر شده است و حتی برخی مخالفت‌های فقهی نیز با آن از همان ابتدا صورت گرفته است (Javidzadeh & Mirehei, 2006)؛ در مواردی نیز مورد سوءاستفاده مقامات قضایی قرار گرفته است. برخی از تحقیقات میدانی نشان داده که برخی بازپرسان، از پابند الکترونیکی برای متهمانی استفاده می‌کنند که در شرایط عادی باید با قرار «کفالت» یا «وثیقه» آزاد می‌شدند (Taghiniam & Ghanbari, 2024). چالش بزرگ دیگر، هزینه تجهیزات است. طبق ماده ۵۵۵ آ.د.ک و آیین‌نامه‌های اجرایی، هزینه نصب و نگهداری پابند بر عهده متهم است. پولی‌شدن نظارت الکترونیکی، منجر به «عدالت طبقاتی» می‌شود. امروز این پیش‌بینی محقق شده است. در مرحله دادسرا، متهم متمول هزینه پابند را می‌دهد و در خانه، کنار خانواده‌اش، منتظر دادگاه می‌ماند؛ اما متهم فقیر که توان پرداخت ودیعه و هزینه ماهانه پابند را ندارد، راهی بازداشتگاه عمومی می‌شود.

بازداشت در زندان، مکان مشخصی دارد. اما نظارت الکترونیکی، ورود دولت به خصوصی‌ترین حریم فرد، یعنی منزل، است. پابندهای مجهز به *GPS*، تمام حرکات متهم را ۲۴ساعته ثبت می‌کنند. این وضعیت، تبدیل‌کردن خانه به سلول انفرادی است. داده‌های جمع‌آوری‌شده از پابند، مانند اینکه متهم کی می‌خوابد، کی بیدار می‌شود، چند بار به دستشویی می‌رود، بسیار فراتر از نیاز امنیتی برای جلوگیری از فرار است. در حقوق ایران، مرکز پیگیری سند تحول بر هوشمندسازی نظارت تأکید دارد (Center for Monitoring the Implementation of the Judicial Transformation, 2024)، اما هنوز پروتکل دقیقی برای «امحای داده‌های مکانی» پس از برائت متهم وجود ندارد.

تکنولوژی عاری از خطا نیست. پابندها ممکن است دچار نقص فنی، اتمام باتری یا اختلال *GPS* شوند. در سیستم‌های نظارتی، «قطع سیگنال» معمولاً به‌عنوان «تلاش برای فرار» تفسیر می‌شود و منجر به صدور دستور جلب فوری و هجوم مأموران به منزل متهم می‌گردد.

چالش‌های فنی و اجرایی در مرحله کشف

مرحله کشف جرم در فضای سایبر، تفاوت ماهوی با فضای فیزیکی دارد. در صحنه جرم سنتی، آثار جرم، مانند خون، پوکه فشنگ یا اثر انگشت، «ملموس» و «پایدار» هستند و با چشم غیرمسلح دیده می‌شوند. اما در صحنه جرم دیجیتال، ادله، مانند فایل‌های لاگ، ردپای *IP* یا تراکنش‌های رمزارز، «نامرئی»، «فرّار» و به‌شدت «آسیب‌پذیر» هستند (Khan & Ahmed, 2025). یک اشتباه کوچک در فشردن دکمه روشن یا خاموش رایانه توسط ضابط غیرمتخصص، یا اتصال یک فلش‌مموری آلوده به سیستم توقیف‌شده، می‌تواند تاریخچه دسترسی‌ها را تغییر دهد و اعتبار دلیل را برای همیشه مخدوش سازد.

آلودگی و دست‌کاری صحنه جرم دیجیتال توسط ضابطین غیرمتخصص

در جرم‌شناسی مدرن، اصل «تبادل لوکارد» بیان می‌دارد که «هر تماس، ردی به جا می‌گذارد» (Mistek, 2018). در دنیای دیجیتال، این اصل با شدت بیشتری حاکم است. هر اقدامی روی سیستم دیجیتال، داده‌ای را تغییر می‌دهد. چالش اصلی زمانی رخ می‌دهد که ضابطین دادگستری که آموزش کافی ندیده‌اند، وارد صحنه جرم می‌شوند و با اقدامات ناشیانه، ادله را «آلوده» می‌کنند. «آلودگی و دست‌کاری صحنه جرم دیجیتال» توسط ضابطین غیرمتخصص، پاشنه آشیل دادرسی نوین و تهدیدی جدی علیه «اصل استحکام ادله» و «تمامیت داده‌ها» است.

یکی از رایج‌ترین اشتباهات ضابطین غیرمتخصص، تغییر وضعیت پاور دستگاه است. بسیاری از اطلاعات حیاتی، مانند پسوردها، اتصالات شبکه و برنامه‌های در حال اجرا، در *RAM* ذخیره می‌شوند. اگر ضابط به‌محض ورود به صحنه، برای جلوگیری از ادامه جرم، کابل برق را بکشد، تمام اطلاعات *RAM* می‌پرد و نابود می‌شود.

گاهی ضابط برای کپی‌کردن اطلاعات متهم، فلش‌مموری خود را به لپ‌تاپ متهم وصل می‌کند. اگر فلش‌مموری ضابط ویروسی باشد یا حاوی فایل‌های پرونده دیگری باشد، این فایل‌ها به سیستم متهم منتقل می‌شوند. این پدیده را «آلودگی متقاطع» می‌نامند. اگر در هارد دیسک متهم، پس از توقیف، فایلی پیدا شود که متعلق به پرونده دیگری است، قاضی نمی‌تواند به هیچ‌یک از محتویات آن هارد اعتماد کند. گزارش‌هایی وجود دارد که ضابطین به دلیل کمبود امکانات، از هارد دیسک‌های شخصی یا پاک‌سازی‌نشده برای ایمیج‌گیری استفاده کرده‌اند که منجر به مخدوش‌شدن ادله شده است.

صحنه جرم دیجیتال دیگر محدود به کامپیوتر نیست. تلویزیون هوشمند، ساعت هوشمند و حتی دستیار صوتی، بخشی از صحنه جرم هستند. ضابطین غیرمتخصص معمولاً این ابزارها را نادیده می‌گیرند یا با دست‌کاری آن‌ها، لاگ‌های حیاتی را پاک می‌کنند. آیین‌نامه‌های فعلی هنوز پروتکل دقیقی برای برخورد با صحنه‌های جرم مبتنی بر اینترنت اشیا ندارند. عدم جمع‌آوری این ادله یا جمع‌آوری غلط آن‌ها، باعث می‌شود که بخش بزرگی از حقیقت، مثلاً صدای ضبط‌شده محیط در لحظه قتل توسط تلویزیون هوشمند، از دست برود.

چالش‌های زنجیره حفاظتی ادله دیجیتال

زنجیره حفاظتی، مستندسازی دقیق و پیوسته تاریخچه یک دلیل از لحظه کشف تا لحظه ارائه در دادگاه است. در ادله دیجیتال، حفظ این زنجیره نیازمند فرآیندهای فنی پیچیده‌ای است که هرگونه گسست در آن، منجر به «بطلان دلیل» می‌شود.

سنگ‌بنای زنجیره حفاظتی دیجیتال، «مقدار هش» است. هش، یک اثر انگشت ریاضی منحصربه‌فرد برای هر فایل است. به‌محض توقیف هارد دیسک، ضابط متخصص باید از آن «ایمیج بیت‌به‌بیت» بگیرد و بلافاصله مقدار هش آن را محاسبه و در صورت‌جلسه قید کند. اگر شش ماه بعد در دادگاه، مقدار هش فایل موجود، حتی یک کاراکتر با هش صورت‌جلسه فرق داشته باشد، یعنی دلیل دست‌کاری شده است. چالش

اجرایی در ایران این است که بسیاری از ضابطین، به‌ویژه در شهرستان‌ها، مفهوم هش را نمی‌دانند یا تجهیزات لازم برای محاسبه آن در صحنه جرم را ندارند. آن‌ها صرفاً فایل‌ها را «*Copy-Paste*» می‌کنند. در کپی معمولی، متادیتاها تغییر می‌کند و هش نیز عوض می‌شود. نتیجه این است که وکیل مدافع می‌تواند به‌راحتی اصالت دلیل را زیر سؤال ببرد.

خطرناک‌ترین زمان برای ادله دیجیتال، فاصله زمانی بین «توقیف در صحنه» تا «تحویل به آزمایشگاه فارنزیک» است. در این بازه، اگر گوشی موبایل در پاکت ضدالکتریسیته قرار نگیرد، ممکن است از راه دور توسط همدستان متهم پاک‌سازی شود (Ferrazzano & Brighi, 2021). «ایزوله‌سازی شبکه» شرط اول زنجیره حفاظتی است. در پرونده‌های داخلی، موارد متعددی مشاهده شده که گوشی متهم، روشن و متصل به اینترنت، در کشوی میز بازپرس مانده و محتوای آن تغییر کرده است. این «سهل‌انگاری در نگهداری»، زنجیره حفاظتی را قطع می‌کند و ادله را از قابلیت استناد می‌اندازد.

زنجیره حفاظتی فقط مربوط به نگهداری نیست، بلکه شامل «فرآیند تحلیل» نیز می‌شود. وقتی کارشناس پلیس فتا روی داده‌ها کار می‌کند تا مدارک جرم را استخراج کند، باید از نرم‌افزارهای استاندارد استفاده کند که تمام اقدامات او را لاگ می‌کنند. اگر کارشناس از ابزارهای غیرمعتبر یا کرک‌شده استفاده کند، یا نتواند توضیح دهد که با چه متدی داده‌های حذف‌شده را بازیابی کرده است، زنجیره اعتبار دلیل قطع می‌شود. در دادگاه‌های ایران، قضات معمولاً به گزارش نهایی کارشناس بسنده می‌کنند و کمتر فرآیند فنی رسیدن به آن گزارش را که بخش مهمی از زنجیره حفاظتی است، بررسی می‌نمایند.

اطاله دادرسی ناشی از ارجاعات نادرست سیستمی و قطعی شبکه

اگرچه قانون‌گذار در ماده ۳ قانون آیین دادرسی کیفری، مراجع قضایی را مکلف به جلوگیری از هرگونه اطاله نموده و در ماده ۶۵۵ همان قانون، اعتبار دادرسی الکترونیکی را تثبیت کرده است، اما وابستگی مطلق فرآیندها به «شبکه ملی عدالت»، موضوع مواد ۶۵۰ و ۶۵۲ ق.آ.د.ک، موجب شده تا «قطعی سامانه» یا «ارجاعات الگوریتمی نادرست» توسط سیستم مدیریت پرونده (*CMS*)، به‌جای تسهیل، به مانعی در برابر «حق رسیدگی در مهلت معقول» تبدیل شود. این چالش فنی، برخلاف تبصره ماده ۶۵۵ که جایگزینی روش‌های سنتی را در زمان اختلال پیش‌بینی کرده، در عمل منجر به توقف دادرسی و سرگردانی اصحاب دعوا میان شعب می‌گردد. تداوم این وضعیت، نه‌تنها امنیت روانی متهم را مخدوش می‌سازد، بلکه در موارد بازداشت موقت، طولانی‌شدن فرآیند به دلیل نقص فنی، مصداق بارز «توقیف غیرموجه» و مغایر با حقوق شهروندی و اصول دادرسی منصفانه است؛ چراکه سرنوشت آزادی افراد نباید به پایداری سرورها یا دقت الگوریتم‌های توزیع پرونده گره خورده باشد.

در سیستم‌های نوین قضایی ایران، تلاش شده تا ارجاع شکوائیه‌ها از دفاتر خدمات قضایی به دادسراها، به‌صورت هوشمند و بر اساس «عناوین اتهامی» انجام شود (Khalouei Tafti & Aghaabbasi, 2021). الگوریتم‌های فعلی، توانایی تشخیص ماهیت دقیق جرم را ندارند و صرفاً بر اساس «کلیدواژه» عمل می‌کنند.

در جرایم سایبری، «زمان» فاکتور حیاتی است. ردپای دیجیتال، مانند *IP* یا لاگ سرور، فرّار است و ممکن است در چند ساعت پاک شود. دسترسی ضابطین و بازپرسان به سامانه‌های استعلام، مانند سامانه سیاق برای مسدودی حساب یا سامانه استعلام خطوط، باید ۲۴ساعته و بدون قطعی باشد.

چالش فنی دیگر، عدم اتصال کامل سامانه‌های ضابطین (ناجا) با سامانه قضایی (*CMS*) است. در بسیاری از موارد، گزارش پلیس فتا به‌صورت الکترونیکی ارسال می‌شود، اما ضمایم آن، مثل فایل‌های لاگ حجیم یا ویدئوها، به دلیل محدودیت حجم آپلود در سامانه، باید روی *CD* رایت شده و به‌صورت فیزیکی (پیک) ارسال شود.

ابهام در صلاحیت محلی در جرایم سایبری و سرگردانی ارباب‌رجوع

یکی از پیچیده‌ترین معضلات دادرسی الکترونیکی، تعیین «محل وقوع جرم» در فضایی است که «مکان» ندارد.

در جرایم رایانه‌ای، مثل کلاهبرداری اینترنتی، رکن مادی جرم در بستر شبکه رخ می‌دهد. در تحلیل ماده ۳۱۰ و رأی وحدت رویه شماره ۷۲۹ دیوان عالی کشور، باید گفت که دیوان تلاش کرده با ملاک قراردادن «محل افتتاح حساب بانکی بزه‌دیده» (محل مبدأ انتقال وجه)، مشکل را حل کند (Khaleghi, 2024). استدلال این است که جرم زمانی محقق می‌شود که پول از حساب قربانی کسر شود. اما این راه‌حل نیز چالش‌زاست. امروزه افتتاح حساب‌ها نیز «الکترونیکی» و بدون شعبه فیزیکی (نئوبانک‌ها) شده است. اگر بانک قربانی، شعبه فیزیکی نداشته باشد و کاملاً مجازی باشد، صلاحیت با کجاست؟ اینجاست که قوانین سنتی در برابر واقعیت‌های دیجیتال کم می‌آورند و منجر به صدور قرارهای عدم صلاحیت متعدد بین دادسراهای شهرهای مختلف می‌شوند.

ابهام در صلاحیت، باعث می‌شود بزه‌دیده نداند کجا شکایت کند. او در تهران شکایت می‌کند، دادسرای تهران می‌گوید چون حساب مقصد در مشهد است، عدم صلاحیت می‌زند. پرونده به مشهد می‌رود، آنجا می‌گویند چون *IP* متهم در تبریز ردیابی شده، عدم صلاحیت می‌زنند. این وضعیت به «پاس‌کاری قضایی» منجر می‌شود که بزرگ‌ترین آفت دادرسی منصفانه است. در این فاصله زمانی که پرونده بین استان‌ها می‌چرخد، ادله دیجیتال از بین می‌روند و متهم متواری می‌شود.

بزرگ‌ترین چالش صلاحیت، جایی است که، مانند تلگرام یا اینستاگرام، داده‌ها در «خارج از کشور» هستند؛ ضابطین ایرانی برای دسترسی به این داده‌ها با مانع «حاکمیت داده‌ها» روبه‌رو هستند. اگر سرور در آمریکاست، قاضی ایرانی صلاحیت دستور تفتیش آن را ندارد. در نتیجه، بسیاری از پرونده‌های سایبری در ایران به دلیل «عدم دسترسی به دلیل» و «عدم صلاحیت بین‌المللی»، مختومه می‌شوند یا بلاتکلیف می‌مانند. این یک «بن‌بست عدالت» است که ناشی از عدم تطابق مرزهای جغرافیایی با مرزهای دیجیتال است.

چالش‌های صلاحیت و نیابت قضایی

قواعد صلاحیت در آیین دادرسی کیفری، بر پایه مفهوم «جغرافیای جرم» استوار شده‌اند. ماده ۳۱۰ قانون آیین دادرسی کیفری، اصل را بر صلاحیت «دادگاه محل وقوع جرم» قرار داده است. این قاعده در دنیای فیزیکی که جرم در یک نقطه مکانی مشخص رخ می‌دهد، منطقی و کارآمد است. اما فضای سایبر، فضایی «بی‌مکان» و «بی‌زمان» است. یک کلاهبرداری اینترنتی ممکن است توسط هکری در مشهد طراحی شود، سرور آن در کانادا باشد، بزه‌دیده در تهران پول را واریز کند و بانک مقصد در اصفهان باشد. در چنین سناریویی، «محل وقوع جرم» کجاست؟

بحران صلاحیت

تعارض صلاحیت، زمانی رخ می‌دهد که دو یا چند مرجع قضایی، هم‌زمان خود را صالح به رسیدگی بدانند یا هیچ‌کدام خود را صالح ندانند. در جرایم سایبری، به دلیل ماهیت «چندمکانی» جرم، تعارض صلاحیت به یک بحران تبدیل شده است. برخی جرایم سایبری، مانند «انتشار تصاویر مستهجن» یا «توهین آنلاین»، جرایمی هستند که در لحظه آپلود، در تمام ایران قابل مشاهده‌اند. طبق اصول دادرسی، هر جایی که جرم واقع شده، دادگاه آنجا صالح است. آیا این یعنی تمام دادگاه‌های ایران صالح‌اند؟ این وضعیت منجر به «تورم پرونده» و خطر «محاکمه مضاعف»

می‌شود. ممکن است علیه یک فرد بابت یک پست اینستاگرامی، در ۱۰ شهر مختلف شکایت شود. سامانه *CMS* باید هوشمند باشد و با شناسایی کد ملی متهم، تمام پرونده‌ها را تجمیع کند. اما در عمل، به دلیل عدم ثبت صحیح موضوعات یا تأخیر در ثبت، متهم مجبور می‌شود به شهرهای مختلف سفر کند تا ثابت کند «من بابت این جرم قبلاً در تهران محاکمه شده‌ام». این نقص در یکپارچگی صلاحیت، اصل «اعتبار امر مختومه» را تهدید می‌کند.

چالش‌های اجرای نیابت قضایی الکترونیک بین حوزه‌های قضایی

در نیابت الکترونیک، چالش اصلی، «کیفیت اجرای نیابت» است. در نیابت قضایی، قاضی مجری نیابت، معمولاً انگیزه و اشراف قاضی اصلی را ندارد (Rahmdel, 2015).

اجرای نیابت برای «تفتیش منزل و توقیف رایانه» نیازمند تخصص است. بازپرس تهران دستور می‌دهد: «سیستم متهم بررسی و ادله استخراج شود». اما اگر در شهر مقصد، پلیس فتا یا کارشناس متخصص وجود نداشته باشد، یا قاضی نایب دستور را کلی و مبهم به ضابط بدهد، چه اتفاقی می‌افتد؟ اجرای نیابت‌های فنی توسط مراجع غیرتخصصی، عامل اصلی «آلودگی صحنه جرم» است. قاضی اصلی نمی‌تواند بر نحوه توقیف نظارت کند و قاضی نایب هم دانش فنی ندارد. نتیجه این است که ادله‌ای که از طریق نیابت جمع شده، اغلب در دادگاه به دلیل نقص زنجیره حفاظتی باطل می‌شوند. سامانه مدیریت پرونده (*CMS*) در بخش نیابت دارای باگ‌های فرآیندی است. گاهی حجم ضمایم پرونده، مثلاً فیلم دوربین مداربسته، زیاد است و از طریق سیستم نیابت الکترونیک ارسال نمی‌شود.

اعتبار تحقیقات انجام‌شده از طریق ویدئوکنفرانس نیابتی

استفاده از ویدئوکنفرانس برای انجام تحقیقات نیابتی، اگرچه جایگزین سفر فیزیکی شده، اما سؤالی بنیادین را در نظریه ادله اثبات دعوا مطرح کرده است: آیا «مشاهده از طریق مانیتور» با «مشاهده مستقیم»، اعتبار یکسانی دارد؟ در فقه و حقوق سنتی، اصل بر «مباشرت قاضی» و «معاینه مستقیم» است. یکی از ابزارهای مهم قاضی برای کشف حقیقت، «فراست» یا شمّ قضایی است که از مشاهده دقیق رفتار متهم، لرزش صدا، تعریق پیشانی و حرکات چشم حاصل می‌شود. «اقناع وجدانی قاضی» نیازمند ارتباط بی‌واسطه است (Ashouri, 2023). در تحقیقات نیابتی ویدئویی، تکنولوژی مانند فیلتر عمل می‌کند. کیفیت پایین تصویر، تأخیر در صدا و کادربندی محدود دوربین، باعث می‌شود که قاضی نتواند سیگنال‌های غیرکلامی را دریافت کند. در جلسات ویدئویی، قضات تمایل کمتری به باورکردن اظهارات متهم دارند و همدلی کمتری نشان می‌دهند؛ بنابراین، تحقیقاتی که از راه دور انجام می‌شود، ممکن است از نظر «شکلی» صحیح باشد، اما از نظر «ماهوی» فاقد عمق و دقت لازم برای کشف حقیقت است و اعتبار اقناع‌کنندگی کمتری دارد.

شهادت شهود، مبتنی بر «حضور» است. اعتبار شهادت به این است که شاهد در محضر دادگاه و زیر سایه ابهت قاضی سوگند یاد کند. در نیابت الکترونیک، شاهد در شهر خود یا حتی در خانه خود، جلوی دوربین می‌نشیند. فضای غیررسمی خانه یا دفتر کار، از جدیت سوگند می‌کاهد. علاوه بر این، امکان «تبانی» در شهادت از راه دور بسیار بیشتر است.

موانع قانونی ضبط و ثبت تحقیقات مقدماتی الکترونیک

تصور می‌شد که با ضبط ویدئویی جلسات بازجویی، دیگر نیازی به صورت‌جلسات طولانی و ناخوانای دستی نیست. اما موانع قانونی و سنتی، باعث ایجاد یک «بوروکراسی موازی» شده‌اند که در آن، هم فیلم ضبط می‌شود و هم کاغذ نوشته می‌شود، و جالب آنکه «کاغذ» همچنان اعتبار بیشتری دارد!

«موانع قانونی ضبط و ثبت تحقیقات مقدماتی الکترونیک»، بیانگر اصطکاک میان «شفافیت دیجیتال» و «اصل محرمانگی تحقیقات»، موضوع ماده ۹۱ قانون آیین دادرسی کیفری، است. اگرچه قانون‌گذار در ماده ۶۵۹ قانون آیین دادرسی کیفری، جواز برگزاری جلسات تحقیق از طریق ویدئوکنفرانس را صادر نموده و طبق ماده ۶۵۵ همان قانون، صورت‌جلسات الکترونیکی را معتبر دانسته است، اما چالش اصلی در «تضمین تمامیت» و «محرمانگی آرشیو» این داده‌های حساس نهفته است. خطر حقوقی آنجاست که ضبط تصویر متهم پیش از اثبات جرم، در صورت فقدان زیرساخت امنیتی نفوذناپذیر، متهم را در معرض هتک حیثیت و نقض ماده ۴ قانون آیین دادرسی کیفری قرار می‌دهد و حتی می‌تواند مصداق جرم انتشار اسرار، موضوع ماده ۷۴۵ قانون مجازات اسلامی، باشد. علاوه بر این، فقدان پروتکل‌های قانونی سخت‌گیرانه برای «اصالت‌سنجی فنی» فایل‌های ضبط‌شده و مقابله با جعل‌های عمیق، ارزش اثباتی این تحقیقات را متزلزل کرده و «حق دفاع متهم» را در چالش با ادله‌ای که امکان دست‌کاری در آن‌ها وجود دارد، تضییع می‌نماید که این امر با استانداردهای دادرسی عادلانه مغایرت دارد.

راهکارهای تضمین اصول در تحقیقات مقدماتی

آسیب‌شناسی صورت‌گرفته در مبحث پیشین، حقیقتی انکارناپذیر را آشکار ساخت: نظام عدالت کیفری ایران در مواجهه با سیل خروشان تحولات دیجیتال، دچار نوعی «تأخر حقوقی» و «ناهمگونی زیرساختی» شده است. برای گذر از این چالش‌ها، راهکارهایی در این قسمت ارائه شده است. علاوه بر این، انزواگرایی در عصر اینترنت معنا ندارد. بهره‌گیری از تجربیات تطبیقی و استانداردهای جهانی، مانند کنوانسیون بوداپست و مقررات اتحادیه اروپا، می‌تواند راه میان‌بری برای پرکردن خلأهای موجود در حقوق داخلی ایران باشد.

راهکارهای تقنینی (اصلاح قوانین)

تأمین امنیت قضایی در عصر دیجیتال، بیش از آنکه نیازمند خرید سرورهای قدرتمند یا توسعه نرم‌افزارها باشد، نیازمند «معماری مجدد قوانین» است. راهکارهای تقنینی در این قسمت، بر محور «محدودسازی قدرت» و «شفاف‌سازی فرآیندها» استوار است.

تدوین ضوابط دقیق برای صدور مجوز تفتیش داده‌های رایانه‌ای

در حقوق سنتی، وقتی قاضی حکم بازرسی منزل را صادر می‌کرد، محدوده فیزیکی مشخص بود؛ اما در فضای دیجیتال، صدور دستور «تفتیش رایانه متهم»، حکمی مبهم و خطرناک است. آیا این دستور شامل ایمیل‌های او، فضای ابری، تاریخچه مرورگر و فایل‌های حذف‌شده نیز می‌شود؟ فقدان «اصل تخصص» در مجوزهای تفتیش دیجیتال، بزرگ‌ترین حفره قانونی در آیین دادرسی فعلی ایران است.

مهم‌ترین خلأ قانونی در مواد ۱۳۷ و ۶۶۷ قانون آیین دادرسی کیفری، کلی‌بودن عبارات است. رویه عملی دادسراها این است که بازپرس دستور می‌دهد: «گوشی متهم توقیف و جهت استخراج ادله به پلیس فتا ارسال شود». این یک «مجوز عام» است که در قرن ۱۸ میلادی منسوخ شده بود، اما در عصر دیجیتال احیا شده است.

چنین دستوری به ضابط اجازه می‌دهد تا نقش «قاضی تحقیق» را بازی کند و در تمام زندگی متهم سرک بکشد (Rahmdel, 2015). اصلاح ماده ۶۶۷ آ.د.ک و الزام بازپرس به تعیین «دامنه دقیق تفتیش» در متن دستور قضایی، راهکار پیشنهادی این مقاله است. قانون باید بازپرس را مکلف کند که در دستور خود، نوع داده‌های مورد جست‌وجو، بازه زمانی و مکان دیجیتال را قید کند.

قانون فعلی، تمایز دقیقی بین شدت مجوز لازم برای دسترسی به «محتوای پیام» و «داده‌های ترافیکی/متادیتا» قائل نشده است. اگرچه ماده ۶۶۸ محدودیت‌هایی دارد، اما در عمل، دسترسی به لیست تماس‌ها بسیار آسان‌تر گرفته می‌شود. قانون باید تصریح کند که «پروفایل‌سازی» افراد بر اساس داده‌های ترافیکی، بدون وجود اتهام مشخص، ممنوع است.

در حقوق فیزیکی، اگر پلیس دنبال اسلحه باشد و مواد مخدر ببیند، می‌تواند ضبط کند؛ اما در فضای دیجیتال، این قاعده خطرناک است. چون در فضای دیجیتال، فایل‌ها درهم‌آمیخته‌اند، جست‌وجو برای یک فایل مالی، ناگزیر چشم ضابط را به عکس‌های خصوصی هم باز می‌کند. اگر قانون اجازه دهد که ضابط هر جرم دیگری را هم که دید گزارش کند، حریم خصوصی نابود می‌شود. افزودن تبصره‌ای به قانون آیین دادرسی که مقرر دارد: «چنانچه ضابط در حین تفتیش داده‌های موضوع مجوز، به داده‌های مجرمانه دیگری برخورد کرد که خارج از موضوع حکم است، حق توقیف یا گزارش آن را ندارد، مگر آنکه جرم مشهود جنایی باشد». در غیر این صورت، ضابط باید فعالیت را متوقف کرده و تقاضای «مجوز تکمیلی» از بازپرس نماید. این وقفه، امکان نظارت قضایی را فراهم می‌کند.

قوانین فعلی ایران در مورد تفتیش داده‌هایی که روی دستگاه نیستند، ساکت یا مبهم‌اند. وقتی گوشی متهم توقیف می‌شود، آیا ضابط حق دارد روی آیکون تلگرام کلیک کند و وارد سروری شود که در کشور دیگری است؟ قانون باید صراحتاً «تفتیش از راه دور» را به‌عنوان یک اقدام تفتیشی متمایز شناسایی کند. باید مقرر شود که: «دسترسی به داده‌های ذخیره‌شده در فضای ابری، نیازمند مجوز قضایی مستقل است و حکم تفتیش سخت‌افزار، به معنای حکم ورود به حساب‌های کاربری آنلاین نیست». همچنین، در مواردی که سرور در خارج از کشور است، قانون باید ضابطین را ملزم به رعایت پروتکل‌های معاضدت قضایی یا استفاده از روش‌های قانونی بین‌المللی نماید تا از بی‌اعتباری ادله در مراجع بین‌المللی جلوگیری شود.

تعیین بطلان برای ادله دیجیتال غیرقانونی

یکی از بزرگ‌ترین ضعف‌های نظام دادرسی کیفری ایران، فقدان صراحت در خصوص «ضمانت اجرای نقض قوانین تحصیل دلیل» است. اگر ضابطی بدون حکم قضایی گوشی متهم را هک کند و مدارک جرم را بیابد، آیا این مدارک در دادگاه قابل استناد است؟ رویه قضایی ایران، تحت تأثیر اصل آزادی ادله، متمایل به پذیرش است، اما این رویکرد در دادرسی الکترونیکی فاجعه‌بار است.

اصلاح ماده ۳۶ قانون آیین دادرسی کیفری یا افزودن ماده‌ای به بخش جرایم رایانه‌ای با این مضمون: «هرگاه ادله الکترونیکی با نقض آشکار حریم خصوصی، بدون مجوز قضایی، یا با توسل به روش‌های غیرقانونی فنی، مانند هک غیرمجاز یا بدافزار، تحصیل شده باشد، فاقد اعتبار بوده و قاضی نمی‌تواند علم خود را بر آن استوار سازد».

قانون باید صراحتاً اعلام کند که «رعایت زنجیره حفاظتی فنی، شرط صحت دلیل دیجیتال است». باید مقرر شود که اگر صورت‌جلسه توقیف فاقد «کد هش» باشد، یا مستندات انتقال امن داده‌ها به آزمایشگاه ناقص باشد، آن دلیل «فرض بر آلودگی» داشته و از عداد دلایل خارج شود، مگر آنکه دادستان سلامت آن را با نظر هیئت کارشناسی اثبات کند.

تدوین ماده قانونی که ضابطین را از «تحریک به جرم» در فضای مجازی منع کند و مقرر دارد: «ادله‌ای که در نتیجه تحریک، فریب یا زمینه‌سازی مستقیم ضابطین از افراد به دست آمده باشد، در صورتی که فرد بدون دخالت ضابط مرتکب آن جرم نمی‌شد، باطل و بلااثر است».

قانون باید صراحتاً «اجبار به افشای رمز عبور» یا «بازکردن قفل بیومتریک با زور»، گرفتن انگشت متهم به زور روی سنسور، را مصداق شکنجه یا رفتار غیرقانونی بداند و ادله مستخرج از آن را مشمول قاعده بطلان قرار دهد. این امر، تضمین‌کننده واقعی اصل منع شکنجه در عصر دیجیتال است.

اصلاح قوانین ابلاغ جهت تضمین «رؤیت واقعی» در جرایم مهم

قانون آیین دادرسی کیفری باید رویکرد «مبتنی بر ریسک» را اتخاذ کند. اصلاح ماده ۱۷۵ و ۶۵۵ آ.د.ک بدین‌صورت که: «در جرایم مستوجب سلب حیات، حبس‌های طولانی‌مدت (درجه ۱ تا ۴)، شلاق و جرایم منافی عفت، اکتفا به ابلاغ الکترونیکی (بارگذاری در سامانه) ممنوع است. در این جرایم، چنانچه متهم ظرف ۴۸ ساعت پس از بارگذاری ابلاغیه، آن را مشاهده نکند (عدم رؤیت سیستمی)، دادسرا مکلف است از طریق تماس تلفنی ضبط‌شده، ارسال پیامک به بستگان درجه‌یک (که شماره آن‌ها در سامانه ثبت شده) یا اعزام مأمور ابلاغ، از آگاهی واقعی متهم اطمینان حاصل کند. صدور حکم غیابی یا جلب متهم در این جرایم، منوط به احراز قطعی اطلاع متهم است.»

همچنین، به‌رسمیت‌شناختن «حق انتخاب روش ابلاغ» برای گروه‌های آسیب‌پذیر لازم و ضروری است. قانون فعلی همه را مجبور به دیجیتالی‌شدن می‌کند. راهکار تقنینی، افزودن تبصره‌ای به ماده ۱۷۵ آ.د.ک است: «افراد بالای ۶۵ سال، افراد فاقد سواد دیجیتال و ساکنان مناطق فاقد پوشش اینترنتی مناسب، حق دارند در زمان تشکیل پرونده، درخواست ابلاغ سنتی (کاغذی) یا ابلاغ تلفنی نمایند. قوه قضاییه مکلف است برای این دسته از شهروندان، کانال‌های جایگزین را فعال نگه دارد.» این قانون، تبعیض ساختاری علیه فقرا و سالمندان را حذف می‌کند.

جرم‌انگاری نقض داده‌های خصوصی متهم توسط ضابطین

در دادرسی الکترونیکی، اگر مأموری عکس‌های خصوصی متهم را از گوشی‌اش استخراج و در گروه دوستانش منتشر کند، یا فیلم بازجویی او را بفروشد، آسیبی به‌مراتب بیشتر از ضرب‌وجرح فیزیکی وارد کرده است؛ با این حال، قوانین فعلی، مانند ماده ۷۵۴ ق.م.ا یا قانون جرایم رایانه‌ای، مجازات‌های سبک و کلی برای این اعمال در نظر گرفته‌اند که بازدارنده نیست. تصویب ماده‌واحده‌ای تحت عنوان «جرم‌انگاری نقض حریم داده‌های قضایی» با این مضمون: «هر یک از مقامات قضایی، ضابطین دادگستری، کارکنان اداری یا پیمانکاران فنی که به مناسبت وظیفه به داده‌های رایانه‌ای یا مخابراتی متهمان یا شکات دسترسی دارند، چنانچه این داده‌ها را برخلاف قانون افشا کنند، در دسترس افراد غیرمجاز قرار دهند، یا از آن‌ها استفاده شخصی نمایند، به حبس درجه ۴ (۵ تا ۱۰ سال) و انفصال دائم از خدمات دولتی محکوم می‌شوند.» نکته مهم در این پیشنهاد، «تشدید مجازات» و «انفصال دائم» است تا هزینه افشای اطلاعات، مانند فیلم‌های بازجویی، برای مأموران بسیار بالا رود.

گاهی ضابط سوءنیت ندارد، اما با سهل‌انگاری، مثلاً گم‌کردن فلش‌ممووری حاوی اطلاعات پرونده یا استفاده از لپ‌تاپ ناامن شخصی، باعث نشت اطلاعات می‌شود. قانون فعلی برای این «ترک فعل»، ضمانت اجرای کیفری قوی ندارد. راهکار تقنینی، جرم‌انگاری «تقصیر در حفظ داده‌های قضایی» است. قانون باید مقرر کند: «هرگاه در اثر بی‌احتیاطی، بی‌مبالاتی یا عدم رعایت پروتکل‌های امنیتی توسط ضابطین یا کارکنان، داده‌های خصوصی اصحاب دعوا افشا شود یا از بین برود، مرتکب به مجازات انتظامی درجه‌یک و جبران کامل خسارت معنوی محکوم می‌گردد.»

راهکارهای فنی و زیرساختی

بهترین قوانین هم بدون ابزار مناسب، نوشته‌هایی بر روی کاغذند. در عصر دیجیتال، تضمین اصول دادرسی، بیش از آنکه نیازمند «بایدها و نبایدهای اخلاقی» باشد، نیازمند «عدالت مبتنی بر طراحی» است. این مفهوم که از دکترین «حریم خصوصی در طراحی» وام گرفته شده، بیانگر این است که زیرساخت‌های فنی دادرسی، اعم از سخت‌افزارهای پلیسی و نرم‌افزارهای قضایی، باید ذاتاً و به‌صورت پیش‌فرض، حامی حقوق متهم باشند، نه اینکه صرفاً ابزاری برای تسریع سرکوب یا مدیریت پرونده باشند (Waldman, 2018).

تجهیز ضابطین به آزمایشگاه‌های سیار جرم‌یابی دیجیتال

در مدل فعلی تحقیقات مقدماتی در ایران، وقتی جرمی سایبری رخ می‌دهد یا نیاز به تفتیش ادله دیجیتال است، ضابطین به محل اعزام می‌شوند، تمام تجهیزات (لپ‌تاپ، کیس کامپیوتر، هارد اکسترنال و...) را توقیف می‌کنند، صورت‌جلسه می‌کنند و با خود به اداره پلیس فتا می‌برند. در آنجا، تجهیزات در نوبت بررسی قرار می‌گیرند که ممکن است هفته‌ها طول بکشد. این فرآیند سنتی، دارای آسیب‌های فنی و حقوقی جبران‌ناپذیری است که تنها با تغییر استراتژی به سمت «جرم‌یابی در صحنه» قابل حل است.

راهکار جهانی برای این معضل، استفاده از واحدهای سیار جرم‌یابی است. این واحدها که معمولاً به‌صورت ون‌های مجهز یا کیف‌های عملیاتی هستند، دارای تجهیزاتی هستند که امکان «ایمیج‌گیری زنده» از *RAM* و هارد دیسک را در همان لحظه ورود به صحنه فراهم می‌کنند، قبل از اینکه متهم فرصت کند رمزها را فعال کند یا سیستم خاموش شود (Soni, 2024). در حقوق ایران، اطاله دادرسی ناشی از صف طولانی آزمایشگاه‌های مرکزی پلیس فتا، گاهی باعث می‌شود متهم ماه‌ها در بازداشت بماند تا نتیجه بررسی هارد بیاید. آزمایشگاه سیار، این زمان را به چند ساعت تقلیل می‌دهد. مهم‌ترین ابزار در آزمایشگاه سیار، سخت‌افزار «رایت بلاکر» است (Teslenko, 2024). وقتی ضابط می‌خواهد فلش‌مموری متهم را بررسی کند، اگر آن را مستقیماً به لپ‌تاپ خود بزند، سیستم‌عامل ویندوز به‌طور خودکار تغییراتی در متادیتاهای فایل ایجاد می‌کند. این دستگاه کوچک که واسط بین کامپیوتر متهم و کامپیوتر ضابط است، اجازه می‌دهد اطلاعات «خوانده» شود، اما حتی یک بیت روی آن «نوشته» یا تغییر داده نشود (Taghiniam & Ghanbari, 2024). تجهیز کلانتری‌ها و تیم‌های گشت به این ابزار ارزان‌قیمت اما حیاتی، گام اول در استانداردسازی کشف جرم است.

امروزه پلیس‌های پیشرفته جهان مجهز به «کیوسک‌های استخراج موبایل» در خودروهای گشت هستند که می‌توانند در ۵ دقیقه، داده‌های منتخب را استخراج کنند و گوشی را به شهروند پس دهند. پیاده‌سازی این زیرساخت در ایران، حجم عظیمی از پرونده‌های توقیف اموال را کاهش می‌دهد.

استفاده از فناوری بلاک‌چین برای ثبت تغییرناپذیر ادله

زنجیره حفاظتی در حال حاضر مبتنی بر «کاغذ» و «اعتماد به پلیس» است. ضابط صورت‌جلسه می‌کند که «هارد دیسک با هش شماره *X* توقیف شد». اما چه تضمینی وجود دارد که فردا این صورت‌جلسه عوض نشود؟ یا عدد هش در دیتابیس پلیس دست‌کاری نگردد؟ فناوری بلاک‌چین، با ویژگی‌های ذاتی خود، یعنی غیرمتمرکزبودن و تغییرناپذیری، می‌تواند پارادایم «اعتماد» را در دادرسی کیفری تغییر دهد (Teslenko, 2024).

راهکار، ثبت «اثر انگشت دیجیتال» (*Hash*) ادله روی بلاک‌چین است. هالاهان و همکاران مدلی را پیشنهاد می‌دهند که در آن، نرم‌افزارهای جرم‌یابی، به‌محض استخراج داده، به‌طور خودکار هش آن را تولید کرده و به‌عنوان یک «تراکنش» روی یک بلاک‌چین قضایی ثبت کنند (Halahan et al., 2023). این تراکنش شامل مقدار هش، زمان دقیق و شناسه دیجیتال ضابط است. به‌محض ثبت، این رکورد در هزاران نود (*Node*) توزیع می‌شود و دیگر هیچ‌کس، حتی رئیس پلیس یا قاضی پرونده، نمی‌تواند آن را پاک کند یا تغییر دهد. این راهکار، اصل «تمامیت ادله» را از یک ادعای قابل خدشه، به یک «حقیقت ریاضی» تبدیل می‌کند که وکیل مدافع نمی‌تواند آن را انکار کند.

ایجاد بستر امن ارتباط تصویری وکیل و متهم در بازداشتگاه

یکی از چالش‌برانگیزترین نقاط تلاقی تکنولوژی و حقوق دفاعی، مسئله ارتباط محرمانه وکیل و موکل در بستر دادرسی الکترونیکی است. در دادرسی سنتی، این حق با «خلوت‌کردن اتاق» یا «نجواکردن در گوش متهم» تأمین می‌شد. اما در دادرسی آنلاین، وقتی متهم در زندان است و وکیل در دفتر کار خود، و هر دو از طریق یک پلتفرم ویدئوکنفرانس که تحت کنترل قاضی یا بازپرس است، با هم در ارتباط‌اند، مفهوم «خلوت» از بین می‌رود. اگر وکیل بخواهد نکته‌ای را به موکلش تذکر دهد، مثلاً: «به این سؤال پاسخ نده» یا «این حق توست که سکوت کنی»، بازپرس و منشی دادگاه نیز آن را می‌شنوند. این وضعیت، نقض آشکار اصل محرمانگی ارتباط وکیل و موکل و تضعیف حق دفاع است. راهکار فنی برای حل این معضل، طراحی و پیاده‌سازی «اتاق‌های ملاقات مجازی امن» با قابلیت‌های رمزنگاری پیشرفته است که در برخی از محاکم آمریکا به کار گرفته شده است (Ray, 2025). نرم‌افزارهای عمومی ویدئوکنفرانس، مانند اسکایپ یا ادوبی کانکت، برای کلاس درس یا جلسات اداری طراحی شده‌اند، نه برای بازجویی کیفری. در این نرم‌افزارها، مدیر جلسه بر تمام صداها مسلط است. برای دادرسی کیفری، نیازمند پلتفرم اختصاصی هستیم که قابلیت «تفکیک کانال‌های صوتی» را داشته باشد.

رابط کاربری (*UI*) نرم‌افزار دادگاه باید دارای دکمه‌ای تحت عنوان «درخواست مشورت خصوصی» باشد که تنها در پنل وکیل فعال است. زمانی که وکیل این دکمه را فشار می‌دهد، سیستم باید به‌طور خودکار اقدامات زیر را انجام دهد:

قطع موقت صدای وکیل و متهم برای قاضی: میکروفون وکیل و متهم برای قاضی و منشی قطع (*Mute*) می‌شود، اما تصویر آن‌ها همچنان باقی می‌ماند تا قاضی نظارت تصویری داشته باشد که تبانی فیزیکی یا ردوبدل‌کردن شیء صورت نگیرد.

ایجاد کانال صوتی اختصاصی: یک کانال صوتی رمزنگاری‌شده و مجزا بین وکیل و متهم برقرار می‌شود که هیچ‌کس دیگری، حتی ادمین سیستم، به آن دسترسی ندارد.

توقف ضبط صدا: اگر جلسه در حال ضبط‌شدن است، سیستم باید به‌طور خودکار ضبط صدای این کانال خصوصی را متوقف کند تا در آرشیو پرونده نیز ثبت نشود.

این معماری فنی، معادل دیجیتال همان «درگوشی صحبت‌کردن» در دادگاه فیزیکی است. بدون این قابلیت، وکیل در جلسه آنلاین «منفعل» می‌شود و نمی‌تواند استراتژی دفاعی خود را پیاده کند. در استانداردهای بین‌المللی، وجود چنین قابلیتی پیش‌شرط اعتبار دادرسی‌های از راه دور دانسته شده است (Ramos, 2021). اعتماد وکیل و متهم به این بستر، تنها با ادعای شفاهی جلب نمی‌شود. زیرساخت فنی باید تضمین کند که مکالمات آن‌ها شنود نمی‌شود. استفاده از پروتکل رمزنگاری سرتاسری لازم است. در این پروتکل، کلید رمزگشایی تنها در دستگاه وکیل و دستگاه متهم، در کیوسک زندان، تولید می‌شود و سرور مرکزی قوه قضاییه صرفاً نقش واسط انتقال داده‌های رمزشده را دارد و توانایی بازکردن و شنود آن را ندارد. محرمانگی ارتباط وکیل، جزو «اسرار حرفه‌ای» است و سطح حفاظتی آن باید بالاتر از سایر داده‌های پرونده باشد. پیاده‌سازی پروتکل رمزنگاری سرتاسری باعث می‌شود که حتی اگر هکری به سرور دادگستری نفوذ کند یا یک کارمند متخلف بخواهد مکالمات خصوصی وکیل را استراق سمع کند، تنها با مشتی داده نامفهوم روبه‌رو شود.

راهکار فنی، ایجاد قابلیت «اشتراک‌گذاری خصوصی» است. سیستم باید فضایی ابری و موقت ایجاد کند که وکیل بتواند فایل را در آن آپلود کند و متهم در کیوسک زندان آن را ببیند و حتی با قلم نوری امضا کند، بدون اینکه فایل در دسترس سایر طرفین پرونده قرار گیرد. در بحث

حقوق دفاعی، دسترسی متهم به اسناد دفاعی حیاتی است (Khaleghi, 2024). این راهکار فنی، معادل همان لحظه‌ای است که در دادگاه سنتی، وکیل پوشه‌ای را از کیفش درمی‌آورد و به دست موکل می‌دهد تا بخواند. تکنولوژی باید عیناً همین قابلیت را شبیه‌سازی کند.

طراحی هشدارهای سیستمی برای رعایت حقوق متهم در نرم‌افزار *CMS*

در سیستم‌های بوروکراتیک و پرفشار قضایی، بسیاری از نقض‌های حقوق بشری نه از روی «سوءنیت»، بلکه ناشی از «فراموشی»، «خستگی» یا «عجله» مقام قضایی است. بازپرس ممکن است فراموش کند که قرار بازداشت موقت ۲۴ ساعت است و باید تمدید شود، یا فراموش کند حق سکوت را تفهیم نماید. در پارادایم «عدالت مبتنی بر طراحی»، سامانه مدیریت پرونده (*CMS*) نباید یک ماشین تایپ منفعل باشد؛ بلکه باید نقش یک «دستیار هوشمند ناظر» را ایفا کند که با استفاده از «معماری انتخاب» و نظریه «تلنگر»، رعایت قانون را تضمین نماید (Greene & Bornstein, 2013).

بازداشت موقت، سلب آزادی است و باید در کمترین زمان ممکن تعیین تکلیف شود. طبق ماده ۲۴۲ آ.د.ک، بازداشت موقت سقف زمانی دارد. در سیستم سنتی یا سیستم‌های فعلی، نظارت بر مواعد بازداشت دستی است. پرونده در قفسه می‌ماند و ممکن است متهم روزها بیش از مهلت قانونی در زندان بماند تا بازپرس یادش بیاید قرار را تمدید یا فک کند.

راهکار فنی، طراحی سیستم «شمارش معکوس» و «قفل سیستمی» است. هشدار زرد باید ۴۸ ساعت قبل از انقضای مهلت قانونی بازداشت، توسط سیستم به بازپرس و دادستان پیامک و نوتیفیکیشن هشدار ارسال کند.

هشدار قرمز باید به این صورت تعیین شود که ۲۴ ساعت قبل، سیستم اجازه انجام هرگونه اقدام دیگر روی پرونده را مسدود کند، تا زمانی که بازپرس تکلیف بازداشت را روشن نماید. اگر مهلت تمام شود و بازپرس اقدامی نکند، سیستم به‌طور خودکار نامه‌ای با امضای دیجیتال سیستمی به زندان ارسال کند، مبنی بر اینکه «مهلت بازداشت قانونی این متهم به پایان رسیده و ادامه حبس او مصداق بازداشت غیرقانونی است». این مکانیزم، تحولی در تضمین آزادی‌های فردی است. در این حالت، «فراموشی بازپرس» منجر به تضییع حق متهم نمی‌شود، بلکه سیستم به نفع آزادی متهم عمل می‌کند.

راهکارهای اجرایی و آموزشی

تضمین اصول حقوق جزا در مرحله تحقیقات مقدماتی، فراتر از «اصلاح قانون» و «توسعه زیرساخت فنی» است؛ حلقه مفقوده در این میان، «عامل انسانی» و «فرآیندهای اجرایی» است. اگر بهترین قوانین حامی حریم خصوصی تصویب شود و امن‌ترین سرورها خریداری گردد، اما بازپرس پرونده تفاوت میان «*IP*» و «*MAC Address*» را نداند، یا ضابط دادگستری تصور کند که «حفظ صحنه جرم» صرفاً به معنای نوار زرد کشیدن دور اتاق است، عدالت قربانی خواهد شد. در واقع، فاصله میان «قانون روی کاغذ» و «قانون در عمل»، تنها با راهکارهای اجرایی و آموزشی پر می‌شود. در نظام حقوقی ایران، سند تحول و تعالی قوه قضاییه بر لزوم «تخصصی‌شدن دادرسی» و «توانمندسازی منابع انسانی» تأکید ویژه‌ای دارد (Center for Monitoring the Implementation of the Judicial Transformation, 2024).

توسعه دادرسی الکترونیکی به جرایم رایانه‌ای و تخصصی‌کردن شعب بازپرسی ویژه جرایم رایانه‌ای

جرایم رایانه‌ای دارای ماهیتی دوگانه (حقوقی ـ فنی) هستند. برخلاف سرقت یا ضرب‌وجرح که ارکان مادی آن‌ها برای هر حقوقدانی ملموس است، جرایمی مانند «فیشینگ»، «باج‌افزار» یا «شنود غیرمجاز»، نیازمند درک مفاهیم فنی شبکه و امنیت است. ارجاع این پرونده‌ها به شعب

عمومی، منجر به اطاله دادرسی، وابستگی محض بازپرس به ضابط و صدور آرای غیردقیق می‌شود. راهکار اجرایی، تأسیس و تقویت «دادسرای ویژه جرایم رایانه‌ای و فناوری اطلاعات» با ساختاری متفاوت است.

در حال حاضر، در بسیاری از مراکز استان‌ها، شعبه‌ای تحت عنوان «ویژه جرایم رایانه‌ای» وجود دارد. اما آیا بازپرس آن شعبه واقعاً متخصص است؟ صرف اختصاص یک شعبه، کافی نیست. اگر بازپرس آن شعبه همان بازپرس عمومی باشد که صرفاً ابلاغش تغییر کرده، تخصص محقق نمی‌شود. تخصص واقعی نیازمند این است که بازپرس، دوره‌های «جرم‌شناسی سایبری» و «ادله الکترونیک» را گذرانده باشد.

آموزش مداوم ضابطین در خصوص حقوق شهروندی در فضای سایبر

ضابطین دادگستری، به‌ویژه پلیس فتا، خط مقدم مبارزه با جرایم سایبری هستند. آن‌ها قدرت فنی بالایی دارند، اما قدرت فنی بدون «سواد حقوق بشری»، منجر به استبداد می‌شود. آموزش ضابطین در ایران عمدتاً بر «کشف جرم» (تکنیک‌های هک، ردیابی، استخراج) متمرکز است و سرفصل‌های مربوط به «حقوق متهم» و «اخلاق حرفه‌ای در فضای مجازی» در حاشیه قرار دارد.

طبق ماده ۳۰ ق.آ.د.ک، ضابطین باید آموزش‌دیده باشند و کارت ضابطیت بگیرند. اما برای جرایم سایبری، کارت عمومی کافی نیست. قوه قضاییه باید برای ضابطان فضای مجازی، «کارت ویژه» صادر کند. این کارت تنها پس از قبولی در آزمون‌های تخصصی شامل مباحث فنی و حقوق بشری صادر می‌شود و هر دو سال یک‌بار نیازمند تمدید و بازآموزی است. این مکانیزم، ضابطین را مجبور می‌کند که دائماً دانش خود را درباره قوانین جدید و استانداردهای حقوقی به‌روز نگه دارند.

نظارت برخط دادستان بر قرارهای نظارت الکترونیکی

در دادرسی الکترونیکی، به‌ویژه در موضوع حساسی مانند «نظارت الکترونیکی»، دادستان باید بتواند به‌صورت «برخط» و «لحظه‌ای» بر کیفیت صدور و اجرای این قرارها نظارت کند تا از تبدیل‌شدن «خانه» به «زندان بی‌ضابطه» جلوگیری شود. در حال حاضر، نظارت دادستان در سامانه *CMS* اغلب به مشاهده گردش کار پرونده‌ها در کارتابل محدود می‌شود. این روش برای مدیریت حجم انبوه پرونده‌ها کافی نیست.

سیستم باید به‌گونه‌ای تنظیم شود که به‌محض صدور قرار منع تعقیب یا برائت توسط قاضی، «دستور سیستمی لغو نظارت» به‌طور خودکار برای مرکز پایش ارسال شود و هم‌زمان پیامی برای دادستان برود. دادستان وظیفه دارد هر روز صبح لیست «لغوشدگان» را چک کند. اگر متهمی در لیست لغو باشد، اما سنسور پابند او هنوز فعال باشد، این یعنی «بازداشت غیرقانونی دیجیتال» و دادستان باید علیه مسئول مربوطه اعلام جرم کند.

استانداردسازی فرم‌های الکترونیکی تحقیقات مقدماتی

در دادرسی الکترونیکی، «فرم» جایگزین «قانون» می‌شود. نحوه طراحی یک صفحه در نرم‌افزار، تعیین می‌کند که بازپرس چه سؤال‌هایی بپرسد و چه حقوقی را رعایت کند. در حال حاضر، بسیاری از فرم‌های موجود در سامانه *CMS*، صرفاً نسخه *PDF*شده همان فرم‌های کاغذی قدیمی هستند و فاقد هوشمندی لازم برای هدایت صحیح دادرسی می‌باشند. استانداردسازی این فرم‌ها، یک راهکار اجرایی بنیادین برای یکسان‌سازی رویه قضایی و تضمین حقوق دفاعی است.

همچنین، در بحث استانداردهای پلیسی، لزوم «زبان مشترک داده‌ای» با مرجع قضایی مورد تأکید است (Rothbard, 2017). راهکار اجرایی، تشکیل کارگروه مشترک قوه قضاییه و ناجا برای تدوین «استاندارد ملی تبادل داده‌های کیفری» است. فرم اولیه شکایت که در کلانتری پر

می‌شود، باید عیناً و بدون نیاز به تایپ مجدد، در کارتابل بازپرس بنشیند. این کار نه‌تنها سرعت را بالا می‌برد، بلکه از «تحریف ناخواسته» اظهارات شاکی یا متهم در حین انتقال دستی از یک فرم به فرم دیگر جلوگیری می‌کند.

مطالعه تطبیقی و استانداردهای جهانی

دادرسی الکترونیکی، مرزهای جغرافیایی و حاکمیت‌های ملی را به چالش کشیده است. یک بزهکار در اروپای شرقی می‌تواند با فشردن یک دکمه، حساب‌های بانکی در تهران را خالی کند. در چنین فضایی، اگر نظام‌های حقوقی کشورها به‌صورت جزیره‌ای و ایزوله عمل کنند، عدالت فلج خواهد شد. ازاین‌رو، مطالعه تطبیقی و بررسی استانداردهای جهانی در دادرسی الکترونیکی، صرفاً یک بحث آکادمیک نیست، بلکه راهکاری برای یافتن «حلقه مفقوده» در کارآمدی نظام قضایی ایران است.

الگوبرداری از تضمین‌های تفتیش دیجیتال در حقوق فرانسه و کنوانسیون بوداپست

یکی از بزرگ‌ترین چالش‌های ما در ایران، «مجوزهای کلی تفتیش» است. برای حل این مشکل، نگاه به حقوق فرانسه که مهد «دادرسی تفتیشی»، اما با تضمینات مدرن، است و کنوانسیون بوداپست که استاندارد نوین است، راهگشاست.

کنوانسیون بوداپست، رویکردی متفاوت به ادله دارد. در حقوق سنتی، اصل بر «توقیف» بود. اما ماده ۱۶ این کنوانسیون، مفهومی به نام «حفظ فوری داده‌ها» را معرفی می‌کند. طبق این اصل، زمانی که بیم امحای داده می‌رود، به‌جای اینکه پلیس بلافاصله سرور را توقیف کند که باعث تعطیلی کسب‌وکارهای مشروع می‌شود، دستور «فریزکردن» داده‌ها را صادر می‌کند. دارنده داده موظف است داده را تا ۹۰ روز حفظ کند تا پلیس مجوز قضایی لازم برای تفتیش را بگیرد (Bucaj & Idrizaj, 2025).

این مکانیزم، تعادلی هوشمندانه میان «امنیت» و «اقتصاد» است. در ایران، توقیف فیزیکی سرورها توسط ضابطین، بارها مورد انتقاد فعالان اقتصادی قرار گرفته است. الگوبرداری از ماده ۱۶ بوداپست، می‌تواند به قانون آیین دادرسی کیفری ایران افزوده شود تا به‌جای توقیف سخت‌افزار، «داده» حفظ شود.

در فرانسه، بازپرس قدرت زیادی دارد، اما قانون‌گذار فرانسوی برای جلوگیری از سوءاستفاده از قدرت در تفتیش‌های دیجیتال، نهاد مستقلی به نام «قاضی آزادی‌ها و بازداشت» ایجاد کرده است (de Gouville, 2011). طبق قانون آیین دادرسی کیفری فرانسه، بازپرس برای اقدامات ناقض حریم خصوصی شدید، مانند شنود، نصب بدافزار دولتی یا دسترسی به داده‌های مکانی، باید از قاضی آزادی‌ها مجوز بگیرد. این قاضی در فرآیند تحقیق دخالت نمی‌کند و فقط نگهبان حقوق بشر است. در ایران، بازپرس هم «محقق» است و هم «صادرکننده مجوز سلب آزادی». این تجمیع قدرت، خطرناک است (Ashouri, 2023). الگوی فرانسوی نشان می‌دهد که تفتیش‌های دیجیتال سنگین، باید توسط مقامی تأیید شود که دغدغه‌اش «کشف جرم» نیست، بلکه «حفظ آزادی» است.

فرانسه در سال‌های اخیر قانونی تصویب کرد که به پلیس اجازه می‌دهد تحت شرایط خاصی، از راه دور به کامپیوتر متهم نفوذ کند. اما این قدرت مشروط به شروط سفت‌وسختی است:

فقط برای جرایم سازمان‌یافته و تروریسم (نه جرایم عادی).

فقط برای مدت محدود (مثلاً ۱۵ روز).

شرط تناسب: اگر روش دیگری برای تحصیل دلیل وجود داشته باشد، این روش ممنوع است.

در فرانسه، اگر پلیس از این ابزار استفاده کند، باید دقیقاً لاگ‌برداری کند که چه فایل‌هایی را دیده است. اگر ضابط از حدود مجوز فراتر رود، طبق «قاعده بطلان»، کل ادله به‌دست‌آمده باطل می‌شود. این دقیقاً همان حلقه مفقوده‌ای است که در گفتار قبلی (راهکارهای تقنینی) برای ایران پیشنهاد دادیم.

در فرانسه، اگر متهم رمز عبور گوشی خود را ندهد، طبق ماده ۲-۱۵-۴۳۴ قانون مجازات، جرم محسوب می‌شود (۳ سال حبس و جریمه سنگین). این رویکرد سخت‌گیرانه، نقطه مقابل رویکرد آمریکا (حق سکوت) است. پلیس فرانسه حق ندارد متهم را شکنجه کند یا فریب دهد. فشار صرفاً «قانونی» (مجازات حبس) است. همچنین، داده‌های استخراج‌شده تنها در محدوده پرونده قابل استفاده‌اند. این الگو برای ایران که در مواجهه با گوشی‌های قفل‌شده دچار ابهام قانونی است، می‌تواند راهگشا باشد: «جرم‌انگاری عدم همکاری»، راه‌حلی متمدنانه‌تر از «اعمال زور فیزیکی» است.

تجربه انگلستان در استفاده از هوش مصنوعی در کشف جرم

انگلستان، به‌عنوان کشوری با بیشترین تعداد دوربین‌های مداربسته و پیشرو در استفاده از هوش مصنوعی در پلیس، آزمایشگاهی زنده برای بررسی تعامل تکنولوژی و حقوق بشر است. تجربه این کشور، به‌ویژه در پرونده‌های اخیر، درس‌های مهمی درباره خطرات «پلیس پیشگیرانه» دارد. پلیس دورهام انگلستان از سیستمی استفاده می‌کند که با هوش مصنوعی، احتمال تکرار جرم توسط متهم را پیش‌بینی می‌کند. این سیستم به بازداشت یا آزادی متهم کمک می‌کند. الگوریتم این سیستم بر اساس داده‌های تاریخی (۵ سال گذشته) آموزش دیده است. چون در گذشته پلیس بیشتر سیاه‌پوستان و فقرا را دستگیر می‌کرد، الگوریتم یاد گرفت که «فقیربودن» یا «کد پستی محل سکونت» مساوی با «خطرناک‌بودن» است (Krishnakumar, 2025).

در سند تحول قضایی ایران، استفاده از فناوری‌های نوین برای تصمیم‌گیری قضایی پیش‌بینی شده است (Keykha & Ehsanifar, 2023). تجربه انگلستان هشدار می‌دهد که اگر داده‌های ورودی به سیستم‌های هوشمند ایرانی، داده‌های سامانه *CMS*، پالایش نشوند، هوش مصنوعی قضایی ما نیز دچار سوگیری شده و علیه اقشار آسیب‌پذیر تبعیض قائل خواهد شد. ما نباید اشتباه انگلستان را تکرار کنیم؛ الگوریتم باید «شفاف» و قابل حسابرسی باشد.

پلیس ولز جنوبی از تکنولوژی تشخیص چهره زنده در معابر عمومی استفاده می‌کرد تا مجرمان تحت تعقیب را در جمعیت شناسایی کند. آقای ادوارد بریجز، فعال حقوق مدنی، شکایت کرد که چهره او اسکن شده است. در سال ۲۰۲۰، دادگاه استیناف انگلستان (*Court of Appeal*) حکمی تاریخی صادر کرد: استفاده پلیس از این تکنولوژی «غیرقانونی» است، زیرا:

قانون مشخصی برای آن وجود ندارد (خلأ قانونی).

معیار اینکه چه کسی در «لیست تماشا» (*Watchlist*) قرار می‌گیرد، شفاف نیست.

پلیس ارزیابی نکرده که آیا این نرم‌افزار نژادپرست است یا خیر؟

این رأی یک نقطه عطف جهانی است. آن برای ایران روشن است: پلیس فتا یا ناجا نمی‌توانند صرفاً به استناد «وظیفه کلی حفظ امنیت»، از ابزارهای نظارت توده‌ای استفاده کنند. استفاده از دوربین‌های چهره‌خوان در متروها یا خیابان‌ها، نیازمند «قانون خاص» مصوب مجلس است؛ صرفاً بخشنامه‌های انتظامی کفایت نمی‌کند.

در انگلستان، با وجود استفاده گسترده از AI، یک اصل طلایی وجود دارد: «تصمیم نهایی با انسان است». هوش مصنوعی فقط «پیشنهاد» می‌دهد. در سیستم قضایی انگلستان، قاضی حق ندارد بگوید «چون کامپیوتر گفت خطرناک است، بازداشت کردم». قاضی باید استدلال مستقل داشته باشد (Krishnakumar, 2025).

در ایران، خطر این است که با هوشمندسازی فرآیندها، مانند ارجاع هوشمند، قضات دچار «تنبلی شناختی» شوند و دربست تسلیم الگوریتم گردند. تجربه انگلستان نشان می‌دهد که باید پروتکل‌هایی تدوین شود که قاضی را ملزم کند دلایل مخالفت یا موافقت خود با پیشنهاد سیستم را مکتوب نماید.

طبق مقررات حفاظت از داده‌های انگلستان، اگر یک سیستم خودکار تصمیمی علیه شهروند بگیرد، مثلاً جریمه کند یا وام ندهد، شهروند حق دارد بپرسد: «چرا؟». سیستم‌های AI اغلب «جعبه سیاه» هستند و نمی‌توانند توضیح دهند. انگلستان در حال حرکت به سمت «هوش مصنوعی قابل تفسیر» در پلیس است (Krishnakumar, 2025).

این موضوع در حقوق ایران مغفول مانده است. اگر سامانه هوشمند پلیس راهور، خودرویی را جریمه می‌کند، یا سامانه مالیاتی، مؤدی را «پرریسک» می‌شناسد، باید منطق آن برای شهروند قابل توضیح باشد. «شفافیت الگوریتمی»، حق جدیدی در دادرسی مدرن است که باید در ایران به رسمیت شناخته شود.

بسیار عالی. در ادامه، دو بند پایانی از گفتار چهارم (مطالعه تطبیقی و استانداردهای جهانی) را تقدیم می‌کنم.

این بخش‌ها، با بررسی اسناد پیشرو اتحادیه اروپا و استانداردهای فنی اینترپل، نقشه راهی دقیق برای ارتقای «استانداردهای دفاعی» و «اعتبار علمی ادله» در نظام حقوقی ایران ارائه می‌دهند.

حق دسترسی به وکیل در تحقیقات سایبری در اسناد اتحادیه اروپا

اتحادیه اروپا (EU) دارای یکی از پیشروترین نظام‌های حقوقی در زمینه تضمین حقوق دفاعی است. برخلاف رویکردهای سنتی که حضور وکیل را محدود به جلسه دادگاه می‌دانستند، اسناد جدید اروپایی بر «دفاع مؤثر» از لحظه شروع تحقیقات، به‌ویژه در جرایم پیچیده سایبری، تأکید دارند. بررسی این اسناد و مقایسه آن با چالش‌های موجود در ایران، مانند تبصره ماده ۴۸، راهکارهای روشنی را پیش رو می‌نهد.

دستورالعمل EU/۴۸/۲۰۱۳: حق دسترسی به وکیل در تمام مراحل را به رسمیت می‌شناسد. این دستورالعمل، سنگ‌بنای حق دفاع در اروپاست. طبق ماده ۳ این سند، متهم حق دارد «بدون تأخیر» و «قبل از هرگونه بازجویی»، حتی بازجویی اولیه توسط پلیس، به وکیل دسترسی داشته باشد.

نکته مهم برای بحث ما، بندهای مربوط به «بازجویی‌های از راه دور» است. اتحادیه اروپا تأکید دارد که اگر تحقیق به‌صورت ویدئوکنفرانس انجام می‌شود، حق دسترسی به وکیل نباید تضعیف شود. وکیل باید بتواند در کنار متهم، در بازداشتگاه، حضور داشته باشد یا اگر او هم آنلاین است، باید «خط ارتباطی محرمانه» برای مشاوره داشته باشد (Novokmet, 2019).

در ایران، حضور وکیل در تحقیقات مقدماتی (ماده ۴۸ آ.د.ک) پذیرفته شده، اما ضمانت اجرای نقض آن ضعیف است. در استاندارد اروپا، اگر پلیس بدون حضور وکیل از متهم بازجویی سایبری کند، آن بازجویی کلاً باطل است. این سطح از ضمانت اجرا، برای ایران که در آن گاهی وکیل را پشت درِ اتاق بازجویی نگه می‌دارند، بسیار آموزنده است.

رأی مشهور دیوان حقوق بشر اروپا (*ECtHR*) در پرونده «سالدوز» (*Salduz v. Turkey*)، اصلی را تثبیت کرد: «متهم در آسیب‌پذیرترین لحظه (بازداشت اولیه)، بیشترین نیاز را به وکیل دارد». در جرایم سایبری، این آسیب‌پذیری بیشتر است. متهم با کوهی از ادله فنی، لاگ‌ها و *IP*ها، روبه‌روست که آن‌ها را نمی‌فهمد. طبق استانداردهای اروپایی، وکیل در جرایم سایبری نباید فقط «حقوقدان» باشد، بلکه باید به «کمک‌های فنی» نیز دسترسی داشته باشد. یعنی حق دفاع شامل «حق داشتن مشاور فنی» در کنار وکیل است تا بتواند ادله دیجیتال پلیس را به چالش بکشد (Novokmet, 2019).

این نکته، خلأ بزرگ حقوق ایران است. در دادسراهای ما، وکیل تنهاست و معمولاً دانش فنی ندارد. الگوبرداری از اروپا ایجاب می‌کند که «دستیاران فنی دفاع» به رسمیت شناخته شوند.

دستورالعمل *EU*/۱۳/۲۰۱۲: با موضوع حق بر اطلاعات، به «دسترسی به پرونده» تمرکز دارد. در دادرسی دیجیتال، این حق یعنی دسترسی به «اصل داده‌ها» تلقی می‌شود و فقط گزارش پلیس کفایت نمی‌کند. در اروپا، پلیس موظف است «ایمیج هارد دیسک» متهم را، با رعایت حریم خصوصی ثالث، به وکیل بدهد تا وکیل بتواند آن را به آزمایشگاه خصوصی ببرد و تحلیل کند (Novokmet, 2019).

در ایران، وکیل معمولاً به «داده‌های خام» دسترسی ندارد و مجبور است گزارش کارشناس دادگستری را وحی منزل بداند. استاندارد اروپا نشان می‌دهد که «تساوی سلاح‌ها» در فضای سایبر، یعنی تساوی در دسترسی به بیت‌ها و بایت‌ها است.

حق «سکوت دیجیتال» در رویه دیوان اروپا، موضوع مهم دیگری است که قابل توجه است. آیا پلیس می‌تواند متهم را مجبور کند قفل بیومتریک گوشی‌اش را باز کند؟ دیوان دادگستری اروپا (*CJEU*) رویکردی بینابینی دارد، اما اصل بر «منع خودمجرم‌انگاری» است (Novokmet, 2019).

اگر بازکردن قفل، منجر به دسترسی به اسنادی شود که وجودشان مستقل از اراده متهم است، مثل فایل‌های موجود، شاید مجاز باشد؛ اما اگر منجر به تولید دلیل جدید شود، ممنوع است. این ظرافت‌های حقوقی در اسناد اروپایی، راهنمای خوبی برای پرکردن خلأهای ماده ۱۹۷ آ.د.ک ایران است.

استانداردهای اینترپل در خصوص ادله الکترونیکی

پلیس بین‌الملل، به‌عنوان بزرگ‌ترین سازمان پلیسی جهان، استانداردهای فنی دقیقی را برای «جرم‌یابی دیجیتال» تدوین کرده است. این استانداردها، نه قانون، بلکه «پروتکل‌های علمی» هستند که رعایت آن‌ها شرط پذیرش ادله در همکاری‌های بین‌المللی است (Ferrazzano & Brighi, 2021).

اینترپل تأکید دارد که آزمایشگاه‌های پلیس فتا باید دارای استاندارد *ISO 17025* باشند. این استاندارد یعنی:

تجهیزات کالیبره باشند.

کارکنان صلاحیت علمی داشته باشند.

محیط آزمایشگاه ایزوله باشد (کنترل دما، رطوبت و الکتریسیته ساکن).

بسیاری از آزمایشگاه‌های ادله دیجیتال در کشورهای درحال‌توسعه، از جمله برخی واحدهای استانی در ایران، فاقد این گواهینامه هستند. در نتیجه، اگر پرونده‌ای جنبه بین‌المللی پیدا کند، وکیل مدافع خارجی می‌تواند با استناد به عدم رعایت *ISO 17025*، کل گزارش فنی پلیس ایران را زیر سؤال ببرد و بی‌اعتبار کند.

چهار اصل طلایی اینترپل در برخورد با ادله دیجیتال به شرح زیر می‌باشند.

اینترپل در راهنمای جهانی خود، چهار مرحله حیاتی را تعریف کرده است:

شناسایی: تشخیص اینکه چه چیزی دلیل است.

جمع‌آوری: ایمیج‌گیری بدون تغییر داده.

تحلیل: استخراج اطلاعات پنهان یا حذف‌شده با نرم‌افزارهای معتبر.

ارائه: تبدیل داده‌های فنی به زبانی که قاضی بفهمد (Ferrazzano & Brighi, 2021).

در ایران، مرحله «گزارش‌دهی» (ارائه) ضعف دارد. گزارش‌ها بیش از حد فنی و نامفهوم هستند. استاندارد اینترپل می‌گوید گزارش باید به‌گونه‌ای باشد که یک «فرد غیرمتخصص» بتواند فرآیند رسیدن از «الف» به «ب» را درک کند.

ادله دیجیتال باید «علمی» باشند. در محاکم ایران، گاهی کارشناس می‌گوید «من با روش‌های خاص خودم فهمیدم». این جمله در استاندارد اینترپل مردود است. روش باید مستند، استاندارد و قابل تست توسط دیگران باشد. اگر کارشناس نتواند روشش را توضیح دهد، آن دلیل «جادوگری» و نه «علم» تلقی می‌شود.

اینترپل دستورالعمل‌های ویژه‌ای برای «جرم‌یابی ابری» دارد. چالش اصلی این است که داده در کلاد، دائماً در حال تغییر است. استاندارد اینترپل می‌گوید برای استناد به داده‌های ابری، باید از روش «اسنپ‌شات معتبر» استفاده کرد. یعنی گرفتن عکس لحظه‌ای از وضعیت سرور با مهر زمانی معتبر از یک مرجع ثالث باید باشد.

در ایران، اسکرین‌شات‌های گرفته‌شده توسط شاکی یا پلیس، اغلب فاقد این استاندارد فنی هستند. رعایت پروتکل اینترپل ایجاب می‌کند که اسنپ‌شات توسط «نرم‌افزار فارنزیک» گرفته شود که هش صفحه را هم ذخیره می‌کند.

نتیجه‌گیری

دادرسی کیفری الکترونیکی در مرحله کشف جرم و تحقیقات مقدماتی، شمشیری دولبه است که از یک سو به تسریع و تدقیق فرآیند رسیدگی کمک شایانی می‌کند و از سوی دیگر، اصول بنیادین و کلاسیک حقوق جزا را در معرض تهدیدات پیچیده‌ای قرار می‌دهد. بررسی‌ها در این پژوهش نشان داد که با جایگزینی ادله دیجیتال به‌جای سرنخ‌های فیزیکی، حریم خصوصی متهمان به‌شدت آسیب‌پذیر شده است؛ به‌گونه‌ای که تفتیش تجهیزات هوشمند و گوشی‌های همراه، دیگر نه یک بازرسی فیزیکی ساده، بلکه ورود به خصوصی‌ترین ابعاد روان و زندگی افراد است. یافته‌های تحلیلی این مقاله مؤید آن است که چالش‌های موجود صرفاً ماهیت فنی ندارند، بلکه ریشه در عدم تطابق تضمینات سنتی با اقتضائات فضای سایبر دارند. مشکلاتی نظیر مخدوش‌شدن حق دفاع در بازجویی‌های آنلاین، نقض مصونیت مکالمات در بستر ارتباطات الکترونیکی، و چالش در احراز «تمامیت ادله»، نیازمند پاسخ‌های حقوقی روزآمد است. در این راستا، بهره‌گیری از تجربیات و استانداردهای بین‌المللی، به‌ویژه اسناد اتحادیه اروپا و دستورالعمل‌های پلیس بین‌الملل (اینترپل)، الگوی مناسبی برای برون‌رفت از این چالش‌ها ارائه می‌دهد. برای تضمین دادرسی منصفانه در عصر دیجیتال، نظام حقوقی باید حقوق نوینی، نظیر «حق سکوت دیجیتال» و منع خودمجرم‌انگاری در ارائه گذرواژه‌ها یا داده‌های بیومتریک، را به رسمیت بشناسد. افزون بر این، حضور مؤثر وکیل در تحقیقات سایبری باید با حق بهره‌مندی از «مشاوران و دستیاران فنی» تکمیل گردد تا اصل برابری سلاح‌ها میان متهم و ضابطین دادگستری محقق شود. همچنین، نهادینه‌سازی استانداردهای علمی در آزمایشگاه‌های پلیس فتا و الزام به استفاده از روش‌های مستند و قابل بازبینی، به‌جای گزارش‌های فنی و نامفهوم، امری

اجتناب‌ناپذیر است. در نهایت، دستیابی به عدالت کیفری در بستر الکترونیک، در گرو بازتعریف اصول حقوق جزا متناسب با عصر اطلاعات است؛ به‌نحوی‌که تسریع در فرآیندها و اقتدار نهادهای کشف جرم، به بهای تضییع حقوق و آزادی‌های مشروع شهروندان تمام نشود و دادرسی الکترونیکی به ابزاری برای نظارت فراگیر تقلیل نیابد.

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

The rapid integration of information technology into criminal justice has fundamentally transformed the nature of crime detection and preliminary investigations. Conventional investigative practices, which were primarily based on physical searches, eyewitness testimony, tangible traces, and direct interaction between judicial authorities and suspects, have increasingly been replaced by digital searches, electronic surveillance, data analysis, remote interrogation, and algorithm-assisted decision-making. This transition has significantly enhanced the capacity of criminal justice institutions to identify offenders, preserve evidence, and accelerate judicial procedures; however, it has also created unprecedented risks for the foundational principles of criminal law and fair trial. The preliminary investigation stage remains the most sensitive phase of criminal proceedings because the state exercises its broadest coercive powers at a time when the accused has not yet been convicted and must still benefit from the presumption of innocence (Khaleghi, 2024). In electronic criminal proceedings, this imbalance becomes more pronounced because law-enforcement authorities may gain access to extensive quantities of personal information contained in mobile phones, computers, cloud storage systems, communication platforms, and digital networks. Electronic adjudication has therefore changed the concept of a search from entry into a physical location into access to the intellectual, social, professional, and private dimensions of an individual's life (Hayat Poursefli, 2021). The expansion of digital surveillance, artificial intelligence, automated data processing, and remote judicial procedures has similarly raised concerns about privacy, equality of arms, access to counsel, informed participation, and the integrity of electronic evidence (Halahan et al., 2023). Accordingly, the present study examines the major challenges confronting the protection of criminal-law principles during crime detection and preliminary investigations in electronic criminal proceedings and proposes legislative, technical, institutional, and comparative strategies for ensuring that technological efficiency does not undermine the defense rights and lawful freedoms of accused persons.

This research was conducted through a descriptive-analytical method based on the examination of Iranian criminal procedural rules, scholarly legal literature, electronic adjudication practices, digital-forensic standards, and selected comparative experiences. The analysis focuses on four interconnected dimensions: violations of privacy and the presumption of innocence in the acquisition of evidence, restrictions on the accused's defense rights during electronic preliminary investigations, technical and operational weaknesses in the detection and preservation of digital evidence, and jurisdictional difficulties arising from the borderless character of cyberspace. Iranian

criminal procedure recognizes the necessity of judicial authorization for many intrusive investigative measures, yet broad and technically imprecise search orders may allow investigators to access large quantities of information unrelated to the suspected crime (Akbari, 2022). The distinction between relevant evidence and protected personal data is particularly difficult when an entire mobile device, computer, or cloud account is searched. Such searches may expose family conversations, medical information, professional documents, private images, and communications belonging to third parties who are not suspected of criminal conduct. This situation increases the risk that digital searches will become general exploratory searches rather than targeted investigative actions. The extension of the plain-view doctrine to digital environments is especially problematic because an investigator searching for one file may inevitably encounter thousands of unrelated files and private records (Ehmann, 1990). Moreover, the compulsory retention of traffic and communication data may facilitate generalized monitoring and gradually transform exceptional surveillance powers into routine mechanisms of social control (Zadeh-Hossein Aliaei, 2017). The analytical framework therefore evaluates whether existing safeguards are sufficiently specific, proportionate, and enforceable to prevent electronic investigations from becoming unlimited forms of surveillance.

The findings indicate that one of the most serious challenges concerns the weakening of the accused's defense rights in electronic prosecutorial proceedings. Electronic notification systems may formally register service without ensuring that the accused has actually received or understood the notification. Technical failures, limited internet access, digital illiteracy, changes in telephone numbers, and dependence on text-message alerts may cause defendants to miss summonses, hearings, and statutory deadlines despite the legal presumption that notification has occurred (Rahimi et al., 2021). This creates a structural disadvantage for elderly persons, economically disadvantaged groups, rural residents, and individuals without reliable digital access, thereby turning technological modernization into a potential barrier to justice (Bastami, 2019). Similar problems arise in online interrogations and videoconference-based investigations. Although remote proceedings may reduce costs and accelerate case processing, they may also weaken confidential attorney-client communication, limit the lawyer's ability to observe the entire interrogation environment, and reduce counsel to a passive image on a screen rather than an effective defender (Neira-Pena, 2023). The absence of secure private communication channels prevents lawyers from advising clients without judicial or prosecutorial monitoring and may expose defense strategies to investigative authorities. Remote communication can also reduce the quality of the explanation of charges, because legally meaningful notification requires more than merely reading an accusation; it requires ensuring that the accused understands the factual and legal basis of the charge (Haddadzadeh Nairi et al., 2023). Furthermore, the electronic extraction of a final defense may violate equality of arms when the prosecution has access to complete digital case files while the accused or counsel can see only limited documents. The study therefore finds that the formal availability of electronic participation does not necessarily amount to effective participation unless access, confidentiality, comprehension, and evidentiary equality are institutionally guaranteed.

The research further demonstrates that the reliability of electronic criminal proceedings depends heavily on the scientific collection, preservation, analysis, and presentation of digital evidence. Unlike traditional evidence, digital data are invisible, volatile, easily altered, and often distributed across multiple devices, networks, and jurisdictions. An untrained investigator may unintentionally destroy volatile memory, modify metadata, contaminate a device, or introduce foreign files merely by turning a computer on or off or connecting an unverified storage device. The principle that every contact leaves a trace becomes especially significant in digital environments because nearly every

interaction with a device changes some element of its data structure (Mistek, 2018). The chain of custody must therefore record every stage from seizure to courtroom presentation, including forensic imaging, hash generation, transfer, storage, analysis, and access by authorized personnel. Failure to calculate and document hash values, use write-blocking devices, isolate seized equipment from networks, or employ validated forensic tools may undermine the authenticity and admissibility of evidence (Teslenko, 2024). The findings also identify substantial infrastructure disparities between major urban forensic units and local jurisdictions, where investigators may lack specialized training, accredited laboratories, secure storage facilities, or standard operating procedures. These deficiencies may prolong detention while devices await examination and may increase the risk of evidence loss or manipulation. The study additionally finds that electronic monitoring before trial may expand rather than reduce coercive control. GPS-enabled devices can continuously record an accused person's movements and transform the home into an electronically supervised detention space, while the financial cost of such monitoring may produce unequal treatment between wealthy and indigent defendants (Taghiniam & Ghanbari, 2024). The absence of clear rules on the retention, deletion, and secondary use of monitoring data also creates serious privacy concerns after acquittal or termination of proceedings.

The proposed strategies are organized into legislative, technical, executive, educational, and comparative measures. At the legislative level, search warrants for digital evidence should specify the categories of data sought, the relevant time period, the accounts or devices covered, and the relationship between the requested data and the suspected offense. Access to cloud-based information should require separate judicial authorization and should not automatically follow from permission to search a physical device. Evidence obtained through unauthorized hacking, coercive password disclosure, forced biometric unlocking, unlawful surveillance, or substantial violations of chain-of-custody requirements should be expressly excluded. Notification rules should be amended to require actual confirmation of receipt in serious criminal cases and should preserve non-digital alternatives for vulnerable individuals. At the technical level, law-enforcement agencies should be equipped with mobile digital-forensic laboratories, validated forensic software, write blockers, secure evidence-storage systems, and automated hash-generation mechanisms (Soni, 2024). Blockchain-based registration may also strengthen the immutability and traceability of digital evidence by recording hash values, timestamps, and investigator identities in tamper-resistant systems (Halahan et al., 2023). Judicial videoconferencing platforms should provide encrypted private consultation rooms, suspend audio recording during attorney-client communication, and permit confidential document sharing (Ray, 2025). Case-management systems should also include automated alerts for detention deadlines, notification failures, missing legal warnings, and incomplete defense access. At the institutional level, specialized cybercrime prosecution branches should be staffed by judges and investigators with both legal and technical competence. Continuous training should address not only investigative techniques but also privacy, proportionality, the presumption of innocence, and defense rights. Comparative experience further supports the creation of independent judicial control over highly intrusive digital searches, similar to the French judge of liberties and detention (de Gouville, 2011), stronger guarantees of access to counsel under European standards (Novokmet, 2019), algorithmic transparency in predictive policing (Krishnakumar, 2025), and rapid preservation of data rather than unnecessary seizure of entire systems under the Budapest Convention framework (Bucaj & Idrizaj, 2025).

In conclusion, electronic criminal proceedings can contribute substantially to the speed, accuracy, accessibility, and administrative efficiency of criminal justice, but these benefits cannot justify the

erosion of the fundamental protections that distinguish lawful investigation from unrestricted state surveillance. The transition from physical evidence to digital data has expanded the investigative power of the state into the most private areas of human life and has created new forms of vulnerability that traditional procedural guarantees were not designed to address. Fairness in electronic preliminary investigations therefore requires more than the digitization of existing procedures; it requires the reconstruction of criminal procedural safeguards in accordance with the technical characteristics of cyberspace. The right to privacy must be protected through narrowly defined digital search powers, the presumption of innocence must prevent prolonged equipment seizure and excessive electronic supervision, and the right to defense must include confidential access to legal counsel, effective participation in remote proceedings, and access to independent technical expertise. Digital evidence must be collected and assessed through transparent, reproducible, and scientifically validated procedures, while automated systems must remain subject to human review and judicial accountability. Ultimately, the legitimacy of electronic criminal justice depends on maintaining a principled balance between the effectiveness of technology in detecting crime and the protection of human dignity, individual freedom, procedural equality, and the defense rights of the accused. Without this balance, electronic adjudication risks becoming an instrument of pervasive monitoring rather than a modern framework for the realization of justice.

References

Akbari, B. (2022). *Criminal Procedure* (Vol. 2 volumes). Javidaneh Publications.

Akhoundi, M. (2015). *Introduction to Criminal Procedure*. Durandishan Publications.

Ashouri, M. (2023). *Criminal Procedure* (8th ed.). Organization for Researching and Composing University Textbooks in the Humanities.

Bastami, N. (2019). *Examining the Role of Electronic and Virtual Equipment in Achieving Fair Criminal Proceedings* [Master's thesis, Islamic Azad University, Khorramabad Branch].

Beiki Shouraki, M., & Fallah, M. (2023). Electronic Adjudication Processes. *Scientific Quarterly of Law and New Studies*, *4*(3), 193-215.

Beiki Shouraki, M., & Fallah, M. (2024). Examining Necessary Changes in the Structure, Organization, and Judicial Establishment for Implementing Electronic Adjudication. *Quarterly Journal of Cyber Law Studies*, *10*(8), 30-40.

Bucaj, E., & Idrizaj, K. (2025). The Need for Cybercrime Regulation on a Global Scale by the International Law and Cyber Convention. *Multidisciplinary Reviews*, *8*(1), 2025024.

Center for Monitoring the Implementation of the Judicial Transformation, D. (2024). *Document for the Transformation and Excellence of the Judiciary: The Second Step of Judicial Transformation*.

de Gouville, P. L. M. (2011). The Judge of Freedoms and Detention between Present and Future. *Les cahiers de la justice*, *4*(4), 145-157.

Ehmann, J. (1990). Criminal Procedure: Expanding the Plain View Doctrine. *Temple Law Review*, *63*, 919.

Ferrazzano, M., & Brighi, R. (2021). Digital Forensics: Best Practices and Perspective. In *Collezione Di Giustizia Penale* (pp. 13-48).

Ghane, R., & Zarei, T. (2022). Improving the Performance of Fair Trial by Identifying and Removing Existing Barriers to the Development of Electronic Adjudication. *Legal Civilization Quarterly*, *5*(12), 289-317.

Greene, E., & Bornstein, B. H. (2013). Nudging the Justice System toward Better Decisions. *University of Chicago Law Review*, *80*, 1155-1170.

Haddadzadeh Nairi, M., Borghi, M., Ehsanpour, S., & Akrami, R. (2023). Using Information Technology in Criminal Proceedings. *Scientific Quarterly of Smart Business Management Studies*, *11*(43), 159-192.

Halahan, O., Krytska, I., Tumanyants, A., & Dubivka, I. (2023). Digitalization of the Criminal Process: Is Simplification Always for the Better? *Revista de Internet, Derecho y Politica*(38).

Hayat Poursefli, M. (2021). *Electronic Adjudication in Iranian Criminal Law*. Sanjesh va Danesh Publications.

Hosseini, S. M. (2023). The Historical Course of Electronic Notification and Electronic Adjudication in Iran. Fourth National Conference on Innovation and Research in Persian Culture, Language, and Literature,

Javidzadeh, H., & Mirehei, H. (2006). Punishment under the EM System: Is Electronic Monitoring of Offenders Compatible with the Foundations of Islamic Jurisprudence? *Quds Newspaper*.

Keykha, M., & Ehsanifar, A. (2023). Electronic Adjudication in the Iranian Judicial System and the Use of Artificial Intelligence in Electronic Adjudication. Second International Conference on Jurisprudence, Law, and Religious Research,

Khaleghi, A. (2024). *Criminal Procedure* (11th ed.). Shahr-e Danesh Legal Research Institute.

Khalouei Tafti, S. S., & Aghaabbasi, R. (2021). The Importance and Role of Electronic Adjudication in Judicial Proceedings. *Journal of Research and Studies in Islamic Sciences*, *3*(28), 105-118.

Khan, M. N. I., & Ahmed, I. (2025). A Systematic Review of Judicial Reforms and Legal Access Strategies in the Age of Cybercrime and Digital Evidence. *International Journal of Scientific Interdisciplinary Research*, *5*(2), 1-29.

Koulaei, M. (2025). *Electronic Adjudication, Computer Crimes, and Legal Persons in Law and Judicial Practice*. Durandishan Publications.

Koushki, G. (2024). *Criminal Procedure*. Ganj-e Danesh Publications.

Krishnakumar, S. (2025). Discrimination Bias in AI: Examining UK Legislation and Policy to Counter Discrimination within Predictive Policing AI. *Leeds Student Law & Criminal Justice Review*, *5*, 41.

Loveymi, N., & Janadeleh, M. (2023). *Electronic Proceedings in Judiciary Adjudication: With Emphasis on the Independence and Relations of Powers*. Mahvareh Publishing.

Mistek, E. (2018). Toward Locard's Exchange Principle: Recent Developments in Forensic Trace Evidence Analysis. *Analytical Chemistry*, *91*(1), 637-654.

Naude, B. C. (2009). A Suspect's Right to Be Informed. *SA Public Law*, *24*(2), 506-527.

Neira-Pena, A. (2023). Digitalization of the Criminal Procedure in Spain: Use of Videoconference and Its Impact on the Rights of the Defense and the Accused. *Access to Justice in Eastern Europe*, *6*(3), 1-17.

Novokmet, A. (2019). The Europeanization of the Criminal Proceedings in the Republic of Croatia through the Implementation of the Directive 2013/48/EU. *European Journal of Crime, Criminal Law and Criminal Justice*, *27*(2), 97-125.

Rahimi, M., Mokhberian-Nejad, M., & Rahimi-Dehsouri, R. (2021). *Electronic Adjudication: Procedure for Computer Crimes and Procedure for Crimes of Legal Persons: Doctrine and Judicial Practice*. Chatr-e Danesh Publications.

Rahmdel, M. (2015). *Criminal Procedure* (2nd ed.). Dadgostar Publications.

Rahnama, Z., & Zafari Kouretash, A. (2025). *The Role of Artificial Intelligence in Transforming the Criminal Justice System: From Criminal Investigations to the Execution of Imprisonment*. Raj Publications.

Ramos, V. C. (2021). European Criminal Bar Association Statement of Principles on the Use of Video-Conferencing in Criminal Cases in a Post-COVID-19 World. *New Journal of European Criminal Law*, *12*(3), 476-493.

Ray, K. P. (2025). *The Criminal CourtZoom: Access to Justice in Remote Criminal Hearings at the US Federal District Courts* [Doctoral dissertation, University of Georgia].

Rothbard, M. (2017). Police, Law, and the Courts. In *Anarchy and the Law* (pp. 19-39). Routledge.

Sayadi, M. (2022). *Law on Criminal Procedure for the Armed Forces and Electronic Adjudication*. Komak Azmoon Edalat Gostar Jam Publications.

Soni, M. (2024). *Security and Cyber Laws: Digital Defenders*. Poorav Publications.

Taghiniam, S., & Ghanbari, V. (2024). *Laws and Regulations on Electronic Monitoring of Convicts and the Semi-Liberty System, together with Regulations, Advisory Opinions, and Sample Judgments*. State Prisons and Security and Corrective Measures Organization; Rah-e Tarbiyat Publications.

Teslenko, I. O. (2024). Specific Features of Obtaining and Using Electronic Evidence in Criminal Proceedings. *Law & Safety*, *186*.

Waldman, A. E. (2018). Privacy's Law of Design. *UC Irvine Law Review*, *9*, 1239.

Zadeh-Hossein Aliaei, Z. (2017). *A Study of Electronic Adjudication in the Iranian Criminal Justice System*. Majd Publications.

Zare, E. (2020). *Electronic Adjudication*. Aftab-e Giti Publications.