New Research in Islamic Humanities Studies
Online ISSN : 2980 - 8944
https://api.lu.ac.ir/
Lorestan University

Procedural Challenges and the Development of Cybercrime Control Mechanisms in Iraq and Egypt: A Comparative Study of Evidence, Jurisdiction, and Digital Investigation

Ahmad Mohammad Naser Al-Salman[1], Mohammad Reza Zafari[2] ✉

1. Ph.D. Student in Criminal Law and Criminology, University of Qom, Qom, Iran.
   Email: ahmedmohamed4254641@gmail.com
2. Corresponding author, Assistant Professor of Criminal Law and Criminology, Payam Noor University, Tehran, Iran.
   Email: mr_zafari@pnu.ac.ir

Article Info

Article type:
Research Article

Article history:
Received 03 January 2026
Received in revised form 06 May 2026
Accepted 07 June 2026
Available online 22 June 2026

Keywords:
Digital Evidence,
Criminal Proof,
Jurisdiction,
Digital Investigation,
Cybercrime,
Iraq and Egypt

ABSTRACT

Objective: The study aims to explain the characteristics of digital evidence and the conditions of its integrity and admissibility, analyze the impact of encryption and anonymization on evidence collection, compare the approaches to proof and jurisdiction in the legal systems of Iraq and Egypt, and then examine the role of specialized units and modern technologies in enhancing investigative efficiency.

Method: The research method is descriptive-analytical and comparative, and relies on the legal and doctrinal materials contained in the original dissertation.

Results: The findings show that the success of digital criminal prosecution depends on preserving the integrity of the chain of contact with evidence from the moment of seizure to its presentation in court, and on the existence of clear rules of jurisdiction and cooperation in cases where the incident transcends territorial boundaries. It also became clear that establishing specialized units and training investigators, judges, and experts is a practical and necessary condition, because legal texts alone are not sufficient to counter encryption technologies, identity concealment, and the evolution of methods of committing crime.

Conclusion: The study concludes that an integrated model must be designed that links legislation with proof, jurisdiction, cooperation, and digital forensic techniques, and that is accompanied by judicial oversight to ensure proportionality and to protect privacy and the rights of defense. In addition, the study emphasizes that the development of technical tools will be effective only when accompanied by the harmonization of professional standards governing the extraction, examination, and documentation of data in such a way that the possibility of reviewing the technical result is provided and the judiciary's confidence in the integrity of the evidence is strengthened.

Cite this article: Mohammad Naser Al-Salman, A. & Zafari, M. R. (2026). Procedural Challenges and the Development of Cybercrime Control Mechanisms in Iraq and Egypt: A Comparative Study of Evidence, Jurisdiction, and Digital Investigation. *New Research in Islamic Humanities Studies*, 5 (10), 1-24. https://doi.org/10.22034/api.2026.2118597.2071

© Author(s) retain the copyright and full publishing rights.
Publisher: Lorestan University.
DOI: https://doi.org/10.22034/api.2026.2118597.2071

Introduction

The formal dimension of combating cybercrimes rests on the fact that a digital crime cannot be proven in the same manner as traditional crimes are proven, because the information that forms the subject of the argument can, within a short period of time, be copied, altered, deleted, and transferred, and its traces may be scattered among devices, servers, and accounts located in multiple places. Therefore, the problem is not limited to finding evidence; it extends to proving the integrity of its origin, the continuity of its possession and preservation, the absence of tampering with its content, and the clarification of the technical and legal link between the evidence, on the one hand, and the criminal incident and the accused, on the other. This requires precise formal rules, specialized personnel, and technical tools capable of preserving the evidence from the moment of seizure until its presentation in court.

Method

The research method is descriptive-analytical and comparative, and relies on the legal and doctrinal materials contained in the original dissertation.

Results

The findings show that the success of digital criminal prosecution depends on preserving the integrity of the chain of contact with evidence from the moment of seizure to its presentation in court, and on the existence of clear rules of jurisdiction and cooperation in cases where the incident transcends territorial boundaries. It also became clear that establishing specialized units and training investigators, judges, and experts is a practical and necessary condition, because legal texts alone are not sufficient to counter encryption technologies, identity concealment, and the evolution of methods of committing crime.

Conclusion

The study shows that the formal challenge in cybercrimes is more complex than merely adding a new means of proof to existing rules; because the nature of digital evidence, its location, and the manner of its production and preservation require a complete chain-based reorganization of investigative measures. Moreover, rapid cross-border movement causes jurisdiction to be linked to international cooperation to the same extent that it depends on the text of domestic law. The comparison makes clear that the existence of more specialized rules in Egypt provides a clearer basis for addressing certain aspects of evidence and jurisdiction, while Iraq needs to strengthen its specialized formal framework and harmonize technical procedures. The findings emphasize that technology does not replace law, but rather increases the need for rules that document seizure and analysis measures and guarantee the possibility of contesting evidence in court. Therefore, the most efficient method of response is one that combines a specialized unit, a qualified expert, a judge capable of evaluating evidence, rapid cooperation channels, and guarantees that protect privacy and the rights of defense against any disproportionate expansion of surveillance and investigative tools.

- The study establishes that digital evidence enjoys a high degree of copyability, alterability, and deletability, and this very fact makes the integrity of collection, preservation, and documentation measures part of the value of the evidence itself. The court does not only need to know the content of the data; it must also be assured of its origin, the manner in which it was obtained, and the continuity of its integrity from the time of seizure until judicial examination.
- It became clear that encryption and anonymization technologies increase the difficulty of investigation, because they may prevent access to content or conceal the link between electronic activity and the person carrying it out. Consequently, developing digital forensic analysis capabilities and specialized training is no longer a secondary matter, but has become an essential element in the possibility of obtaining evidence in a reliable manner in court.
- The comparison showed that recognizing the admissibility of electronic records and data requires complementary formal rules that explain the manner of seizure, copying, impounding, and technical examination. In the Iraqi situation, there is a greater need for harmonizing standards and procedures, while Egypt's specialized law provides a clearer framework for certain measures; however, the need for disciplined technical and judicial implementation remains.
- Cross-border crimes reveal the inadequacy of relying solely on the territorial criterion, because the conduct, the result, the server, and the victim may each be in a different country. Therefore, drafting broad national jurisdiction is not sufficient; it must be accompanied by criteria that prevent conflicts of jurisdiction and make it possible to obtain data and evidence located abroad through legal channels.
- The study emphasizes that specialized cybercrime units enhance the efficiency of the response when they are linked to the public prosecution, the judiciary, experts, and continuous training programs. The effect of establishing these units is weakened if they are not equipped with technical tools, human resources, and uniform standards for dealing with devices and data, or if their technical results remain detached from the requirements of judicial proof.
- The analysis concludes that modern technology in investigations must operate under clear legal and judicial oversight, because tracking, analysis, and surveillance tools may harm privacy if used without regulation. Therefore, formal efficiency is not measured only by the speed of access to data, but also by the system's ability to achieve this while respecting legality, proportionality, and the rights of defense.
- It is recommended that uniform national protocols be drafted for the collection, copying, preservation, and examination of digital evidence, such that every stage and every person who has dealt with the evidence from the seizure of the device or account to the presentation of the result in court is documented. This documentation helps reduce disputes about the integrity of the evidence and provides the judiciary with a clearer basis for assessing its probative value.
- It is appropriate to establish specialized and continuous training programs for investigators, members of the public prosecution, judges, and experts in the field of digital investigations, and to update the training content in line with changing methods of committing crime. Training should combine the technical aspect with legal rules so that technical skill does not lead to unlawful action and legal knowledge does not lead to an inability to understand technical evidence.

- It is recommended that the rules of jurisdiction in cross-border cybercrimes be developed in a manner that clearly specifies the link between the crime and Iraq or Egypt and provides mechanisms for resolving cases of conflict of jurisdiction. These rules should be accompanied by practical channels of judicial assistance, information exchange, and expedited data preservation based on monitorable legal procedures.
- It is appropriate that specialized cybercrime units be supported with the human resources, hardware, and software necessary for digital forensic analysis, and that working standards be harmonized among the competent institutions. It is also preferable to establish stable coordination channels among the police, public prosecution, courts, and forensic centers to prevent duplication of measures or loss of evidence during transfer between institutions.
- It is recommended that criteria be established for accrediting experts and laboratories responsible for examining digital evidence, and that minimum requirements for documentation, re-testing, and the possibility of reviewing results be determined. The validity of a technical tool does not replace the validity of the manner of its use, and providing the possibility of reviewing examinations helps the court and the parties to discuss the evidence more fairly.
- The powers of access to data, surveillance, and tracking must be accompanied by clear judicial guarantees that respect the necessity, proportionality, scope, and duration of the authorization. These rules help create a balance between the speed of investigation and the protection of privacy and the rights of defense, and prevent the need to combat cybercrimes from leading to the unregulated expansion of data collection.

Author Contributions

All authors contributed equally to the conceptualization of the article and writing of the original and subsequent drafts.

Data Availability Statement

Data available on request from the authors.

Acknowledgements

The authors would like to thank the anonymous reviewers for their insightful comments and constructive feedback, which significantly improved the quality of this manuscript. We also extend our gratitude to our colleagues for their valuable discussions and technical support throughout this research.

Ethical Considerations

The authors strictly adhered to the highest standards of research integrity. The authors avoided data fabrication, falsification, plagiarism, and any other form of scientific misconduct.

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Conflict of Interest

The authors declare no conflict of interest.

پژوهش های نوین در مطالعات علوم انسانی اسلامی
شاپا الکترونیکی: ۸۹۴۴-۲۹۸۰
https://api.lu.ac.ir/
دانشگاه لرستان

چالش‌های شکلی و توسعهٔ سازوکارهای مقابله با جرائم سایبری در عراق و مصر: مطالعهٔ تطبیقی در اثبات، صلاحیت و تحقیقات دیجیتال

احمد محمد ناصر السلمان[۱]، محمدرضا ظفری[۲] ✉

۱. دانشجوی دکتری حقوق کیفری و جرم‌شناسی، دانشگاه قم، قم، ایران. رایانامه: ahmedmohamed4254641@gmail.com

۲. نویسنده مسئول، استادیار حقوق کیفری و جرم‌شناسی، دانشگاه پیام نور، تهران، ایران. رایانامه: mr_zafari@pnu.ac.ir

اطلاعات مقاله

نوع مقاله:
مقاله پژوهشی،

تاریخچه مقاله:
تاریخ دریافت: ۱۴۰۴/۱۰/۱۳
تاریخ بازنگری: ۱۴۰۵/۰۲/۱۵
تاریخ پذیرش: ۱۴۰۵/۰۳/۱۷
تاریخ انتشار: ۱۴۰۵/۰۴/۰۱

کلیدواژه‌ها:
دلیل دیجیتال،
اثبات کیفری،
صلاحیت قضایی،
تحقیقات دیجیتال،
جرائم سایبری،
عراق و مصر

چکیده

هدف: هدف پژوهش، تبیین ویژگی‌های دلیل دیجیتال و شرایط سلامت و حجیت آن، تحلیل تأثیر رمزنگاری و گمنام‌سازی بر گردآوری ادله، مقایسهٔ رویکردهای اثبات و صلاحیت در نظام‌های حقوقی عراق و مصر و سپس بررسی نقش واحدهای تخصصی و فناوری‌های نوین در ارتقای کارایی تحقیقات است.

روش پژوهش: روش پژوهش توصیفی ـ تحلیلی و تطبیقی است و بر مواد حقوقی و دکترینی مندرج در رسالهٔ اصلی تکیه دارد.

یافته‌ها: یافته‌ها نشان می‌دهد که موفقیت تعقیب کیفری دیجیتال در گرو حفظ سلامت زنجیرهٔ مواجهه با دلیل از لحظهٔ ضبط تا ارائه در دادگاه و نیز وجود قواعد روشن صلاحیت و همکاری در مواردی است که واقعه از قلمرو سرزمینی فراتر می‌رود. همچنین روشن شد که ایجاد واحدهای تخصصی و آموزش بازپرسان، قضات و کارشناسان شرطی عملی و ضروری است؛ زیرا متون قانونی به‌تنهایی برای مقابله با فناوری‌های رمزنگاری، پنهان‌سازی هویت و تحول شیوه‌های ارتکاب جرم کفایت نمی‌کنند.

نتیجه‌گیری: پژوهش نتیجه می‌گیرد که باید الگویی یکپارچه طراحی شود که قانون‌گذاری را با اثبات، صلاحیت، همکاری و فنون جرم‌یابی دیجیتال پیوند دهد و با نظارت قضایی همراه باشد تا تناسب را تضمین کند و از حریم خصوصی و حقوق دفاع صیانت نماید. افزون بر این، پژوهش تأکید می‌کند که توسعهٔ ابزارهای فنی تنها زمانی اثربخش خواهد بود که با یکسان‌سازی استانداردهای حرفه‌ای حاکم بر استخراج، بررسی و مستندسازی داده‌ها همراه شود؛ به‌گونه‌ای که امکان بازبینی نتیجهٔ فنی فراهم آید و اعتماد دستگاه قضایی به سلامت دلیل تقویت شود.

استناد: محمد ناصر السلمان، احمد و ظفری، محمدرضا. (۱۴۰۵). چالش‌های شکلی و توسعهٔ سازوکارهای مقابله با جرائم سایبری در عراق و مصر: مطالعهٔ تطبیقی در اثبات، صلاحیت و تحقیقات دیجیتال. *پژوهش های نوین در مطالعات علوم انسانی اسلامی*، (۱۰) ۵، ۲۴-۱.

https://doi.org/10.22034/api.2026.2118597.2071

ناشر: دانشگاه لرستان.

© نویسندگان.

DOI: https://doi.org/10.22034/api.2026.2118597.2071

مقدمه

گفتار اول: دلیل دیجیتال و چالش‌های اثبات در جرائم سایبری

بُعد شکلی مقابله با جرائم سایبری بر این واقعیت استوار است که جرم دیجیتال به همان شیوه‌ای که جرائم سنتی اثبات می‌شوند، قابل اثبات نیست؛ زیرا اطلاعاتی که موضوع استدلال قرار می‌گیرد در مدتی کوتاه قابل نسخه‌برداری، تغییر، حذف و انتقال است و آثار آن ممکن است میان دستگاه‌ها، سرورها و حساب‌هایی پراکنده باشد که در مکان‌های متعددی قرار دارند. از این رو، مسئله تنها به یافتن دلیل محدود نمی‌شود، بلکه به اثبات سلامت منشأ آن، استمرار تصرف و نگهداری آن، عدم دستکاری در محتوای آن و تبیین پیوند فنی و حقوقی میان دلیل از یک سو و واقعهٔ مجرمانه و متهم از سوی دیگر نیز گسترش می‌یابد. این امر مستلزم قواعد شکلی دقیق، نیروهای متخصص و ابزارهای فنی‌ای است که بتوانند دلیل را از لحظهٔ ضبط تا زمان ارائه به دادگاه حفظ کنند.

بند اول: ویژگی‌های دلیل دیجیتال و شرایط حجیت آن

مسئلهٔ اثبات در جرائم سایبری یکی از پیچیده‌ترین چالش‌هایی است که دستگاه‌های عدالت کیفری با آن روبه‌رو هستند؛ به‌ویژه در کشورهایی که فاقد زیرساخت فنی پیشرفته و نیروهای قضایی واجد صلاحیت برای مواجهه با ادلهٔ دیجیتال‌اند. منشأ این دشواری متعدد و گسترده است و ماهیت خودِ دلیل دیجیتال، مشکلات تصرف، نگهداری و تحلیل جرم‌یابانه و نیز میزان حجیت آن در دادگاه را دربر می‌گیرد (سرور، ۲۰۱۵، ۴۵).

دلیل دیجیتال تفاوتی بنیادین با دلیل مادی سنتیِ شناخته‌شده در دکترین کلاسیک اثبات کیفری دارد؛ چرا که مجموعه‌ای از ویژگی‌های فنی و مجازی را داراست که به‌کارگیری و اتکا به آن را در دعوای کیفری دشوار می‌سازد. در حالی که دلیل سنتی بر موجودیتی فیزیکی، ملموس و پایدار مانند سلاح یا اثر انگشت استوار است، دلیل دیجیتال در جوهر خود داده‌هایی رمزگذاری‌شده یا اطلاعاتی غیرمادی است که بر رسانه‌های الکترونیکی و سرورهای ابری ذخیره شده‌اند؛ امری که آن را به‌شدت شکننده و تغییرپذیر می‌سازد و امکان حذف یا نسخه‌برداری از آن را به‌آسانی و به دست افراد حرفه‌ای فراهم می‌کند، بی‌آنکه هیچ اثر مادی آشکاری بر جای بماند که با چشم غیرمسلح قابل درک باشد.

این دلیل از قابلیت منحصربه‌فردِ انتشار آنی، تغییر شکل و عبور آزادانه از مرزها و موانع جغرافیایی در کسری از ثانیه از طریق شبکه‌های بین‌المللی برخوردار است؛ امری که به آن خصلتی فراقاره‌ای می‌بخشد و قواعد سنتی صلاحیت قضایی مکانی را دچار اختلال می‌کند. این سیالیت فنی، فقدان ماهیت مادی و سهولت از بین رفتن، فرایند حفظ، استخراج و بررسی دلیل دیجیتال را به چالشی بزرگ بدل می‌سازد که نیازمند سازوکارهای شکلی نوآورانه و پروتکل‌های سخت‌گیرانه در تحقیقات دیجیتال است تا از آلودگی یا دستکاری دلیل جلوگیری شود و قاضی کیفری به حجیت آن و سلامت زنجیرهٔ نگهداری‌اش از لحظهٔ ضبط تا صدور حکم اقناع گردد. ادبیات تخصصی در دانش جرم‌یابی دیجیتال چهار ویژگی بنیادین برای دلیل دیجیتال برمی‌شمارد: نخست، شکنندگی: زیرا در صورت مواجهه با آن بدون رعایت پروتکل‌های فنی معین، به‌آسانی آسیب می‌بینند. دوم، تکرارپذیری: زیرا می‌توان نسخه‌ای کاملاً منطبق با اصل از آن تهیه کرد. سوم، پراکندگی: زیرا ممکن است بر سرورهایی در کشورهای متعدد توزیع شده باشد. و چهارم، پنهان‌بودگی: زیرا می‌توان آن را با فنون رمزنگاری و پنهان‌سازی دیجیتال مخفی کرد (قانون مکافحة جرائم تقنیة المعلومات، ۲۰۱۸، م. ۴).

دلیل دیجیتالِ قانوناً پذیرفتنی باید سه معیار تجمعی و سخت‌گیرانه را احراز کند تا حجیت آن و توانایی‌اش در ایستادگی در برابر ایرادهای حقوقی در دادرسی کیفری تضمین شود. نخستین معیار، اصالت است که مقامات فنی را ملزم می‌کند ثابت کنند دلیل از منبع اصلی خود استخراج شده و از لحظهٔ ضبط و گردآوری دستخوش هیچ‌گونه تغییر، دستکاری یا آلودگی نشده است امری که از نظر فنی از طریق تطبیق مقادیر درهم‌ساز (هش) فایل‌ها احراز می‌شود. معیار دوم، سلامت است که پیوندی تنگاتنگ

با مستندسازی کامل زنجیرهٔ نگهداری دارد و مستلزم ثبت دقیق و مستمر هر مرحله‌ای است که دلیل از آن گذشته است از شخصی که آن را ضبط کرده و شیوهٔ انتقال آن گرفته تا شرایط محیطی بررسی و هویت کارشناسانی که با آن سروکار داشته‌اند، تا اطمینان حاصل شود که هیچ خلأ زمانی یا شکلی که امکان نفوذ یا دستکاری در داده‌ها را فراهم کند، وجود ندارد.

معیار سوم، ارتباط و پیوستگی است که اثبات وجود رابطه‌ای منطقی، حقوقی و مستقیم میان دلیل دیجیتالِ استخراج‌شده و واقعهٔ مجرمانهٔ موضوع اتهام را ایجاب می‌کند؛ زیرا صحت فنی دلیل کافی نیست، بلکه دلیل باید عملاً در کشف حقیقت مؤثر باشد، خواه با اثبات جرم و خواه با نفی آن از متهم مانند پیوندی که میان نشانی IP مظنون و زمان وقوع حملهٔ سایبری برقرار می‌شود. فقدان هر یک از این سه معیار، وصف حقوقی دلیل را زائل می‌کند و دادگاه را از استناد به آن محروم می‌سازد و این نشان می‌دهد که پذیرش دلیل دیجیتال تنها به ارزش فنی آن وابسته نیست، بلکه به انضباط شکلی بسیار دقیق آن نیز بستگی دارد. احتمال تغییر یا حذف دلیل دیجیتال از جدی‌ترین مشکلاتی است که مراجع تحقیق با آن مواجه‌اند، خواه این امر از سوی مرتکب جرم و به قصد امحای ادله صورت گیرد و خواه در نتیجهٔ خطای غیرعمدی ضابطان دادگستری هنگام کار با دستگاه‌های الکترونیکی. دکترین کیفری دیجیتال قاعده‌ای را بنا نهاده است که بر اساس آن، پیش از آغاز تحلیل هر رسانهٔ الکترونیکی باید نسخه‌ای کاملاً مطابق با اصل از آن تهیه شود و اصل آن سالم نگه داشته شود تا امکان راستی‌آزمایی آن در دادگاه فراهم باشد (قانون الإثبات العراقی، ۱۹۷۹، م. ۳).

بند دوم: گردآوری ادله و حفظ سلامت آن‌ها در برابر تغییر، رمزنگاری و گمنام‌سازی

گسترش فناوری‌های رمزنگاری قوی و نرم‌افزارهای گمنام‌سازی، مانند شبکه‌های پنهان‌سازی هویت و برنامه‌های پیام‌رسان رمزگذاری‌شده، لایه‌ای تازه از پیچیدگی را به فرایند گردآوری و تحلیل ادلهٔ دیجیتال افزوده است چرا که گروه‌های جرائم سازمان‌یافته و شبکه‌های جرائم سایبری به‌طور فزاینده‌ای برای مصون‌سازی ارتباطات و پنهان‌کردن تراکنش‌های مالی الکترونیکی خود به این فناوری‌ها روی می‌آورند به‌گونه‌ای که بازپرسان گاه حتی با به‌کارگیری پیشرفته‌ترین ابزارهای موجود در تحلیل جرم‌یابانهٔ دیجیتال نیز از عبور از این موانع فنی ناتوان می‌مانند.

قانون‌گذار مصری قانونی ویژه را به مقابله با جرائم سایبری اختصاص داد که در قالب قانون شمارهٔ ۱۷۵ مصوب ۲۰۱۸ تجلی یافت. این قانون در پی مباحثات گسترده دربارهٔ خلأ تقنینی موجود در مواجهه با جرائم دیجیتال به تصویب رسید و توجه ویژه‌ای به مسئلهٔ اثبات مبذول داشت چنان‌که مادهٔ چهارم آن، استناد به سوابق و داده‌های الکترونیکی را به‌عنوان دلیل در دعاوی کیفریِ مرتبط با جرائم رایانه‌ای مجاز دانست.

این قانون ارائه‌دهندگان خدمات اینترنتی و سکوهای دیجیتال را مکلف کرد که سوابق استفاده را دست‌کم به مدت یکصدوهشتاد روز نگهداری کنند و در صورت درخواست، بر اساس ضوابط قانونی معین در اختیار مراجع تحقیق قرار دهند. قانون‌گذار مصری پیش‌تر برخی از صور جرائم سایبری را در قانون امضای الکترونیکی شمارهٔ ۱۵ مصوب ۲۰۰۴ مورد توجه قرار داده بود قانونی که نخستین گام تقنینی و سنگ‌بنای به رسمیت شناختن معاملات مجازی به شمار می‌رفت. این قانون صراحتاً امضای الکترونیکی و اسناد دیجیتال را به‌عنوان ادلهٔ اثبات رسمی و عادی به رسمیت شناخت و برای آن‌ها همان حجیت قانونی مقرر برای امضاها و اسناد کاغذی سنتی را در حوزهٔ معاملات مدنی و تجاری قائل شد. فلسفهٔ تقنینی این حکم در تشویق سرمایه‌گذاری، پشتیبانی از خدمات بانکی و فراهم‌آوردن امنیت حقوقی برای نظام نوپای تجارت الکترونیکی در آن زمان نهفته بود. با این حال، این قانون از خلأ عملی آشکاری رنج می‌برد زیرا دامنهٔ اجرای آن در دعاوی کیفری و در دادگاه‌های جزایی محدود و ناکافی باقی ماند و به شکل مطلوب به اقتضائات مقابله با بزهکاری رایانه‌ای رو به رشد پاسخ نداد.

این کاستی کیفری از آنجا ناشی می‌شود که فلسفهٔ قانون ۲۰۰۴ در درجهٔ نخست مدنی و تجاری بود و از نظر ساختاری برای مقابله با فنون پیچیدهٔ جرائم سایبری آماده نبود؛ از این رو، جرائمی چون نفوذ به شبکه‌ها، سرقت هویت دیجیتال، ازکاراندازی سرورها و تعرض به داده‌های شخصی بیرون از چتر شکلی و ماهوی این قانون باقی ماندند. افزون بر این، دادگاه‌های کیفری که تابع اصل سخت‌گیرانهٔ قانونی بودن جرائم و مجازات‌ها هستند، از قیاس یا تفسیر موسع مواد این قانون برای

جرم‌انگاری الگوهای نوظهور سرقت و کلاهبرداری دیجیتال ناتوان بودند امری که تصویب قانونی متأخر و تخصصی یعنی قانون مبارزه با جرائم فناوری اطلاعات شمارهٔ ۱۷۵ مصوب ۲۰۱۸ را برای پرکردن این شکاف و تأمین حمایت کیفری کامل از فضای دیجیتال، ضروری و فوری ساخت (الحلبی، ۲۰۰۰، ۱۳۴).

در سطح رویهٔ قضایی، دادگاه‌های تجدیدنظر مصر همواره بر لزوم صدور گزارش از سوی کارشناس رسمی برای اعطای حجیت کامل به دلیل دیجیتال سخت‌گیری کرده‌اند. این رویکرد از نظر شکلی صحیح است، اما بار سنگینی بر دوش مقامات تعقیب می‌گذارد و با توجه به کمبود کارشناسان رسمیِ جرم‌یابی دیجیتال، رسیدگی به پرونده‌ها را طولانی می‌کند. دکترین حقوقی مصر همچنان دربارهٔ ماهیت دلیل دیجیتال دچار اختلاف است: آیا این دلیل در زمرهٔ نوشته به مفهوم سنتیِ مندرج در قانون اثبات مدنی قرار می‌گیرد، یا امارهٔ قضایی مستقلی به شمار می‌آید؟

قانون مبارزه با جرائم فناوری اطلاعات شمارهٔ ۱۷۵ مصوب ۲۰۱۸ نظامی نظارتی و شکلیِ یکپارچه پدید آورد که به موجب آن، نظارت فنی جامع بر فضای دیجیتال و هماهنگی مستقیم با مراجع تحقیق و ضابطان دادگستری در جرائم سایبری به سازمان ملی تنظیم مقررات ارتباطات به‌عنوان مرجع عالی واگذار شد. این نظام از لحاظ نظری به تسهیل ردیابی مرتکبان، دستیابی به ادلهٔ دیجیتال از منابع آن‌ها و تأمین حفظ این ادله بر اساس پروتکل‌هایی که مانع دستکاری یا آلودگی فنی آن‌ها می‌شود، کمک می‌کند. با این همه، اجرای عملی در میدان واقعیت، شکاف‌ها و خلأهای شکلی آشکاری را نمایان ساخت به‌ویژه در سازوکارهای هماهنگی میدانی و زمانی میان مهندسان سازمان ملی و دادسرا، چرا که دلیل دیجیتال مستلزم سرعت بسیار بالا در ضبط و تحقیق است و این امر گاه با بوروکراسی اداری و کندی در صدور مجوزهای قضایی پیشین تعارض پیدا می‌کند. مانع دیگری نیز در قالب ناهمگونی فنی و ضعف امکانات فنی و مادی برخی از واحدهای مبارزه با جرائم اینترنتی در استان‌ها در مقایسه با حجم جهش فناورانهٔ شتابان رخ نمود زیرا برخی از این واحدهای فرعی فاقد نرم‌افزارهای نوین برای رمزگشایی پیچیده یا ابزارهای بازیابی داده‌های حذف‌شده از فضاهای ذخیره‌سازی ابری‌اند و افزون بر آن، با کمبود عددی نیروی انسانیِ واجد صلاحیت برای همگامی با روش‌های پیچیدهٔ رخنه‌گران مواجه‌اند. این فاصله میان متن تقنینیِ بلندپروازانه و واقعیت عملی موجب شده است که بسیاری از ادلهٔ دیجیتال به دلیل خطاهای شکلی در بررسی یا انتقال، در معرض ایراد بطلان در دادگاه‌ها قرار گیرند امری که راهبردی ملی و مستمر برای نوسازی زیرساخت این واحدها و آموزش کارکنان آن‌ها به منظور تضمین کارآمدی قانون را ایجاب می‌کند (حجازی، ۲۰۰۹، ۲۰۱).

گسترش اختیارات نظارتی و گردآوری پیشدستانهٔ داده‌ها که قانون ۱۷۵ مصوب ۲۰۱۸ به مراجع تحقیق اعطا کرده است، پرسش‌های بنیادینی را دربارهٔ توازن میان اقتضائات تعقیب کیفری و تضمینات حمایت از حریم خصوصی که در مادهٔ نوزدهم قانون اساسی ۲۰۱۴ مصر تضمین شده است، برمی‌انگیزد. گروهی از حقوق‌دانان بر این باورند که برخی از احکام این قانون متضمن درجه‌ای از خودسری در نظارت دیجیتال است که از حدود قابل قبول در پرتو معیارهای بین‌المللی حقوق بشر فراتر می‌رود.

یکی از برجسته‌ترین چالش‌های دیجیتال معاصر، دشواری اثبات جرائم سایبری به سبب ماهیت غیرمادی آن‌ها و اتکا به ادلهٔ دیجیتالی است که به تخصص فنی بالایی نیاز دارد. در عراق، نظام قضایی از کمبود کارشناسان حقوقیِ متخصص در جرائم سایبری رنج می‌برد؛ امری که به رد بسیاری از پرونده‌ها یا تأخیر چندساله در رسیدگی به آن‌ها می‌انجامد، چنان‌که در پرونده‌های کلاهبرداری الکترونیکی رخ داد که تحقیقات به سبب عدم مستندسازی صحیح ادله ناکام ماند. افزون بر این، مرتکبان از فناوری‌های پیشرفتهٔ رمزنگاری و شبکه‌های خصوصی مجازی (VPN) بهره می‌گیرند که هویت آنان را پنهان می‌سازد و کار پلیس را مختل می‌کند، به‌ویژه با توجه به ضعف زیرساخت دیجیتال کشور؛ و این نشان می‌دهد که چالش‌های فنی از توانمندی‌های کنونی تعقیب کیفری فراتر رفته است. این دشواری‌ها با فقدان قانونی تخصصی برای جرائم سایبری تشدید می‌شود چرا که تلاش‌ها برای تصویب لایحهٔ قانون جرائم رایانه‌ای در سال‌های ۲۰۱۱ و ۲۰۱۹ به دلیل نگرانی از محدودشدن آزادی بیان ناکام ماند و همین امر، اجرای قوانین سنتی را برای مقابله با جرائم نوظهوری مانند جعل عمیق (دیپ‌فیک) مبتنی بر هوش مصنوعی که در اخاذی و افترا به کار می‌رود، ناکافی ساخته است.

بند سوم: مقایسهٔ عراق و مصر در اثبات دیجیتال

برخلاف تجربهٔ مصر، عراق همچنان فاقد قانونی جامع برای مبارزه با جرائم سایبری است زیرا با وجود طرح لوایح متعدد در پارلمان عراق طی بیش از یک دهه، قانون جرائم رایانه‌ای در شکل نهایی خود به تصویب نرسیده است. در غیاب این قانون، دادگاه‌های عراق ناگزیرند به قواعد عام مندرج در قانون مجازات شمارهٔ ۱۱۱ مصوب ۱۹۶۹ و قانون آیین دادرسی کیفری شمارهٔ ۲۳ مصوب ۱۹۷۱ استناد کنند قواعدی که در دوره‌ای پیش از پیدایش اینترنت تدوین شده‌اند و همین امر به خلأهای آشکاری در مواجهه با جرائم دیجیتال منجر می‌شود (محمود، ۱۹۸۱، ۹۵).

در زمینهٔ اثبات، برخی از دادگاه‌های عراق با تفسیر موسع به مادهٔ سوم قانون اثبات شمارهٔ ۱۰۷ مصوب ۱۹۷۹ برای پذیرش اسناد الکترونیکی به‌عنوان دلیل استناد کرده‌اند؛ اما این توسع قضایی در پذیرش دلیل مجازی همچنان محدود و فاقد نظم شکلی منضبط است و بر معیارهای تقنینی روشن یا پروتکل‌های فنی یکسان تکیه ندارد. نتیجهٔ این وضع، تعارض آشکار در احکام صادره از دادگاه‌های عراق در قبال مسائل اثباتی یکسان و واقعهٔ دیجیتال واحد است برای نمونه، در حالی که یک دادگاه تصاویر صفحه‌نمایش (اسکرین‌شات) را دلیلی کامل بر محکومیت تلقی می‌کند، دادگاهی دیگر آن را صرفاً امارهٔ ساده‌ای می‌داند که به‌آسانی قابل جعل است امری که اصل ثبات رویهٔ قضایی را متزلزل می‌سازد و به تضمینات دادرسی منصفانه خدشه وارد می‌کند. این آشفتگی در پرتو کمبود شدید آزمایشگاه‌های تخصصی و دولتیِ جرم‌یابی دیجیتال، که برای بررسی و ارزیابی دقیق ادلهٔ سایبری دشوار لازم‌اند، در دستگاه‌های امنیتی و قضایی عراق عمیق‌تر می‌شود.

این کاستی نهادیِ تلخ، دادگاه‌ها را در موارد آشکار و فراوان وادار می‌کند که برای پرکردن خلأ فنی از کارشناسان مستقل و دفاتر نرم‌افزاری بخش خصوصی کمک بگیرند؛ آن هم بدون وجود معیارهای قانونی سخت‌گیرانه یا چارچوب‌های تنظیمی روشن برای تأیید صلاحیت این کارشناسان، ارزیابی توانمندی فنی آنان یا حتی تضمین بی‌طرفی و رازداری‌شان در تحقیقات حساس. این رویه باب اعتراض به سلامت گزارش‌های فنیِ ارائه‌شده را کاملاً می‌گشاید چرا که دفاع به‌آسانی می‌تواند احتمال آلودگی یا دستکاری دلیل را در جریان دست‌به‌دست‌شدن آن در خارج از مقرهای رسمی نشان دهد. این امر دستگاه قضایی کیفری را از یقینی که احکام جزایی اقتضا می‌کنند محروم می‌سازد و تصویب قانونی جامع را که ادلهٔ دیجیتال را تنظیم کند و آزمایشگاه‌های ملیِ حاکمیتی تأسیس نماید، به ضرورتی عاجل و تأخیرناپذیر بدل می‌کند.

برخی از دادگاه‌های عراق از راه قیاس، احکام جرائم کلاهبرداری، فریب و سرقت مندرج در قانون مجازات شمارهٔ ۱۱۱ مصوب ۱۹۶۹ را بر جرائم سایبری دارای ماهیت مالی اعمال کرده‌اند. این راه‌حل از نظر حقوقی تکلف‌آمیز می‌نماید زیرا قیاس در امور کیفری متضمن نقض صریح اصل قانونی بودن جرائم و مجازات‌هاست که در مادهٔ نوزدهم خودِ قانون مجازات عراق مقرر شده و بر اساس آن، هیچ جرم و مجازاتی جز به موجب نص قانون وجود ندارد. این خلأ تقنینی، معضلی بنیادین در سطح قانون اساسی و قوانین عادی است که با اجتهاد قضایی قابل رفع نیست (ن. صالح، ۲۰۲۰، ۴۵).

لوایح قانون جرائم رایانه‌ای عراق که در جریان بررسی بوده‌اند، نشان می‌دهند که قانون‌گذار عراقی به ضرورت مبرم رفع این خلأ تقنینی آگاه شده است اما این لوایح طی سال‌ها به دلیل مناقشات سیاسیِ مطرح‌شده دربارهٔ برخی از احکام آن‌ها که به آزادی بیان و روزنامه‌نگاری دیجیتال مربوط است، متوقف مانده‌اند. در مقابل، مدافعان حقوق بشر معتقدند که برخی از عبارات این لوایح متضمن محدودیت‌هایی ناروا است که ممکن است به‌جای ابزاری برای مبارزه با جرم، به ابزاری برای سرکوب سیاسی تبدیل شود. مقایسهٔ تجربه‌های مصر و عراق، تفاوت آشکاری را در سطح آمادگی تقنینی نشان می‌دهد: مصر از چارچوب قانونی تخصصی برخوردار است، هرچند با کاستی‌هایی در اجرا همراه است در حالی که عراق در سایهٔ خلأ تقنینی‌ای به سر می‌برد که مانع مقابلهٔ مؤثر با جرائم دیجیتال است. وجه مشترک دو کشور، نیاز به سرمایه‌گذاری در آموزش قضایی و فنی و استقرار معیارهای روشن و الزام‌آور برای مواجهه با ادلهٔ دیجیتال است به‌گونه‌ای که هم حق دولت در تعقیب کیفری و هم حق متهم بر دادرسی منصفانه تضمین شود.

مقایسه نشان می‌دهد که توسعهٔ قواعد اثبات دیجیتال تنها با به رسمیت شناختن نظریِ حجیت داده‌های الکترونیکی محقق نمی‌شود، بلکه مستلزم زنجیره‌ای به‌هم‌پیوسته از تضمینات است که از مشروعیت گردآوری دلیل آغاز می‌شود، از مستندسازی

اقدامات استخراج، نسخه‌برداری و تحلیل آن می‌گذرد و با فراهم‌آوردن امکان بررسی دلیل و مناقشه در سلامت فنی آن برای دادگاه و طرفین دعوا پایان می‌یابد. این نیاز در عراق به سبب اتکای بیشتر به قواعد عام و تجربهٔ عملی شدیدتر است؛ در حالی که وجود قانون تخصصی در مصر عرصهٔ روشن‌تری برای تنظیم نحوهٔ مواجهه با سوابق و داده‌های الکترونیکی فراهم آورده است. با این حال، توانمندی فنی بازپرس، کارشناس و قاضی در هر دو نظام عنصری تعیین‌کننده باقی می‌ماند (عبدالرازق، ۲۰۲۱، ۲۸).

گفتار دوم: صلاحیت قضایی و همکاری در جرائم سایبری فرامرزی

ماهیت دیجیتال جرم تنها به دشواری اثبات محدود نمی‌شود، بلکه به تعیین دادگاه صالح و قانون حاکم نیز گسترش می‌یابد. ممکن است رفتار مجرمانه در یک کشور آغاز شود، از سروری در کشور دوم عبور کند و نتیجهٔ آن در کشور سوم پدیدار شود، در حالی که بزه‌دیده یا مرتکب در کشور دیگری حضور دارد. این تعدد مکانی، قواعد سنتی صلاحیت را در معرض آزمونی واقعی قرار می‌دهد زیرا معیار محل ارتکاب جرم یا محل تحقق نتیجه دیگر همواره به‌تنهایی کافی نیست. از این رو، جست‌وجوی ضوابطی که هم از بی‌کیفرمانی جلوگیری کنند و هم مانع تعدد محاکمات و تعارض مراجع قضایی شوند، به بخشی اساسی از سیاست جنایی ویژهٔ جرائم سایبری بدل می‌شود.

بند اول: ماهیت فرامرزی و تعارض صلاحیت

صلاحیت قضایی در حوزهٔ جرائم سایبری معضلی بسیار پیچیده است که ابعاد آن از قلمرو حقوق کیفری داخلی فراتر می‌رود و به عمق حقوق بین‌الملل خصوصی و قواعد حل تعارض متداول در سطح بین‌المللی می‌رسد. این معضل از تعارض ریشه‌ای میان مجازی بودن فضای سایبر که مرزهای جغرافیایی را به رسمیت نمی‌شناسد و اصل حاکمیت سرزمینی که ستون اصلی صلاحیت کیفری در حقوق بین‌الملل معاصر است، سرچشمه می‌گیرد. معضل صلاحیت قضایی در جرائم سایبری در آشکارترین صورت خود هنگامی نمایان می‌شود که جرمی واحد هم‌زمان در چند کشور واقع شود چنان‌که ممکن است مرتکب در یک کشور اقامت داشته باشد، سرور الکترونیکی در کشور دوم قرار گیرد و بزه‌دیده در کشور سوم ساکن باشد. در این فرض، به سبب تعارض قواعد صلاحیت در قوانین کشورهای مختلف، تعیین کشور صالح دشوار می‌شود. این وضعیت پدیده‌ای را پدید آورده که در ادبیات بین‌المللی به پناهگاه‌های امن سایبری شهرت دارد یعنی مجرمان سایبری عامدانه حملات خود را از کشورهایی هدایت می‌کنند که قوانین ضعیف یا همکاری قضایی بین‌المللی اندکی دارند.

نظریه‌های صلاحیت قضایی در جرائم سایبری در دکترین تطبیقی به سه رویکرد اصلی تقسیم می‌شوند: رویکرد نخست به اصل صلاحیت سرزمینی پایبند است که بر اساس آن، کشوری صالح است که نتیجهٔ جرم در آن تحقق یافته یا رفتارهای مجرمانه از آن آغاز شده است. رویکرد دوم اصل صلاحیت شخصی فعال را می‌پذیرد که به موجب آن، صلاحیت قضایی برای تعقیب مرتکبی که تابعیت کشور تعقیب‌کننده را دارد، صرف‌نظر از محل ارتکاب جرم، گسترش می‌یابد و رویکرد سوم صلاحیت جهانی را مطابق آنچه کنوانسیون‌های بین‌المللی برای دسته‌های معینی از جرائم سایبری شدید، مانند تروریسم سایبری و حمله به زیرساخت‌های حیاتی، مقرر می‌دارند، مجاز می‌شمارد.

فضای سایبر دو نوع متضاد از معضلات صلاحیت را پدید می‌آورد: تعارض مثبت که در آن دو یا چند کشور بر سر صلاحیت رسیدگی به جرمی واحد رقابت می‌کنند و ممکن است به محاکمهٔ مضاعف بینجامد و تعارض منفی که در آن همهٔ کشورها از پذیرش صلاحیت شانه خالی می‌کنند و جرم به‌کلی از مجازات می‌گریزد. تعارض منفی بزرگ‌ترین خطر را برای نظام عدالت کیفری بین‌المللی در پی دارد به‌ویژه در جرائم سایبری با پیچیدگی فنی بالا که به منابع تحقیقاتی عظیمی نیاز دارند و کشورهای کوچک یا در حال توسعه ممکن است از تأمین آن‌ها ناتوان باشند (م. ع. حسن، ۲۰۱۹، ۱۳۴). از این وضعیت، تعارض مثبت هنگامی پدید می‌آید که بیش از یک کشور بر صلاحیت خود نسبت به فعل واحد پافشاری کند و تعارض منفی هنگامی که هر کشور به این بهانه که بخش مهم‌تر رفتار در خارج از قلمرو آن واقع شده است، از تعقیب خودداری ورزد. اهمیت همکاری قضایی

دقیقاً در همین نقطه آشکار می‌شود زیرا ادله، حساب‌ها و داده‌ها ممکن است تحت کنترل ارائه‌دهندهٔ خدمات یا نهادی خارجی باشند که مرجع تحقیق ملی نمی‌تواند مستقیماً به آن دسترسی یابد. بنابراین، کارآمدی صلاحیت تنها با گستردگی متن قانونی سنجیده نمی‌شود، بلکه به وجود مجاری قانونی‌ای بستگی دارد که تبادل اطلاعات، درخواست‌های معاضدت و حفظ فوری داده‌ها را به نحوی که حاکمیت کشورها و تضمینات دادرسی منصفانه را محترم بشمارد، امکان‌پذیر سازد.

بند دوم: قواعد صلاحیت در قانون‌گذاری و رویهٔ مصر

قانون‌گذار مصری در قانون آیین دادرسی کیفری، به‌ویژه در مواد دوم و سوم آن، اصل صلاحیت سرزمینی را مبنای صلاحیت قضایی قرار داده است؛ بدین معنا که دادگاه‌های مصر به جرائمی که کلاً یا جزئاً در سرزمین مصر واقع می‌شوند، رسیدگی می‌کنند. قانون مبارزه با جرائم فناوری اطلاعات شمارهٔ ۱۷۵ مصوب ۲۰۱۸ تحولی شکلی و کیفی پدید آورد و دامنهٔ صلاحیت قضایی دادگاه‌های مصر را به نحو چشمگیری به فراسوی مرزهای سرزمینی کلاسیک گسترش داد تا با ماهیت مجازی و فراقاره‌ای جرم سایبری مقابله کند. از آنجا که قواعد سنتی قانون مجازات اساساً بر اصل صلاحیت سرزمینی استوار بود که صلاحیت را به محل وقوع رفتار مادی جرم پیوند می‌داد، مادهٔ پنجم این قانون اصل صلاحیت واقعی (حمایتی) و اصل صلاحیت شخصی فعال را پذیرفت و صراحتاً به دادگاه‌های مصر اجازه داد به تعقیب قضایی جرائم سایبری‌ای که به‌طور کامل از خارج از مرزهای کشور و از طریق سرورهای خارجی ارتکاب یافته‌اند، رسیدگی کنند مشروط بر آنکه این جرائم اثری بر منافع اساسی مصر برجای گذارند، امنیت ملی را تهدید کنند یا به شهروندان و ساکنان مصر آسیب رسانند.

این گسترش تقنینی، سدی حقوقی برای حمایت از دولت در عصر جنگ‌های سایبری و رخنه‌گری سازمان‌یافته به شمار می‌آید زیرا دیگر نمی‌توان مرتکبان را صرفاً به این دلیل که دکمهٔ تخریب یا اخاذی را از آن سوی دریاها فشار می‌دهند، مصون داشت. اگر شخص یا سازمانی خارجی به شبکهٔ ارتباطات دولتی نفوذ کند، زیرساختی حیاتی مانند برق و بانک‌ها را از کار بیندازد یا از شهروندی مصری به‌صورت الکترونیکی اخاذی کند، دستگاه قضایی مصر صلاحیت قانونی کامل برای صدور قرار بازداشت بین‌المللی و توصیف اتهام را دارد امری که حاکمیت دیجیتال دولت را تقویت می‌کند. با این حال، فعال‌سازی این حکم بلندپروازانه در عمل همچنان به میزان انعطاف و قوت موافقت‌نامه‌های همکاری قضایی و امنیتی بین‌المللی و استرداد مجرمان وابسته است با توجه به پیچیدگی‌هایی که برخی کشورهای خارجی ایجاد می‌کنند و ممکن است به بهانهٔ تفاوت قوانین یا حمایت از آزادی‌های کاربران شبکه‌هایشان از همکاری سر باز زنند.

در چارچوب همکاری بین‌المللی، مصر شماری از موافقت‌نامه‌های دوجانبه را برای تبادل اطلاعات و استرداد مجرمان منعقد کرده و به پروتکل‌های مرتبط سازمان ملل متحد در زمینهٔ مبارزه با جرائم سازمان‌یافتهٔ فراملی پیوسته است. با این حال، عدم الحاق مصر به کنوانسیون بوداپست دربارهٔ جرائم رایانه‌ای مصوب ۲۰۰۱، که جامع‌ترین مرجع در این زمینه به شمار می‌رود، دامنهٔ همکاری این کشور را با کشورهای غربیِ عضو آن محدود می‌کند و آن را از بهره‌مندی از سازوکارهای تبادل فوری ادلهٔ دیجیتال مقرر در این کنوانسیون محروم می‌سازد (شورای اروپا، ۲۰۰۱).

دادگاه‌های مصر با پرونده‌های سایبری بسیار پیچیده‌ای که دارای عنصر خارجی بوده‌اند، روبه‌رو شده‌اند (س. صالح، ۲۰۲۳، ۱۷) و ناگزیر شده‌اند به احکام همکاری قضایی بین‌المللی مندرج در فصل سوم قانون آیین دادرسی کیفری استناد کنند. این امر در برخی موارد به تأخیر محسوس در جریان تحقیقات انجامیده است به سبب طولانی بودن و پیچیدگی تشریفات نیابت قضایی بین‌المللی، به‌ویژه با کشورهایی که موافقت‌نامهٔ دوجانبهٔ روشنی با مصر ندارند. دکترین کیفری مصر خاطرنشان می‌سازد که ایجاد واحدی ملی، تخصصی و مستقل که انحصاراً وظیفهٔ هماهنگی و رسیدگی به پرونده‌های جرائم سایبری فرامرزی را بر عهده داشته باشد، در پرتو افزایش تهدیدهای سایبری پیچیده به ضرورتی تقنینی و شکلی بدل شده است که تأخیر برنمی‌تابد. علت این دیدگاه آن است که پراکندگی صلاحیت‌های کنونی میان بخش‌های وزارت کشور (مانند ادارهٔ مبارزه با جرائم رایانه‌ای)، دادسرا، سازمان ملی تنظیم مقررات ارتباطات و سازمان اطلاعات عمومی، نوعی کندی اداری پدید می‌آورد که به هیچ وجه با

ماهیت آنیِ جرم دیجیتال تناسب ندارد چرا که ادلهٔ مجازیِ ذخیره‌شده بر سرورهای خارجی ممکن است ظرف چند ثانیه پاک یا رمزگذاری شوند، در حالی که مراجع داخلی در انتظار طی تشریفات اداری روزمره‌اند.

حقوق‌دانان بر این باورند که این واحد پیشنهادی باید به‌عنوان مرکز ارتباطی حاکمیتیِ واحد به‌صورت شبانه‌روزی فعالیت کند و از اختیارات فنی و حقوقی لازم برای تنظیم و اجرای درخواست‌های معاضدت متقابل فوری و هماهنگی مستقیم با سازمان‌های بین‌المللی مانند اینترپل و شبکه‌های جهانی مبارزه با جرائم سایبری برخوردار باشد. وجود نهادی مرکزی که نخبگانی از مشاوران حقوقی، کارشناسان تحقیقات دیجیتال و نمایندگان دیپلماسی امنیتی را گرد هم آورد، تدوین پاسخی فوری و قاطع را در برابر حملاتی که امنیت ملی را هدف می‌گیرند یا اخاذی بین‌المللی تضمین خواهد کرد و با رفع موانع صلاحیت قضایی و تعارض قوانین با سایر کشورها با کارایی و سرعتی بسیار بالا، از حاکمیت دیجیتال دولت حمایت خواهد نمود. اعمال احکام قانون ۱۷۵ مصوب ۲۰۱۸ بر محتوای دیجیتالیِ منتشرشده از طریق سکوهای بین‌المللی، مسئلهٔ ظریفی را مطرح کرده است: میزان الزام‌آور بودن این قانون برای شرکت‌های خارجی‌ای که در مصر حضور حقوقی ندارند. مقامات مصری در برخی موارد بر اساس سیاست‌های داخلی این شرکت‌ها مستقیماً با آن‌ها ارتباط برقرار کرده‌اند، بی‌آنکه سازوکار قانونیِ الزام‌آور و مدونی برای وادارکردن آن‌ها به تسلیم داده‌ها یا ادلهٔ دیجیتال درخواستی وجود داشته باشد.

بند سوم: وضعیت صلاحیت در عراق و نیاز به همکاری بین‌المللی

عراق در زمینهٔ صلاحیت قضایی با چالشی دوگانه روبه‌روست: از یک سو فاقد قانون ملی تخصصی است که قواعد این صلاحیت را در جرائم سایبری مشخص کند و از سوی دیگر، تنها شمار محدودی موافقت‌نامهٔ همکاری بین‌المللی در این زمینه منعقد کرده است. حقوق عراق در حال حاضر به مادهٔ پنجم قانون مجازات شمارهٔ ۱۱۱ مصوب ۱۹۶۹ استناد می‌کند که اصل صلاحیت سرزمینی را تثبیت می‌کند و در عین حال تعقیب کیفری جرائم ارتکابی در خارج از مرزها را، در صورتی که به منافع عالی عراق لطمه زند یا شهروندان عراقی در خارج را هدف قرار دهد، مجاز می‌شمارد.

پیچیدگی این وضعیت را مجموعه‌ای از عوامل ساختاری تشدید می‌کند که در صدر آن‌ها محدودیت توانمندی‌های فنی دستگاه‌های امنیتی و تحقیقاتی، ضعف پیوستگی عراق به نظام بین‌المللی همکاری در زمینهٔ مبارزه با جرائم سایبری و اثر سال‌ها گسست امنیتیِ کشور بر ظرفیت‌سازی نهادی قرار دارد. عراق تاکنون نهاد ملی تخصصی در حوزهٔ امنیت سایبری ندارد که در سطح مأموریت لازم برای مقابله با جرائم سایبری فرامرزی و هماهنگی با همتایان بین‌المللی خود باشد. عراق تاکنون کنوانسیون بوداپست دربارهٔ جرائم رایانه‌ای را تصویب نکرده است و مشارکت و تعامل آن در چارچوب‌ها و موافقت‌نامه‌های منطقه‌ای عربی و بین‌المللیِ مرتبط با امنیت سایبری نیز بسیار کم‌رنگ و محدود به نظر می‌رسد و به هیچ روی با حجم و عمق چالش‌های دیجیتال و تهدیدهای امنیتیِ فزاینده‌ای که زیرساخت و نهادهای حاکمیتی آن را هدف گرفته‌اند، تناسب ندارد. بر پایهٔ این خلأ بین‌المللی، دکترین حقوقی معاصر عراق بر این باور است که الحاق رسمی و قطعی به این کنوانسیون جهانی یا دست‌کم تدوین و پذیرش نظام تقنینی ملی‌ای که معیارهای فنی آن را دقیقاً شبیه‌سازی کند ستون اصلی و نقطهٔ عزیمت ناگزیرِ هرگونه اصلاح جدی در حقوق کیفری دیجیتال با هدف حمایت از فضای مجازی کشور است (الحصاوی، ۲۰۱۹، ۲۴۵).

علت اساسی این دیدگاه آن است که جرائم سایبری، به اقتضای ماهیت فرامرزی خود، با ابزارهای حقوقی محلی و منزوی قابل مقابله نیستند زیرا کنوانسیون بوداپست سازوکاری بی‌نظیر برای همکاری امنیتی و قضایی در زمان واقعی در اختیار کشورهای عضو قرار می‌دهد که امکان تبادل فوری اطلاعات و ادلهٔ دیجیتال حیاتی و حفظ فوری داده‌های ذخیره‌شده بر سرورهای بین‌المللی را پیش از پاک‌شدن آن‌ها به دست گروه‌های تروریستی یا شبکه‌های سازمان‌یافتهٔ اخاذی فراهم می‌سازد. این مشارکت بین‌المللی، رفع موانع صلاحیت قضایی و تعارض قوانین را برای دادگاه‌های عراق تضمین می‌کند و به مراجع تحقیق ملی توان ردیابی و تعقیب مرتکبان در آن سوی دریاها را می‌بخشد؛ امری که کارایی عدالت کیفری را ارتقا می‌دهد و امنیت ملی را در عصر جنگ‌های دیجیتال مستحکم می‌سازد (أبو خطوة، ۱۹۹۹، ۸۸).

در غیاب چارچوب تقنینی تخصصی و با محدودیت موافقت‌نامه‌های دوجانبه، بازپرسان عراقی در پرونده‌های جرائم سایبری بین‌المللی ناگزیرند از مسیرهای غیررسمی و از طریق مجاری همکاری نامنظم با همتایان خود در کشورهای دیگر ارتباط برقرار کنند. این امر غالباً به از دست رفتن ادلهٔ دیجیتال به سبب گذشت زمان و کهنگی داده‌ها یا حذف آن‌ها از سرورها، پیش از رسیدن درخواست‌های رسمی نیابت قضایی به مقصد، منجر می‌شود؛ و این واقعیت نمونهٔ زنده‌ای از چیزی است که دکترین کیفری بین‌المللی آن را بی‌کیفرمانی دیجیتال می‌نامد.

مقایسهٔ مواضع مصر و عراق، تفاوت آشکاری را در میزان آمادگی حقوقی برای مقابله با معضلات صلاحیت قضایی نشان می‌دهد: مصر از متون تقنینی پیشرفته‌تری برخوردار است و در شماری از سازوکارهای همکاری بین‌المللی مشارکت دارد، در حالی که عراق در سایهٔ خلأ تقنینی و نهادی‌ای به سر می‌برد که توانایی آن را در مقابله با جرائم سایبری فرامرزی محدود می‌سازد. شاید برجسته‌ترین وجه مشترک دو تجربه، نیاز مبرم به پیوستن به چارچوب‌های بین‌المللی همکاری در مبارزه با جرائم سایبری، تدوین موافقت‌نامه‌های دوجانبه و چندجانبه با شرکای منطقه‌ای و بین‌المللی، ظرفیت‌سازی فنی و انسانیِ تخصصی در دستگاه‌های قضایی و امنیتی و استقرار سازوکارهای پیشرفته برای تبادل آنی و ایمن داده‌ها و ادلهٔ دیجیتال باشد (ثروت، ۱۹۸۹، ۱۵۶).

جرائم سایبری فرامرزی چالشی افزون برای حمایت کیفری در عراق ایجاد می‌کنند زیرا مرتکبان ممکن است از سرورها یا سکوهایی خارج از کشور استفاده کنند و این امر اقدامات ردیابی و دستیابی به داده‌ها را پیچیده می‌سازد و نیاز به همکاری قضایی و فنی بین‌المللی را افزایش می‌دهد. وضعیت مقررات، چنان‌که در رساله آمده است، نشان می‌دهد که عراق کنوانسیون بوداپست دربارهٔ جرائم رایانه‌ای را تصویب نکرده است و محدودیت موافقت‌نامه‌ها و سازوکارهای تبادل فوری اطلاعات و ادلهٔ دیجیتال، توانایی مراجع تحقیق را در تعقیب مرتکبانی که در بیش از یک کشور فعالیت می‌کنند، کاهش می‌دهد. این دشواری با استفاده از فناوری‌های رمزنگاری و گمنام‌سازی و جابه‌جایی داده‌ها میان سرورهای متعدد افزایش می‌یابد امری که تقویت مجاری معاضدت حقوقی متقابل، توسعهٔ توانمندی‌های فنی واحدهای تخصصی و یکسان‌سازی رویه‌های حفظ و انتقال ادلهٔ دیجیتال را به عناصری ضروری برای ارتقای کارایی حمایت کیفری در برابر جرائم سایبری فرامرزی بدل می‌کند (الفریجات، ۲۰۱۸، ۸۹). تحلیل به این نتیجه می‌رسد که ایجاد صلاحیتی کارآمد در عراق نیازمند وضوح بیشتر در تعیین موارد گسترش صلاحیت به خارج از قلمرو و پیوند آن‌ها با ضوابطی عینی مانند تابعیت مرتکب یا بزه‌دیده، محل تحقق ضرر و منفعت اساسیِ مورد حمایت است. همچنین تکمیل این بنا مستلزم سازوکارهای عملی برای همکاری قضایی و تبادل ادلهٔ دیجیتال است زیرا متن قانون ملی، هر اندازه هم گسترده باشد، به‌تنهایی نمی‌تواند از مرزهای فنی عبور کند. ایجاد توازن میان سرعت دستیابی به دلیل و احترام به صلاحیت‌های حاکمیتی و حقوق شکلی افراد همچنان ضروری است تا مبارزه با جرائم فرامرزی به توجیهی برای نادیده‌گرفتن تضمینات تبدیل نشود.

گفتار سوم: توسعهٔ سازوکارهای مقابله و تحقیقات دیجیتال

توسعهٔ سازوکارهای مقابله تنها به معنای افزایش متون کیفری نیست، بلکه مستلزم ساختاری نهادی است که توان اجرای آن‌ها را داشته باشد. رساله نشان می‌دهد که سرعت تغییر شیوه‌های مرتکبان و اتکای آنان به ابزارهای پیشرفتهٔ رمزنگاری و پنهان‌سازی، دستگاه‌های اجرای قانون را ناگزیر می‌سازد که از تحقیقات سنتی به تحقیقات دیجیتال تخصصی گذار کنند. این ساختار بر واحدهای فنی تخصصی، آموزش مستمر، همکاری میان پلیس، دادسرا، دستگاه قضایی و کارشناسان و بهره‌گیری منضبط از ابزارهای تحلیل دیجیتال استوار است و باید با تضمیناتی همراه باشد که از گسترش ناموجه نظارت یا تعرض به حریم خصوصی کاربران جلوگیری کند.

بند اول: واحدهای تخصصی و ظرفیت‌سازی نهادی

در سال‌های اخیر، عراق و مصر دریافته‌اند که مبارزه با جرائم سایبری نیازمند نیروهای امنیتی و قضاییِ متخصص در این جرائم با مهارت‌های فنی و حقوقی بالاست از این رو، واحدهای تخصصی به شرح زیر ایجاد شده است: نخست، در عراق، ادارهٔ

کل مبارزه با جرائم رایانه‌ای وابسته به وزارت کشور تأسیس شد که دریافت گزارش‌ها، گردآوری ادلهٔ دیجیتال و تحقیق در جرائم سایبری با همکاری دادسرا را بر عهده دارد و شماری از قضات و اعضای دادسرا نیز برای تحقیق در این جرائم آموزش دیده‌اند. همچنین واحدهای فنی‌ای در شورای عالی قضایی برای کمک به دستگاه قضایی در فهم ادلهٔ دیجیتال ایجاد شده است (یونس، ۲۰۰۴، ۲۶۷). دوم، در مصر، قانون شمارهٔ ۱۷۵ مصوب ۲۰۱۸ واحد مبارزه با جرائم فناوری اطلاعات را در وزارت کشور ایجاد کرد. این واحد با همکاری دادسرای تخصصی جرائم سایبری فعالیت می‌کند و آزمایشگاه‌های دیجیتال مرکزی نیز برای تحلیل ادلهٔ الکترونیکی و استخراج آن‌ها از دستگاه‌های توقیف‌شده به منظور مبارزه با جرائم فناوری اطلاعات تأسیس شده است.

موفقیت این واحدها تا حد زیادی به همکاری بین‌المللی وابسته است زیرا ادلهٔ دیجیتال ممکن است بر سرورهایی در کشورهای دیگر نگهداری شوند و دستیابی به آن‌ها مستلزم مجاری حقوقی و فنی سریعی است که سلامت آن‌ها و قابلیت استناد به آن‌ها را در دادگاه حفظ کند. عراق و مصر موافقت‌نامه‌های دوجانبه و چندجانبه‌ای در زمینهٔ همکاری کیفری منعقد کرده‌اند و کنوانسیون بوداپست دربارهٔ جرائم رایانه‌ای الگویی هنجاری و مهم در تنظیم حفظ فوری داده‌ها و تبادل آن‌ها به شمار می‌رود. از این رو، ارتقای کارایی واحدهای تخصصی مستلزم تقویت مسیرهای معاضدت حقوقی متقابل، تعیین نقاط تماس روشن میان مقامات صالح و یکسان‌سازی رویه‌های فنی لازم برای انتقال ادلهٔ دیجیتال از کشوری به کشور دیگر، بدون خدشه به تضمینات حریم خصوصی و حقوق دفاع، است.

قانون‌گذار مصری به تدوین مواد جرم‌انگاری و مجازات بسنده نکرد، بلکه دریافت که اجرای مؤثر قانون مستلزم نظامی نظارتی و شکلیِ یکپارچه است که ابزارهای پایش فنی را در اختیار داشته باشد. از همین رو، قانون شمارهٔ ۱۷۵ مصوب ۲۰۱۸ نقشی محوری و اختیاراتی گسترده برای نظارت فنی جامع بر فضای دیجیتال مصر و هماهنگی مستقیم با ضابطان دادگستری (مانند ادارهٔ مبارزه با جرائم رایانه‌ای وزارت کشور) و دادسرا به سازمان ملی تنظیم مقررات ارتباطات اعطا کرد. این نظام از لحاظ نظری به تسهیل ردیابی حملات سایبری، تسهیل دستیابی به ادلهٔ دیجیتال از منابع آن‌ها (مانند ارائه‌دهندگان خدمات اینترنتی) و تأمین حفظ آن‌ها بر اساس پروتکل‌های فنی‌ای که از آلودگی‌شان جلوگیری می‌کند، کمک می‌کند. قانون همچنین شرکت‌های ارتباطاتی را به رعایت پروتکل‌های سخت‌گیرانهٔ نگهداری دیجیتال (ذخیرهٔ داده‌های ترافیک و هویت کاربران دست‌کم به مدت ۱۸۰ روز) ملزم کرد تا در صورت درخواست و بر اساس دستورهای قضایی مستدل در اختیار مراجع تحقیق قرار گیرد.

با این همه، واقعیت عملی و اجرای واقعی در سال‌های گذشته از وجود شکاف‌ها و خلأهای شکلی و هماهنگی آشکار پرده برداشت به‌ویژه در سرعت واکنش میدانی و زمانی میان مهندسان سازمان ملی و اعضای دادسرا. دلیل دیجیتال نیازمند سرعت بسیار بالا در ضبط و تحقیق است که گاه با چرخهٔ اسنادی و بوروکراسی اداری در صدور مجوزهای قضایی پیشین تعارض پیدا می‌کند و به مرتکبان فرصت پاک‌کردن آثارشان را می‌دهد. افزون بر این، مانع ناهمگونی فنی و ضعف امکانات مادی و فنی برخی از واحدهای فرعیِ مبارزه با جرائم اینترنتی در استان‌ها در مقایسه با جهش فناورانهٔ شتابان رخ نمود زیرا این واحدها گاه فاقد نرم‌افزارهای نوین رمزگشایی پیچیده یا ابزارهای بازیابی داده‌های حذف‌شده از فضاهای ذخیره‌سازی ابری‌اند و افزون بر آن، با کمبود عددی نیروی انسانیِ واجد صلاحیت برای همگامی با روش‌های پیچیدهٔ رخنه‌گران مواجه‌اند. این فاصله میان متن تقنینیِ بلندپروازانه و واقعیت عملی موجب شده است که برخی از ادلهٔ دیجیتال به سبب خطاهای شکلی در بررسی یا انتقال، در معرض ایراد بطلان در دادگاه‌ها قرار گیرند (قانون أصول المحاکمات الجزائیة العراقی، ۱۹۷۱).

در برابر خلأهای عملی و شدت‌گرفتن تهدیدهای سایبری پیچیده، دکترین کیفری نوین مصر به طرح دیدگاهی راهبردی گرایش یافته است که از راه‌حل‌های سنتی فراتر می‌رود چنان‌که حقوق‌دانان معتقدند ایجاد واحد ملیِ تخصصی و مستقل برای هماهنگی در پرونده‌های جرائم سایبری فرامرزی به ضرورتی تقنینی و شکلی و فوری بدل شده است که تأخیر یا تعلل اداری را برنمی‌تابد.

علت این دیدگاه آن است که پراکندگی صلاحیت‌های کنونی و توزیع اختیارات میان بخش‌های متعدد (مانند ادارهٔ مبارزه با جرائم رایانه‌ای وزارت کشور، دادسرا، سازمان ملی تنظیم مقررات ارتباطات و سازمان اطلاعات عمومی) نوعی تعارض اداری و کندی شکلی پدید می‌آورد که به هیچ وجه با ماهیت آنیِ جرم دیجیتال سازگار نیست زیرا ادلهٔ مجازیِ ذخیره‌شده بر سرورهای

خارجی ممکن است ظرف چند ثانیه پاک یا رمزگذاری شوند، در حالی که مراجع داخلی در انتظار طی تشریفات اداری روزمره و مکاتبه با مراجع خارجی از طریق مجاری دیپلماتیک سنتی‌اند. بر این اساس، دیدگاه حقوق‌دانان در این قالب شکل می‌گیرد که این واحد پیشنهادی به‌عنوان مرکز ارتباطی حاکمیتیِ واحد به‌صورت شبانه‌روزی فعالیت کند و از اختیارات کامل فنی، حقوقی و دیپلماتیک برای تنظیم و اجرای درخواست‌های معاضدت متقابل فوری و هماهنگی مستقیم و لحظه‌ای با سازمان‌های بین‌المللی مانند اینترپل و شبکه های جهانی مبارزه با جرائم سایبری برخوردار باشد. گردآوردن نخبگانی از مشاوران حقوقی، کارشناسان تحقیقات دیجیتال و نمایندگان دیپلماسی امنیتی زیر سقف نهادی مرکزی و واحد، تدوین پاسخی فوری و قاطع را در برابر حملاتی که امنیت ملی را هدف می‌گیرند یا عملیات اخاذی بین‌المللی تضمین می‌کند و با رفع موانع صلاحیت قضایی و تعارض قوانین با کارایی و سرعتی بسیار بالا، از حاکمیت دیجیتال دولت صیانت می‌نماید.

بند دوم: به‌کارگیری فناوری‌های نوین در تحقیقات کیفری

جرم‌یابی دیجیتال به معنای به‌کارگیری ابزارها و فنون علمی برای گردآوری ادلهٔ دیجیتال از رایانه‌ها، تلفن‌های هوشمند و شبکه‌ها، همراه با حفظ سلامت آن‌ها و قابلیتشان برای استفاده در دادگاه است. واحدهای تخصصی در هر دو کشور به نرم‌افزارها و سخت‌افزارهای پیشرفته‌ای برای تهیهٔ نسخه‌های مطابق با اصل از ادلهٔ دیجیتال و تحلیل آن‌ها مجهز شده‌اند (الوقاد، ۱۹۹۹، ۶۷). در برخی از جرائم سایبری که شهود یا کارشناسان در کشورهای دیگر حضور دارند یا متهم در مکانی دوردست است، استفاده از فناوری‌های ارتباط تصویری برای انجام تحقیقات امکان‌پذیر شده است امری که روند رسیدگی را تسریع می‌کند و از هزینه‌ها می‌کاهد، مشروط بر آنکه تضمینات لازم برای حقوق دفاع فراهم باشد. برخی از دادسراهای تخصصی در مصر و عراق استفاده از سامانه‌های هوش مصنوعی را برای کمک به تحلیل حجم عظیمی از داده‌ها، کشف الگوهای مجرمانه، شناسایی هویت مرتکبان جرائم سایبری و پیش‌بینی حملات آینده آغاز کرده‌اند. هرچند این استفاده هنوز در مراحل ابتدایی است، آیندهٔ تحقیقات کیفری را نمایندگی می‌کند.

دلیل دیجیتال محور اصلی تحول در قانون آیین دادرسی کیفری مصر به شمار می‌رود زیرا از مجموعه‌ای از ویژگی‌های فنی و مجازی برخوردار است که نظریه‌های کلاسیک اثبات را با بن‌بستی واقعی روبه‌رو ساخته است. در حالی که دلیل سنتی بر موجودیتی مادی و پایدار استوار است که می‌توان آن را توقیف و با موم سرخ مهروموم کرد، دلیل دیجیتال در جوهر خود عبارت است از پالس‌های الکترونیکی و داده‌های رمزگذاری‌شده‌ای که بر رسانه‌ها یا سرورهای ابری ذخیره شده‌اند (قرنی، ۲۰۰۶، ۸۷).

این ماهیت مجازی سبب می‌شود که دلیل دیجیتال از شکنندگی شدید برخوردار باشد زیرا می‌توان آن را پاک کرد، محتوایش را تغییر داد یا داده‌هایش را به‌آسانی و به دست اشخاصی با مهارت‌های فنی ساده نسخه‌برداری کرد، بی‌آنکه این تغییر هیچ اثر مادی آشکاری بر جای گذارد که با چشم غیرمسلح یا ابزارهای سنتی معاینه قابل درک باشد. افزون بر این، دلیل دیجیتال از قابلیت منحصربه‌فرد انتشار آنی و جابه‌جایی میان قاره‌ها در کسری از ثانیه برخوردار است؛ امری که معضل داده‌های فرّار را پدید می‌آورد که به‌محض خاموش‌شدن دستگاه یا قطع جریان برق از میان می‌روند.

این پیچیدگی‌های فنی، قانون‌گذار مصری را در قانون ۱۷۵ مصوب ۲۰۱۸ ناگزیر ساخت ضوابط و معیارهای شکلی دقیقی وضع کند و مفهوم تحقیقات کیفری دیجیتال را پدید آورد. به موجب قواعد جدید، گردآوری دلیل دیجیتال به روش‌های تصادفی دیگر پذیرفتنی نیست، بلکه این مقررات احراز معیارهای تجمعی‌ای را لازم دانسته است که با معیار اصالت از طریق راستی‌آزمایی سلامت فایل‌ها و عدم دستکاری در آن‌ها آغاز می‌شود و با معیار سلامت ادامه می‌یابد که مستندسازی زنجیرهٔ نگهداری را از زمان ضبط فنی تا ارائهٔ دلیل به دادگاه ایجاب می‌کند به نحوی که ارزش اثباتی دلیل حفظ شود و از اعتراض به سلامت اقدامات مربوط به آن کاسته شود. ارزش فناوری در تحقیقات هنگامی آشکار می‌شود که به‌عنوان ابزاری برای کشف و مستندسازی به کار رود، نه جایگزینی برای قواعد حقوقی. تحلیل جرم‌یابانهٔ دیجیتال به بازیابی فایل‌های حذف‌شده، ردیابی سوابق ورود و پیوند زمان‌ها و نشانی‌های دیجیتال با دستگاه‌ها و حساب‌ها کمک می‌کند و ابزارهای تحلیل کلان‌داده نیز به کشف الگوهای تکرارشونده و روابط میان وقایع یاری می‌رسانند. با این حال، کارآمدی این ابزارها به سلامت اقدامات دستیابی به آن‌ها و مستندسازی‌شان و نیز به

توانایی کارشناس در تبیین نتایج آن‌ها به زبانی قابل فهم برای دستگاه قضایی وابسته است. از این رو، سرمایه‌گذاری در تجهیزات بدون معیارهای فنی یکسان و برنامه‌های آموزش و تأیید صلاحیت کارشناسان به هدف خود نمی‌رسد.

بند سوم: چارچوبی یکپارچه برای حمایت کیفری و پشتیبانی از بزه‌دیدگان

گسترش فناوری‌های دیجیتال در عراق عاملی اصلی در افزایش جرائم سایبری است جرائمی که کلاهبرداری مالی، اخاذی، سرقت هویت دیجیتال، افترا از طریق شبکه‌های اجتماعی و تعرض به حساب‌ها و داده‌ها را دربر می‌گیرد. این تنوع به زیان‌های روانی، مادی و اجتماعی‌ای می‌انجامد که ممکن است برای گروه‌های آسیب‌پذیر سنگین‌تر باشد در حالی که چارچوب حقوقی عراق در بخش مهمی از مقابله، بر مواد عام قانون مجازات و قوانین پراکنده‌ای تکیه دارد که در اصل برای دربرگرفتن همهٔ صور جرم دیجیتال وضع نشده‌اند. رساله نشان می‌دهد که ایجاد واحدهای تخصصی و مرکز امنیت سایبری گامی نهادی و مهم است؛ اما تحول سریع شیوه‌های رمزنگاری، جعل عمیق و گمنام‌سازی، نوسازی مستمر توانمندی‌های فنی و قواعد شکلی را ایجاب می‌کند تا شکاف میان متن قانون و اجرا گسترده‌تر نشود (س. ع. حسن، ۱۹۹۹، ۳۹).

از دیگر چالش‌های برجسته، تأثیر جرائم سایبری بر گروه‌های اجتماعی آسیب‌پذیر است چرا که زنان ممکن است در معرض صوری از اخاذی مبتنی بر تهدید به انتشار تصاویر یا داده‌های خصوصی قرار گیرند و کودکان نیز ممکن است مورد بهره‌کشی و آزار قرار گیرند یا به تولید محتوای نامشروع واداشته شوند. این صور، آثار روانی و اجتماعی‌ای را آشکار می‌سازند که از زیان مادی مستقیم فراتر می‌رود و نیاز به سازوکارهای محرمانه و ایمن برای گزارش‌دهی و نیز خدمات حمایت روانی، اجتماعی و حقوقی را برجسته می‌کنند که حریم خصوصی بزه‌دیده را رعایت کنند و از داغ ننگِ مرتبط با برخی جرائم بکاهند. این امر اقتضا می‌کند که حمایت کیفری بخشی از نظامی گسترده‌تر باشد که بازدارندگی حقوقی، پیشگیری دیجیتال، حمایت از داده‌ها و تسهیل دسترسی به عدالت را با هم جمع کند. افزون بر این، نظام حقوقی با چالش همگامی با تحولات سریع فناوری روبه‌روست چرا که فناوری‌هایی مانند دیپ‌فیک (جعل عمیق) در جرائم اجتماعی به کار می‌روند و ثبات اجتماعی و امنیتی عراق را تهدید می‌کنند. این امر به افزایش جرائمی مانند ترویج مواد مخدر یا آدم‌ربایی از طریق اینترنت انجامیده و وزارت برنامه‌ریزی نیز از سهم بزرگی از جرائم ارتکابی از طریق شبکه‌های اجتماعی پرده برداشته است. حمایت کیفری از کمبود آموزش قضات و بازپرسان رنج می‌برد، زیرا برنامه‌های مستمری برای مواجهه با ادلهٔ دیجیتال وجود ندارد و این امر به صدور احکام ناعادلانه یا آزادی مرتکبان می‌انجامد. برای نمونه، در پرونده‌های شنود الکترونیکی، تعیین مسئولیت به سبب استفاده از رسانه‌های دیجیتال ناشناس دشوار است. این چالش‌ها مستلزم اصلاحات تقنینی فوری است؛ مانند تصویب قانونی که جرائم دیجیتال نوظهور را جرم‌انگاری کند و همکاری با کشورهای همسایه را تقویت نماید.

فضای دیجیتال در عراق بستری گسترده برای ظهور صور متعددی از جرائم سایبری مانند کلاهبرداری مالی، اخاذی، سرقت هویت و افترا از طریق سکوهای شبکه‌های اجتماعی است جرائمی که ممکن است زیان‌های روانی و مادی شدیدی به بزه‌دیدگان وارد کنند. چارچوب حقوقی موجود بر متون عام و پراکنده‌ای تکیه دارد که صور نوینی مانند جعل عمیق و تعرض‌های پیچیده به داده‌ها را به نحو یکپارچه پوشش نمی‌دهند. ایجاد واحدهای تخصصی و مرکز امنیت سایبری به بهبود پایش و تحقیق کمک کرده است اما فقدان سازوکارهای یکپارچهٔ حمایت از بزه‌دیدگان، از جمله رویه‌های گزارش‌دهی ایمن و پشتیبانی روانی و اجتماعی، همچنان از نقاط ضعفی است که چاره‌جویی تقنینی و نهادیِ هماهنگ را می‌طلبد.

از جمله چالش‌های اجتماعی آن است که بزه‌دیدگان، به‌ویژه زنان و کودکان، از داغ ننگ اجتماعی‌ای رنج می‌برند که مانع گزارش جرائم از سوی آنان می‌شود، به‌خصوص در موارد اخاذی جنسی امری که نیاز به مراکز تخصصی حمایت روانی و اجتماعی را نشان می‌دهد. در حال حاضر دولت عراق چنین مراکزی را فراهم نمی‌کند و این امر بزه‌دیدگان را بدون پشتیبانی کافی رها می‌سازد. بهره‌کشی از کودکان از طریق اینترنت، مانند آزار یا واداشتن آنان به تولید محتوای غیرقانونی، مشکل را تشدید می‌کند زیرا با وجود افزایش ۲۷ درصدی این جرائم در سال ۲۰۲۴، برنامه‌های حمایتی ویژهٔ کودکان وجود ندارد. این شکاف‌ها توسعهٔ سازوکارهای حمایت اجتماعی متمرکز بر گروه‌های آسیب‌پذیر را ایجاب می‌کند (سالم، ۲۰۱۳، ۲۰۵).

کارزارهای آگاه‌سازی یکی از سازوکارهای مهم حمایت پیشگیرانه‌اند زیرا به کاربران کمک می‌کنند خطرات اشتراک‌گذاری داده‌های شخصی و شیوه‌های کلاهبرداری، اخاذی و مهندسی اجتماعی را درک کنند. رساله نشان می‌دهد که اثر این کارزارها همچنان متفاوت است، به‌ویژه در محیط‌هایی که آگاهی دیجیتال یا دسترسی به برنامه‌های آموزشی منظم در آن‌ها اندک است. از این رو، تقویت پیشگیری مستلزم گنجاندن مفاهیم ایمنی دیجیتال در مدارس و دانشگاه‌ها و مشارکت‌دادن نهادهای عمومی و رسانه‌ها در ارائهٔ پیام‌های کاربردی دربارهٔ حفاظت از حساب‌ها، راستی‌آزمایی محتوا و مقابله با صور جعل عمیق است؛ به‌گونه‌ای که آگاهی جمعی مکمل حمایت تقنینی و شکلی شود.

از منظر حقوقی، توسعهٔ قوانین تخصصی ضرورتی مبرم برای تقویت حمایت از بزه‌دیدگان است. قواعد جدید باید تعاریف روشنی از جرائم نوظهور ارائه دهند، رویه‌های دقیقی برای حفظ، بررسی و ارائهٔ ادلهٔ دیجیتال وضع کنند و هنگامی که جرم گروه‌های آسیب‌پذیر را هدف می‌گیرد یا زیان‌های شدیدی به بار می‌آورد، حمایت را تشدید نمایند. همچنین ساختن نظام حمایتی مستلزم پذیرش پروتکل‌های استاندارد برای حفظ داده‌ها و زنجیرهٔ نگهداری و بررسی امکان ایجاد سازوکارهای نهادی برای پشتیبانی از بزه‌دیدگان و جبران خسارت آنان بر اساس ضوابط قانونی روشن است؛ به نحوی که گزارش‌دهی را تشویق کند و از آثار روانی و مادی جرم بکاهد (أحمد، ۲۰۰۵، ۱۷۸).

اقدامات اجرایی، مانند ایجاد مرکز امنیت سایبری و واحدهای تخصصی، به بهبود هماهنگی میان نهادهای دولتی کمک می‌کند اما کمبود نیروی انسانی و آموزش فنی ممکن است کارایی مواجهه با ادلهٔ دیجیتال را محدود سازد. رفع این کاستی مستلزم برنامه‌های آموزشی مستمر برای پلیس، قضات، اعضای دادسرا و کارشناسان، در کنار سرمایه‌گذاری در آزمایشگاه‌ها و تجهیزات لازم برای بررسی و تحلیل است. یافته‌های رساله تأکید می‌کند که عراق کنوانسیون بوداپست دربارهٔ جرائم رایانه‌ای را تصویب نکرده است و این امر بر اهمیت توسعهٔ مجاری همکاری بین‌المللی و معاضدت حقوقی متقابل و بهره‌گیری از معیارهای فنی‌ای که این کنوانسیون در حفظ داده‌ها و تبادل ادله بنا نهاده است، می‌افزاید. ایجاد خدمات حمایت روانی، اجتماعی و حقوقی برای بزه‌دیدگان نیز مکمل این اقدامات است؛ به نحوی که از داغ ننگ بکاهد و اعتماد به سازوکارهای گزارش‌دهی و تعقیب را تقویت کند. ضعف زیرساخت دیجیتال در عراق لایهٔ دیگری بر چالش‌ها می‌افزاید زیرا بی‌ثباتی فنی و ضعف تدابیر حفاظتی ممکن است فرصت‌های نفوذ و تعرض به سامانه‌ها و داده‌ها را افزایش دهد. افزون بر این، گسترش استفاده از فناوری‌های هوش مصنوعی و جعل عمیق، دشواری راستی‌آزمایی محتوای دیجیتال را دوچندان می‌کند و وظیفهٔ اثبات در دادگاه را پیچیده‌تر می‌سازد. مواجهه با این خطرات مستلزم سرمایه‌گذاری مستمر در امنیت سایبری، توسعهٔ توانمندی‌های بررسی فنی و پیوند نوسازی زیرساخت فنی با قواعد حقوقی و شکلی روشن است تا شکاف‌های فناورانه به عاملی برای تضعیف کارآمدی تعقیب کیفری یا اعتماد افراد و نهادها به محیط دیجیتال بدل نشوند.

از جنبهٔ اجتماعی، کمبود آگاهی دیجیتال چالش‌ها را تشدید می‌کند زیرا بسیاری از افراد، به‌ویژه در مناطق روستایی، از خطرات اشتراک‌گذاری داده‌های شخصی آگاهی ندارند و این امر آسیب‌پذیری آنان را در برابر کلاهبرداری یا اخاذی افزایش می‌دهد و نیاز به کارزارهای ملی آگاه‌سازی را برجسته می‌سازد. همچنین جرائم سایبری با افراط‌گرایی پیوند دارند چرا که گروه‌های افراطی از اینترنت برای انتشار تبلیغات استفاده می‌کنند و این امر امنیت ملی را تهدید می‌کند و حمایت کیفری را به سبب مرزهای دیجیتال پیچیده می‌سازد. در این زمینه، به نظر می‌رسد راه‌حل در یکپارچه‌سازی اقدامات اجرایی و تقنینی برای توسعهٔ توانمندی‌های تحقیق و فراهم‌آوردن حمایت از بزه‌دیدگان نهفته است چرا که چالش‌های دیجیتال معاصر در عراق مانعی بزرگ بر سر راه حمایت کیفری در برابر جرائم سایبری به شمار می‌آید. با وجود شکاف‌های حقوقی و فنی‌ای که اصلاحات فوری را ایجاب می‌کنند، می‌توان از طریق تصویب قوانین تخصصی، تقویت آموزش و گسترش همکاری بین‌المللی به حمایتی بهتر دست یافت که از توسعهٔ دیجیتال پایدار پشتیبانی کند (خ. حسن، ۲۰۱۹، ۳۰).

یکی از سازوکارهای اساسی حمایت، توانمندسازی بزه‌دیدگان برای طرح شکایت نزد واحدهای تخصصی مبارزه با جرائم سایبری است؛ اما کارآمدی این مسیر به سرعت واکنش، کیفیت حفظ ادله و وجود تخصص فنی نزد بازپرسان وابسته است. خطا در نسخه‌برداری یا مستندسازی داده‌ها یا تأخیر در بررسی ممکن است ارزش دلیل را کاهش دهد یا به از دست رفتن آن بینجامد

و این نیاز به پروتکل‌های یکسان از لحظهٔ دریافت گزارش تا ارجاع دلیل به آزمایشگاه و دادگاه را برجسته می‌سازد. توسعهٔ آزمایشگاه‌های دیجیتال پیشرفته و آموزش بازپرسان در زمینهٔ جدیدترین فنون تحلیل جرم‌یابانهٔ دیجیتال به کاهش این خطرات و بهبود فرصت دستیابی به نتیجهٔ قضایی قابل اتکا کمک می‌کند.

چالش‌های دیجیتال معاصر مانعی بزرگ بر سر راه حمایت از بزه‌دیدگان است زیرا برخی از مرتکبان از فناوری‌های رمزنگاری، شبکه‌های مجازی و ابزارهای پنهان‌سازی هویت استفاده می‌کنند و این امر ردیابی و گردآوری دلیل را دشوار می‌سازد. این دشواری در جرائم فرامرزی، هنگامی که داده‌ها یا سرورها یا طرفین در خارج از کشور قرار دارند، به‌ویژه با محدودیت مجاری همکاری فوری، افزایش می‌یابد. رساله تأکید می‌کند که عدم تصویب کنوانسیون بوداپست دربارهٔ جرائم رایانه‌ای از سوی عراق، در کنار نیاز به توسعهٔ قوانین و زیرساخت فنی، تقویت معاضدت حقوقی متقابل و مجاری تبادل اطلاعات را بر اساس تضمینات روشن ایجاب می‌کند. این مسیر می‌تواند از تعقیب مرتکبان پشتیبانی کند و از اتلاف ادله بکاهد و در عین حال مشروعیت شکلی، حریم خصوصی و حقوق دفاع را حفظ نماید.

مقایسه تأیید می‌کند که کارآمدترین الگو، الگویی است که قانون‌گذاری، آیین دادرسی، نهاد و فناوری را در نظامی واحد به هم پیوند دهد. متن کیفری رفتار ممنوع را تعیین می‌کند، قواعد اثبات نحوهٔ مواجهه با دلیل را تنظیم می‌کنند، صلاحیت مبنایی برای تعقیب در اختیار دستگاه قضایی می‌گذارد و واحدهای تخصصی توانایی عملی را فراهم می‌کنند در حالی که نظارت قضایی تضمین می‌کند ابزارهای دیجیتال به تعرضی نامتناسب به حقوق تبدیل نشوند. این یکپارچگی همچنین امکان می‌دهد بخشی از سیاست جنایی به پیشگیری، حمایت از بزه‌دیدگان و آموزش دیجیتال معطوف شود؛ امری که از حجم جرائم می‌کاهد و اعتماد به توانایی نظام عدالت در پاسخ به تحول فنی را افزایش می‌دهد (دفتر مقابله با مواد مخدر و جرم سازمان ملل متحد [UNODC]، ۲۰۱۹، ۸).

نتیجه‌گیری

پژوهش نشان می‌دهد که چالش شکلی در جرائم سایبری پیچیده‌تر از صرف افزودن وسیلهٔ اثباتی جدید به قواعد موجود است؛ زیرا ماهیت دلیل دیجیتال، محل وجود آن و شیوهٔ تولید و نگهداری‌اش، بازتنظیم زنجیره‌ای کامل از اقدامات تحقیق را ایجاب می‌کند. همچنین عبور سریع از مرزها سبب می‌شود صلاحیت قضایی به همان اندازه که به متن قانون داخلی وابسته است، به همکاری بین‌المللی نیز پیوند یابد. مقایسه روشن می‌سازد که وجود قواعد تخصصی‌تر در مصر مبنای روشن‌تری برای مواجهه با برخی جنبه‌های دلیل و صلاحیت فراهم می‌کند، در حالی که عراق به تقویت چارچوب شکلی تخصصی و یکسان‌سازی رویه‌های فنی نیاز دارد. یافته‌ها تأکید می‌کنند که فناوری جایگزین قانون نمی‌شود، بلکه نیاز به قواعدی را که اقدامات ضبط و تحلیل را مستند کنند و امکان مناقشه در دلیل را در دادگاه تضمین نمایند، افزایش می‌دهد. از این رو، کارآمدترین شیوهٔ مقابله آن است که واحدی تخصصی، کارشناسی واجد صلاحیت، قاضی‌ای توانا در ارزیابی دلیل، مجاری همکاری سریع و تضمیناتی را که حریم خصوصی و حقوق دفاع را در برابر هرگونه گسترش نامتناسب ابزارهای نظارت و تحقیق حفظ کند، با هم جمع کند.

۱. پژوهش ثابت می‌کند که دلیل دیجیتال از درجهٔ بالایی از قابلیت نسخه‌برداری، تغییر و حذف برخوردار است و همین امر سلامت اقدامات گردآوری، نگهداری و مستندسازی را به بخشی از ارزش خودِ دلیل بدل می‌کند. دادگاه تنها به شناخت محتوای داده‌ها نیاز ندارد، بلکه باید به منشأ آن‌ها، نحوهٔ دستیابی به آن‌ها و استمرار سلامتشان از زمان ضبط تا بررسی قضایی اطمینان یابد.

۲. روشن شد که رمزنگاری و فناوری‌های گمنام‌سازی دشواری تحقیق را افزایش می‌دهند؛ زیرا ممکن است مانع دسترسی به محتوا شوند یا پیوند میان فعالیت الکترونیکی و شخص انجام‌دهندهٔ آن را پنهان سازند. در نتیجه، توسعهٔ توانمندی‌های تحلیل جرم‌یابانهٔ دیجیتال و آموزش تخصصی دیگر موضوعی فرعی نیست، بلکه به عنصری اساسی در امکان دستیابی به دلیل به شکلی قابل اتکا در دادگاه بدل شده است.

۳. مقایسه نشان داد که به رسمیت شناختن حجیت سوابق و داده‌های الکترونیکی نیازمند قواعد شکلی مکملی است که نحوهٔ ضبط، نسخه‌برداری، توقیف و بررسی فنی را تبیین کنند. در وضعیت عراق، نیاز بیشتری به یکسان‌سازی معیارها و رویه‌ها

احساس می‌شود، در حالی که قانون تخصصی مصر چارچوب روشن‌تری برای برخی اقدامات فراهم می‌کند؛ هرچند نیاز به اجرای فنی و قضایی منضبط همچنان باقی است.

۴. جرائم فرامرزی ناکافی بودن اتکای صرف به معیار سرزمینی را آشکار می‌سازند زیرا رفتار، نتیجه، سرور و بزه‌دیده ممکن است هر یک در کشوری متفاوت باشند. از این رو، تدوین صلاحیت ملیِ گسترده کافی نیست، بلکه باید با ضوابطی همراه شود که از تعارض صلاحیت جلوگیری کنند و دستیابی به داده‌ها و ادلهٔ موجود در خارج از کشور را از طرق قانونی امکان‌پذیر سازند.

۵. پژوهش تأکید می‌کند که واحدهای تخصصی مبارزه با جرائم سایبری هنگامی کارایی واکنش را ارتقا می‌دهند که با دادسرا، دستگاه قضایی، کارشناسان و برنامه‌های آموزش مستمر پیوند داشته باشند. اثر ایجاد این واحدها در صورتی تضعیف می‌شود که به ابزارهای فنی، نیروی انسانی و معیارهای یکسان برای مواجهه با دستگاه‌ها و داده‌ها مجهز نشوند یا نتایج فنی آن‌ها از اقتضائات اثبات قضایی جدا بماند.

۶. تحلیل به این نتیجه می‌رسد که فناوری نوین در تحقیقات باید تحت نظارت حقوقی و قضایی روشن عمل کند؛ زیرا ابزارهای ردیابی، تحلیل و نظارت در صورت استفادهٔ بی‌ضابطه ممکن است به حریم خصوصی لطمه زنند. بنابراین، کارآمدی شکلی تنها با سرعت دستیابی به داده‌ها سنجیده نمی‌شود، بلکه با توانایی نظام در تحقق این امر همراه با رعایت مشروعیت، تناسب و حقوق دفاع سنجیده می‌شود.

پیشنهادات

۱. پیشنهاد می‌شود پروتکل‌های ملی یکسانی برای گردآوری، نسخه‌برداری، نگهداری و بررسی ادلهٔ دیجیتال تدوین شود به‌گونه‌ای که هر مرحله و هر شخصی که با دلیل سروکار داشته است، از زمان ضبط دستگاه یا حساب تا ارائهٔ نتیجه در دادگاه مستند شود. این مستندسازی به کاهش اختلافات دربارهٔ سلامت دلیل کمک می‌کند و مبنای روشن‌تری برای ارزیابی ارزش اثباتی آن در اختیار دستگاه قضایی می‌گذارد.

۲. شایسته است برنامه‌های آموزشی تخصصی و مستمری برای بازپرسان، اعضای دادسرا، قضات و کارشناسان در حوزهٔ تحقیقات دیجیتال ایجاد شود و محتوای آموزش متناسب با تغییر شیوه‌های ارتکاب جرم به‌روز گردد. آموزش باید جنبهٔ فنی و قواعد حقوقی را با هم جمع کند تا مهارت فنی به اقدامی نامشروع نینجامد و دانش حقوقی نیز به ناتوانی در فهم دلیل فنی منجر نشود.

۳. پیشنهاد می‌شود قواعد صلاحیت در جرائم سایبری فرامرزی به نحوی توسعه یابد که پیوند جرم با عراق یا مصر را به‌روشنی مشخص کند و سازوکارهایی برای حل موارد تعارض صلاحیت پیش‌بینی شود. این قواعد باید با مجاری عملی معاضدت قضایی، تبادل اطلاعات و حفظ فوری داده‌ها بر اساس رویه‌های قانونیِ قابل نظارت همراه باشد.

۴. شایسته است واحدهای تخصصی مبارزه با جرائم سایبری با نیروی انسانی، سخت‌افزار و نرم‌افزارهای لازم برای تحلیل جرم‌یابانهٔ دیجیتال پشتیبانی شوند و معیارهای کار میان نهادهای ذی‌صلاح یکسان گردد. همچنین بهتر است مسیرهای هماهنگی ثابتی میان پلیس، دادسرا، دادگاه‌ها و مراکز کارشناسی ایجاد شود تا از تکرار اقدامات یا از دست رفتن دلیل در جریان انتقال میان نهادها جلوگیری شود.

۵. پیشنهاد می‌شود معیارهایی برای تأیید صلاحیت کارشناسان و آزمایشگاه‌هایی که بررسی ادلهٔ دیجیتال را بر عهده دارند وضع شود و حداقل الزامات مستندسازی، آزمون مجدد و امکان بازبینی نتایج تعیین گردد. اعتبار ابزار فنی جایگزین اعتبار شیوهٔ به‌کارگیری آن نمی‌شود و فراهم‌آوردن امکان بازبینی بررسی‌ها به دادگاه و طرفین دعوا کمک می‌کند تا دلیل را منصفانه‌تر به بحث بگذارند.

۶. اختیارات دسترسی به داده‌ها، نظارت و ردیابی باید با تضمینات قضایی روشنی همراه باشد که ضرورت، تناسب، دامنه و مدت مجوز را رعایت کند. این ضوابط به ایجاد توازن میان سرعت تحقیق و حمایت از حریم خصوصی و حقوق دفاع کمک می‌کنند و مانع از آن می‌شوند که نیاز به مبارزه با جرائم سایبری به گسترش بی‌ضابطهٔ گردآوری داده‌ها بینجامد.

ملاحظات اخلاقی

مشارکت نویسندگان

نویسندگان به نحو مساوی در نگارش مقاله همکاری داشتند.

تعارض منافع

بر اساس اظهارات نویسندگان، این مقاله تعارض منافعی ندارد.

حامی مالی

بنابر اظهارات نویسندگان این پژوهش هیچگونه حامی مالی ندارد.

سپاسگزاری

از تمامی مشارکت کنندگان در این پژوهش سپاسگزاری می شود.

منابع

أبو خطوة، أحمد شوقی عمر. (۱۹۹۹). *شرح الأحکام العامة لقانون العقوبات، الجزء الأول: النظریة العامة للجریمة*.دار النهضة العربیة.

أحمد، إبراهیم سید. (۲۰۰۵). *الحمایة التشریعیة لبطاقات الدفع الإلکترونی*. الدار الجامعیة.

الحصاوی، مروی السید. (۲۰۱۹). *مبدأ العالمیة فی القانون الجنائی* [رسالة دکتری، دانشکدة حقوق، دانشگاه المنصورة]

الحلبی، خالد. (۲۰۰۰). *إجراءات التحری والتحقیق فی جرائم الحاسوب والإنترنت*. دار الثقافة للنشر والتوزیع.

الفریجات، خالد. (۲۰۱۸). *الجریمة المعلوماتیة وسبل مکافحتها فی التشریع الأردنی: دراسة مقارنة*.

الوقاد، عمر إبراهیم. (۱۹۹۹). *الحمایة الجنائیة للمعلوماتیة*. دار النهضة العربیة.

ثروت، جلال. (۱۹۸۹). *نظم القسم العام فی قانون العقوبات المصری*. منشأة المعارف.

حجازی، عبدالفتاح بیومی. (۲۰۰۹). *الجوانب الإجرائیة لأعمال التحقیق الابتدائی فی الجرائم المعلوماتیة: دراسة مقارنة* (چاپ اول).

حسن، خالد. ۲۰۱۹۹. *الدلیل الرقمی ودوره فی إثبات الجریمة المعلوماتیة*. دار الفکر الجامعی.

حسن، سعید عبداللطیف. (۱۹۹۹). *إثبات جرائم الکمبیوتر والجرائم المرتکبة عبر الإنترنت* (چاپ اول). دار النهضة العربیة.

حسن، محمد عبدالرحیم. ۲۰۱۹۹. *الجریمة الإلکترونیة وإشکالیات الاختصاص القضائی*. دار النهضة العربیة.

دفتر مقابله با مواد مخدر و جرم سازمان ملل متحد. (۲۰۱۹). *وحدة التعلیم الإلکترونی للجرائم الإلکترونیة، الوحدة الرابعة: مقدمة فی الجنایات الرقمیة*. سازمان ملل متحد.

unodc.org/e4j/en/cybercrime/module-4/index.html

سالم، عمر محمد. (۲۰۱۳). *مظاهر استخدام التکنولوجیا الحدیثة فی مجال القانون الجنائی: المراقبة الإلکترونیة والتحقیق الجنائی عن بعد*. دار النهضة العربیة.

سرور، أحمد فتحی. (۲۰۱۵). *الوسیط فی قانون العقوبات: القسم العام*. دار النهضة العربیة.

شورای اروپا. (۲۰۰۱۹). *کنوانسیون جرائم سایبری (کنوانسیون بوداپست)* (سری معاهدات اروپایی، شمارهٔ ۱۸۵)

rm.coe.int/1680081561

صالح، سلمی. (۲۰۲۳). جهود منظمات مکافحة الجریمة المعلوماتیة فی الأمن السیبرانی *مجلة دراسات فی الخدمة الاجتماعیة، (۶۳)*، بخش ۳، ۸۰۹–۸۵۲.

dss.journals.ekb.eg/article_310334_627fe721ea71f199bd8f846d6487cba8.pdf

صالح، نبیل. (۲۰۲۰). الإثبات الجنائی الرقمی فی التشریع المقارن *مجلة الحقوق (الکویت)، (۲)*.

عبدالرازق، سمیر. (۲۰۲۱). التحقیق فی الجرائم الإلکترونیة *مجلة الفکر القانونی، کلیة الحقوق، جامعة القاهرة*.

قانون الإثبات العراقی رقم ۱۰۷ لسنة (۱۹۷۹).

قانون أصول المحاکمات الجزائیة العراقی رقم ۲۳ لسنة ۱۹۷۱ وتعدیلاته. (۱۹۷۱).

قانون مکافحة جرائم تقنیة المعلومات رقم ۱۷۵ لسنة (۲۰۱۸). *الجریدة الرسمیة، العدد ۳۰ مکرر (أ)*، ۵ أغسطس ۲۰۱۸.

fra.gov.eg/wp-content/uploads/2025/01/%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%B1%D9%82%D9%85-175-%D9%84%D8%B3%D9%86%D8%A9-2018-%D8%A8%D8%AA%D8%A7%D8%B1%D9%8A%D8%AE-2018-08-14.pdf

قرنی، عادل یحیی. (۲۰۰۶). *التحقیق والمحاکمة الجنائیة عن بعد: دراسة تحلیلیة تأصیلیة* (چاپ اول). دار النهضة العربیة.

محمود، حسین. (۱۹۸۱). *الوسائل العلمیة الحدیثة فی الإثبات الجنائی*. دار النهضة العربیة.

یونس، عمر محمد أبو بکر. (۲۰۰۴). *الجرائم الناشئة عن استخدام الإنترنت: الأحکام الموضوعیة والجوانب الإجرائیة* [رسالهٔ دکتری، دانشگاه عین شمس]. دار النهضة العربیة.

References

Abdel-Razek, S. (2021). Investigation of cybercrimes. *Journal of Legal Thought, Faculty of Law, Cairo University*.

Abu Khatwa, A. S. O. (1999). *Explanation of the general provisions of the Penal Code, Part One: The general theory of crime*. Dar Al-Nahda Al-Arabiya.

Ahmed, I. S. (2005). *Legislative protection of electronic payment cards*. Al-Dar Al-Jamiiya.

Al-Faraijat, K. (2018). *Cybercrime and methods of combating it in Jordanian legislation: A comparative study*.

Al-Hasawi, M. A. (2019). *The principle of universality in criminal law* [Doctoral dissertation, Faculty of Law, Mansoura University].

Al-Halabi, K. (2000). *Procedures of investigation and inquiry in computer and internet crimes*. Dar Al-Thaqafa for Publishing and Distribution.

Al-Waqad, O. I. (1999). *Criminal protection of information technology*. Dar Al-Nahda Al-Arabiya.

Council of Europe. (2001). *Convention on Cybercrime (Budapest Convention)* (European Treaty Series No. 185). rm.coe.int/1680081561

Hassan, K. (2019). *Digital evidence and its role in proving cybercrime*. Dar Al-Fikr Al-Jamii.

Hassan, M. A. (2019). *Cybercrime and the problems of judicial jurisdiction*. Dar Al-Nahda Al-Arabiya.

Hassan, S. A. (1999). *Proving computer crimes and crimes committed via the internet* (1st ed.). Dar Al-Nahda Al-Arabiya.

Hegazy, A. B. (2009). *Procedural aspects of preliminary investigation in cybercrimes: A comparative study* (1st ed.).

Iraqi Code of Criminal Procedure No. 23 of 1971 and its amendments. (1971).

Iraqi Evidence Law No. 107 of 1979. (1979).

Law No. 175 of 2018 on Combating Information Technology Crimes. (2018). *Official Gazette, Issue No. 30 Bis (A)*, August 5, 2018.

fra.gov.eg/wp-content/uploads/2025/01/%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%B1%D9%82%D9%85-175-%D9%84%D8%B3%D9%86%D8%A9-2018-%D8%A8%D8%AA%D8%A7%D8%B1%D9%8A%D8%AE-2018-08-14.pdf

Mahmoud, H. (1981). *Modern scientific methods in criminal evidence*. Dar Al-Nahda Al-Arabiya.

Qarni, A. Y. (2006). *Remote criminal investigation and trial: An analytical and foundational study* (1st ed.). Dar Al-Nahda Al-Arabiya.

Saleh, N. (2020). Digital criminal evidence in comparative legislation. *Journal of Law (Kuwait)*, (2).

Saleh, S. (2023). Efforts of organizations combating cybercrime in cybersecurity. *Journal of Studies in Social Service*, (63), Part 3, 809–852.

dss.journals.ekb.eg/article_310334_627fe721ea71f199bd8f846d6487cba8.pdf

Salem, O. M. (2013). *Aspects of using modern technology in the field of criminal law: Electronic monitoring and remote criminal investigation*. Dar Al-Nahda Al-Arabiya.

Sorour, A. F. (2015). *Al-Wasit in the Penal Code: The general part*. Dar Al-Nahda Al-Arabiya.

Tharwat, J. (1989). *Systems of the general part in the Egyptian Penal Code*. Manshaat Al-Maaref.

United Nations Office on Drugs and Crime. (2019). *E4J cybercrime university module series, Module 4: Introduction to digital forensics*. United Nations. unodc.org/e4j/en/cybercrime/module-4/index.html

Younes, O. M. A. (2004). *Crimes arising from the use of the internet: Substantive provisions and procedural aspects* [Doctoral dissertation, Ain Shams University]. Dar Al-Nahda Al-Arabiya.