DOI: 10.22124/jol.2024.25877.2415

Research Article

University of Guilan Iranian association of penal law

*Criminal law Research*
**A Biannual Journal**
***Vol . 15, No.1, Spring & Summer 2024(Serial 29)***

# The challenges of the Iranian police in the Search and Seizure of data and the System in the Prevention and Detection of crime

1. Sayyad Darvishi,
Associate Professor of Police Command and Management Department. Dafoos College. Amin Comprehensive University of Police Sciences. Tehran. Iran.
(CorrespondingAuthor:s49darvishi@gmail.com)

2. Mohsen Rezaee,
Assistant Professor of Law Department. Faculty of Police Sciences and Techniques. Imam Hasan Mojtaba University of Officers and Police Training. Tehran. Iran.

| **Submit Date:2023/10/25** | **Accept Date:2024/06/16** |
|---|---|

***Abstract:***
The use of data and computer systems as the subject and means of committing a crime is one of the manifestations of the negative link between these technologies and criminal law. The purpose of this research is to identify the challenges of the Iranian police in the search and seizure of data and the system in the prevention and detection of crime. The current research is applied in terms of its purpose, and descriptive-analytical in terms of its type and in the category of qualitative research. By using library resources and interviews with university experts, data has been collected and analyzed by qualitative content analysis method. The findings indicate that the police faces challenges in the search and seizure of data and the system with two types of challenges including: The The challenges are in the field of protecting the privacy of individuals and in the field of legislative limitations and loopholes. Therefore, the elimination of legislative gaps in the field of privacy and police powers and their access to databases for the prevention and detection of crime are effective in solving the challenges of the police in inspecting and confiscating data and systems in Iran.

***Key Words:*** *Electronic data, Prevention, Crime Detection, Inspection, Seizure, Iranian police*

## 1. Introduction

Today, due to the advances made in the field of information and communication technology, new challenges have arisen in some areas such as their inspection and stopping. These challenges are often aimed at the police, who, in the capacity of law enforcement, are the main body for the implementation of search and seizure operations and the system. If the judicial officers pursue and continue to search and seize the crime without the permission of the judicial authority, not only the reasons they have obtained are invalid, but the violation is subject to criminal prosecution. Therefore, the police should be able to create a balance between the rights of individuals and the implementation of legal duties in the search and seizure of data and the system. In this regard, by identifying the many challenges facing the police and providing legal and interactive solutions, it is possible to overcome most of these challenges. On the other hand, considering the lack of research in this field and the weakness of the literature on this issue, the necessity of conducting research in this regard is felt. Therefore, this study seeks to answer the question:What are the challenges of the police in investigating and confiscating data and systems in Iran with the approach of crime prevention and detection?

## 2. Methodology

The current research is applied in terms of purpose, and descriptive-analytical in terms of research type and it is qualitative in terms of data collection method. Based on this, to identify the challenges of the police in inspecting and confiscating data and systems in Iran with a prevention Approach and crime detection using the statistical population Including: Library sources, documents and interviews with academic experts and legal Experts. The data was collected And, using the content analysis method as a research technique, concepts, categories and main and secondary factors were identified and analyzed.

## 3. Results and Discussion

The challenges of the Iranian police in the investigation and seizure of data and the system in the prevention and detection of crime in the field of violation of the privacy of individuals and in the legal field were identified, which challenges related to the violation of privacy include; 1) lack of transparency and comprehensiveness of the rights of data subjects, 2) inadequacy of regulations in protecting the confidentiality of data,3) lack of provision of differential regulations for the inspection of evidence of witnesses and victims and 4) weak protection of the privacy of third parties and victims be Also, the legal challenges to the collection and processing of data by the police include things such as; 1) Limitations due to judicial nature of search and seizure, 2) Gap of detailed regulations in explaining the principles and methods of data collection by the police, 3) Lack of provision of technical advice authority and differential regulations for encrypted data 4) Lack of regulations It becomes clear about preventive inspection and data discovery and, 5) not determining police powers in relation to access and hosting service providers .

## 4. Conclusions

This research was conducted with the aim of identifying the challenges of the Iranian police in the search and seizure of data and the system in the prevention and detection of crime. The police, in the position of law enforcement and police command of the country, as a security force that is responsible for establishing social order and security, on the one hand, assumes the duty of guaranteeing an important part of citizen's rights, such as the protection of life and property, and the rights and security of citizens. On the other hand, while performing his duties, due to his direct relationship with the citizens, he may take actions that, rightly or wrongly, are considered as a violation of citizen's rights. The results of this research indicate that one of the challenges of police officers, the ambiguities and interference of their duties in the search and seizure of evidence for the prevention and detection of crime, is "challenges surrounding the privacy of individuals". Therefore, in general, it can be said that in adapting this situation to the restrictions placed on the powers of the Iranian police in terms of obeying the judicial authorities, or measures limited to the urgency and necessity for the inspection or seizure of data and systems, practically due to the lack of The transparency and comprehensiveness of the rights of data subjects are challenged. Because it is not possible to create a discourse and a common understanding of expressions such as strong suspicion,

verification of urgency and necessity between the officers and the judicial authority. Also, on the other hand, due to the lack of provision of differential regulations for the inspection of the evidence of witnesses and victims and the weakness of the necessary regulations to protect the privacy of third parties and victims in the process of collecting electronic evidence, civil and criminal challenges are created for the officers. Sometimes a new criminal or civil case is opened against the officers. Also, the absence of a technical consulting authority and differential regulations for encrypted data and clear regulations regarding preventive inspection and data discovery in the context of laws doubles the problems of the police.

## 5. Selection of References

Ashawa, M., Mansour, A., Riley, J., Osamor, J., & Owoh, N. P. (2024). Digital Forensics Challenges in Cyberspace: Overcoming Legitimacy and Privacy Issues Through Modularisation. Cloud Computing and Data Science, 140-156.

Baraz, A., & Montasari, R. (2023). Law Enforcement and the Policing of Cyberspace. In Digital Transformation in Policing: The Promise, Perils and Solutions (pp. 59-83). Cham: Springer International Publishing.

Jaafari Langroudi, M. J. (2022), expanded on legal terminology. Tehran: Ganj Danesh Publications, [In Persisn]

Khater, M. H. (2023). International Perspective on Securing Cyberspace Against Terrorist Acts. International Journal of Sociotechnology and Knowledge Development (IJSKD), 15(1), 1-11.

Rahiminejad, I. (2023). Basic challenges of crime prevention rights in Iran. Research Journal of Criminal Law, 14(1), 115-89. [In Persisn]

Tabrizi, S., Aalipour, H., Elahi Menesh, M.R. (2022). The principle of proportionality in the seizure of data and the system in the criminal process. Justice Journal, 86(117), 131-152. [In Persisn]

Taghi Zadeh, M., & Kosha, J. (2022). the effectiveness of traditional police powers in detecting transnational cyber crimes, International Police Studies Quarterly, 13(52), 55-78 [In Persisn]

**Citation:**
Darvishi, S. & Rezaee,M (2024), "The challenges of the Iranian police in the Search and Seizure of data and the System in the Prevention and Detection of crime", **Criminal Law Research,** 15(29), pp. 85-98. DOI: 10.22124/jol.2024.25877.2415



DOI: 10.22124/jol.2024.25877.2415

نشریه علمی

پژوهشنامه حقوق کیفری

سال پانزدهم، شماره اول، بهار و تابستان ۱۴۰۳، پیاپی ۲۹

مقاله پژوهشی

صفحات مقاله: ۸۵-۹۸

# چالش‌های پلیس ایران در تفتیش و توقیف داده و سامانه در پیشگیری وکشف جرم

۱- صیاد درویشی*

دانشیار گروه فرماندهی و مدیریت انتظامی. دانشکده دافوس. دانشگاه جامع علوم انتظامی امین، تهران، ایران.

✉ s49darvishi@gmail.com

۲- محسن رضایی

دکتری حقوق. دانشکده علوم و فنون انتظامی. دانشگاه افسری و تربیت پلیس امام حسن مجتبی(ع)، تهران، ایران.

| تاریخ ارسال: ۱۴۰۲ /۰۸/۰۳ | تاریخ پذیرش : ۱۴۰۳/۰۳/۲۷ |
|---|---|

## چکیده:

استفاده از داده‌ها و سامانه‌های رایانه‌ای به‌عنوان موضوع و ابزار ارتکاب جرم از جمله نمودهای پیوند منفی بین این فناوری‌ها با حقوق کیفریاست . هدف این پژوهش شناسایی چالش‌های پلیس ایران در تفتیش و توقیف داده و سامانه در پیشگیری و کشف جرم است. پژوهش حاضر از نظر هدف، کاربردی و از نظر نوع پژوهش توصیفی– تحلیلی و در زمرهٔ تحقیق کیفی است. با استفاده از منابع کتابخانه‌ای و مصاحبه با خبرگان دانشگاهی، داده‌ها جمع‌آوری و به روش تحلیل محتوای کیفی تجزیه و تحلیل شده است. یافته‌ها بیانگر این است که پلیس در تفتیش و توقیف داده و سامانه با دو دسته از چالش‌ها شامل؛ چالش‌ها در حوزه حفظ حریم خصوصی اشخاص و درحوزه محدودیت و خلاءهای تقنینی است. بنابراین رفع خلاءهای تقنینی در حوزه حریم خصوصی و اختیارات پلیسی و دسترسی آن‌ها به پایگاه‌های داده جهت پیشگیری و کشف جرم، در رفع چالش‌های پلیس در تفتیش و توقیف داده و سامانه در ایران مؤثرند.

**واژگان کلیدی:** داده‌های الکترونیکی، پیشگیری، کشف جرم، تفتیش، توقیف، پلیس ایران

**مقدمه**

امروزه با توجه به پیشـرفت‌هایی که در زمینهٔ فناوری اطلاعات و ارتباطات ایجاد شـده، چالش‌های جدیدی در برخی حوزه‌ها همچون تفتیش و توقف آن‌ها به‌وجود آمده اسـت. این چالش‌ها اغلب متوجه پلیس بوده که در مقام ضـابطیت، نهاد اصـلی اجرای عملیات تفتیش و توقیف داده و سامانه می‌باشد. نظام‌های حقوقی در اعتباربخشی به تفتیش و توقیف و به‌طور کلی در تحصیل ادله رایلنه‌ای دارای رویکردهای متفاوتی هسـتند؛ در حقوق انگلسـتان به‌عنوان نماینده اصـلی نظام کامن‌لا، باوجود اختیار تقویم و تشخیص اعطائی به قاضی در خصوص ادله غیرقانونی، وجود چنین اختیاراتی به قاضی اجازه نمی‌دهد که یک دلیل تحصیل شده از طریق غیرقانونی را رد کند. در حقوق فرانسـه، به‌عنوان نماینده اصـلی رژیم رومی - ژرمنی، رویه قضـایی و دکترین محدودیت‌های ناشـی از موازین اصولی را علاوه بر محدودیت‌های قانونی حاکم براصل آزادی دلیل، مورد قبول قرارمی دهند. قاضی در امور کیفری نمی‌تواند اعتقاد باطنی خود را بر اموری متکی سازد، که در جریان رسیدگی به‌طور قانونی تحصیل نگردیده و به بحث آزاد طرفین در دعوی گذارده نشـده اسـت. بدین‌ترتیب، بر اسـاس ضـوابط قانونی داخلی و ماده ۳ قرارداد اروپایی حقوق بشـر، قاضـی از صـدور دسـتور تحصـیل دلایل ممنوعه مانند اعمال شـکنجه ممنوع گردیده است. همچنین بکار بردن شـیوه‌های علمی برای به‌دست آوردن اقرار یا کشف دروغ ممنوع است.

در مقابل، دادگاه های فرانسه خود را درمورد استفاده از ضبط صوت و ضبط مکالمات تلفنی و میکروفون، موافق نشان داده اند. با وجود این دادگاه های مزبور اسـتفاده از روش‌های متقلبانه را محکوم می‌نماید. در حقوق ایران هر گونه تفتیش و توقیف ادله جزء در موارد جرایم مشهود باید با اجازه مقام قضایی باشد. بنابراین اگر ضابطان دادگستری بدون اجازه مقام قضایی دست به تعقیب و در ادامه تفتیش و توقیف جرم بزنند نه تنها دلایلی که به دسـت آورده اند، فاقد اعتبار اسـت بلکه تخلف از آن مسـتوجب تعقیب کیفری است. پس پلیس در کشور نمی‌تواند از طرق غیرقانونی اقدام به جمع‌آوری دلایل کند. به عبارت دیگر با توجه بر اصل برائت و اصل قانونی بودن، تحصیل ادله کیفری نیز تحت الشعاع قرار گرفته‌اند. پس این اصول بر فضای سایبری نیز حاکم است و پلیس عملا در موارد زیادی در تفتیش و توقیف داده و سامانه با رویکرد پیشگیری و کشف جرم با چالش هایی مواجه است. لذا با عنایت به آنچه که بیان شد؛ می‌توان دریافت که پلیس در تفتیش و توقیف داده و سامانه باید بتواند در تقابل بین حقوق اشخاص و اجرای وظایف قانونی توازن ایجاد نماید. در این راستا، با شناسایی چالش‌های متعددی که متوجه پلیس می‌باشد و ارائه راهکارهای قانونی و تعاملی، می‌توان به رفع بخش زیای از این چالش ها فائق آمد. از سـوی دیگر با توجه به کمبود پژوهش در این زمینه و ضـعف ادبیات در این موضوع ضرورت انجام پژوهش در این خصوص احساس می‌شود. بنابراین این مطالعه در پی پاسخ به این سوال است که چالش های پلیس در تفتیش و توقیف داده و سامانه در ایران با رویکرد پیشگیری و کشف جرم کدامند؟

**پیشینه پژوهش**

تحقیق رحیمی نژاد در رابطه با «چالش‌های اسـاسـی حقوق پیشـگیری از جرم در ایران» نشـان داد که در وضـعیت فعلی، حقوق پیشـگیری از جرم در ایران با نوعی بحران هویت و نبود جایگاه شـایسـته مواجه اسـت(Rahiminejad,2023). پور نجفی، فخر و پورقهرمانی در بررسـی« پالایش فضـای سـایبری به مثابه جرم یا ابزار پیشـگیری ازآن؟» نشـان دادند که اکتفای دولت‌ها به قانونی بودن پالایش و عدم توجه به شـرایطی چون «ضـرورت و تناسـب» در اعمال آن، موجب مداخله بی رویه آن‌ها در حقوق بنیادین شهروندان شده است( Pournajafi, Fakhr & Pourgahermani,2022 ).

تقی‌زاده و کوشـا در پژوهش«اثربخشـی اختیارات سـنتی پلیس در کشـف جرایم سـایبری فراملی» به این نتیجه می‌رسـند که جهت توجه به ویژگی‌های جرایم سایبری، پلیس نیازمند ایجاد تحول در سیاست‌گذاری‌ها و افزایش اختیارات گسترده‌تر برای پلیس می‌باشد(Taghi Zadeh & Kosha,2022). تبریزی، عالی پور و الهی منش در پژوهش«اصل تناسب در توقیف داده و سامانه در فرایند کیفری» به این نتیجه می‌رسـد که اصـل تناسـب در توقیف داده، به معنای برقراری توازن میان چهار عنصـر ضـرورت توقیف، اهمیت داده و سامانه، ارتباط داده یا سامانه با جرم و ارتباط داده یا سامانه با داده‌ها و سامانه‌های دیگر است( Tabrizi , Aalipour

Elahi Menesh,2022 &). مرادی حق‌گو، شاملو و سایبانی در بررسی« صلاحیت منفعل در رسیدگی به جرایم سایبری: شرایط؛ چالش‌ها و پیامدها» به این نتیجه می‌رسند که چالش‌های صلاحیت منفعل در جرایم سایبری مواردی نظیر تورم کیفری و ایجاد چالش در کشف، تعقیب و رسیدگی و تعدد بزه‌دیدگان و تعارض در صلاحیت شخصی منفعل است( Moradi Haqgo, Shamlou & Saibani,2022). جعفری لنگرودی در بررسی «جرائم سایبر و رویکرد افتراقی حقوق کیفری بانگاهی به قانون مجازات اسلامی بخش جرائم رایانه‌ای» نشان داد که؛ اثربخشی و کارایی قوانین برای مقابله با جرائم دیجیتال مستلزم نگاهی متفاوت به مقوله‌هایی مانند تعریف جرم، ارکان جرم و مسئولیت های کیفری است (Jaafari Langroudi,2016). میرفلاح در پژوهش«شگردهای پلیس فتا در کشف جرایم سایبری» به این نتیجه می‌رسد که ذات مخفی و پوشیده فضای سایبر و حس ناشناخته ماندن، محیط ناملموس اما واقعی این فضا را بعضاً با هرج و مرج و ویران‌گری مواجه می‌سازد(Mirfallah,2015). کرمی در پژوهش«سیاست کیفری افتراقی در جرایم سایبر با تأکید بر حقوق کیفری ایران» به این نتیجه می‌رسد که تدوین یک سیاست منسجم کیفری در برخورد با جرایم سایبری در حقوق ایران ضروری است(Karami,2015).

آشیوا و همکاران در بررسی «چالش‌های پزشکی قانونی دیجیتال در فضای سایبری: غلبه بر مشروعیت و مسائل حریم خصوصی از طریق مدولارسازی» نشان دادند که فضای ابری چالش‌هایی را در تحقیقات پزشکی قانونی دیجیتال در رابطه با حفاظت از داده‌ها، مالکیت و مرزهای قضایی ایجاد می‌کند(Ashawa and et al,2024). براز و منتصری در بررسی«اجرای قانون و پلیس فضای مجازی» نشان می‌دهند که پلیس در برابر خطر رو به رشد جرایم سایبری، در حفاظت از داده‌های مردم با چالش جدی مواجه می‌باشد(Baraz & Montasari,2023). رینگارت در بررسی« صلاحیت اجرای فراسرزمینی در فضای مجازی: تغییرات هنجاری» به این نتیجه رسید که چشم نوازترین اثر دیجیتالی شدن بر قانون صلاحیت اجرایی، محو شدن صلاحیت سرزمینی است(Ryngaert,2023). نتایج مطالعات حسن تحت عنوان« کاربرد حقوق اساسی در فضای مجازی: تشریح قانون امنیت دیجیتال» نشان داد که علیرغم اجرای این قانون، لیکن نگرانی‌هایی در مورد اینکه چگونه این قانون بر حق آزادی بیان و سایر حقوق اساسی تأثیر می‌گذارد، وجود دارد(Hasan,2023). خاتر در بررسی«کاربرد حقوق اساسی در فضای مجازی: تشریح قانون امنیت دیجیتال» با استفاده از رویکردهای حقوقی نشان می‌دهد که ادامه تلاش های بین المللی برای تقویت مبارزه با تروریسم سایبری و ایجاد یک معاهده قانونی الزام آور در این زمینه یک امر ضروری است(Khater,2023). همچنین نتایج تحقیق ان جی سی ای و مکایز تحت عنوان« مطالعه اکتشافی سیستم‌های خدمات پلیس آفریقای جنوبی[1] در مبارزه با جرایم سایبری » نشان دادند که عصر دیجیتال چالش‌های جدیدی را برای اجرای قانون ایجاد کرده و تهدیدی مهم برای حریم خصوصی شخصی بوده است( Ngcece & Mkhize,2023).

با ملاحظه و تحلیل پیشینه و تحقیقات گذشته، بیشتر تحقیقات داخلی بر توجه به ویژگی‌های جرایم سایبری، لزوم ایجاد تحول در سیاست‌گذاری‌ها و تغییر در برنامه‌ریزی‌ها، چالش‌های صلاحیت منفعل در جرایم سایبری، فرامرزی بودن و سیاست کیفری افتراقی در جرایم سایبر با تأکید بر حقوق کیفری ایران مورد کنکاش قرار گرفته و در حوزه مطالعات خارجی نیز؛ چالش‌های پزشکی قانونی دیجیتال در فضای سایبری، چالش‌های اجرای قانون توسط پلیس در فضای مجازی، ایجاد مبانی قانونی برای پیشگیری و تعقیب جرایم دیجیتال و سیستم‌های خدمات پلیس در مبارزه با جرایم سایبری مورد مطالعه قرار گرفته است و بنابراین نتایج این تحقیق دارای نوآوری و جدید است.

## ادبیات پژوهش

**مفهوم داده و سامانه:** درکنوانسیون جرایم سایبر، معروف به «کنوانسیون جرایم سایبری بوداپست» [2]منظور از «داده رایانه‌ای» هرگونه نمایش حقایق، اطلاعات یا مفاهیم به شکلی مناسب که برای پردازش در یک سیستم رایانه‌ای که شامل برنامه‌ای مناسب

1 . SAPS
2 . "Budapest Cybercrime Convention"

است و باعث می‌شود که این سیستم عملکرد خود را به مرحله اجرا گذارد، مورد استفاده قرار می‌گیرد. واژه «داده» به صورت خاص در نظام حقوقی ایران تعریف نشده است ولی به صورت «داده پیام» و «داده ترافیک» از آن تعریف به عمل آمده است. داده پیام در بند الف ماده یک قانون تجارات الکترونیک به این صورت تعریف شده است: «داده پیام هر نمادی از واقعه، اطلاعات یا مفهوم است که با وسایل الکترونیکی، نوری و یا فناوری‌های جدید اطلاعات تولید، ارسال، دریافت، ذخیره یا پردازش می‌شود. داده ترافیک نیز در تبصره یک ماده ۳۲ قانون جرایم رایانه‌ای (تبصره ۱ ماده ۶۶۷ ق.آ.د.ک 1392) تعریف شده است: «داده ترافیک، هرگونه داده‌ای است که سامانه‌های رایانه‌ای در زنجیره ارتباطات رایانه‌ای و مخابراتی تولید می‌کنند تا امکان ردیابی آنها از مبدأ تا مقصد وجود داشته باشد.

مطابق بند (د)، کنوانسیون جرایم سایبر، منظور از «داده ترافیک» هر گونه داده رایانه‌ای است که مرتبط با ارتباط برقرار شده به وسیله سیستم رایانه‌ای است (Fazli,2012: 76) . طبق ماده ۲ قانون تجارت الکترونیک داده پیام «هر نمادی از واقعه، اطلاعات یا مفهوم است که با وسایل الکترونیکی، نوری یا فناوری‌های جدید اطلاعات تولید، ارسال، دریافت، ذخیره یا پردازش می‌شود». به‌طورکلی داده‌های الکترونیکی به دو دسته تقسیم می‌شوند: الف) داده‌های شکلی؛ ب) داده‌های محتوایی.

منظور از داده‌های شکلی هرگونه اطلاعاتی اعم از الکترونیکی و غیر الکترونیکی راجع به مشخصات محتوای ارتباطات الکترونیکی است. داده‌های محتوا نیز هر نوع داده‌ای است که منعکس‌کننده منظور و مضمون یک ارتباط الکترونیکی باشد در بر می‌گیرد . (Thomas & Davies,2016:15)

در کنوانسیون جرایم سایبر، منظور از «سیستم رایانه‌ای و سامانه» هر گونه ابزار یا مجموعه‌ای از ابزارهای مرتبط و متصل به هم است که مطابق با یک برنامه، پردازش خودکار داده‌ها را انجام می دهد. در نظام حقوقی ایران، این واژه تا قبل از تصویب آیین‌نامه نحوه استفاده از سامانه‌های رایانه‌ای یا مخابراتی مصوب ۱۳۹۵؛ مورد مفهوم‌شناسی قرار نگرفته بود. بند «ب» ماده یک آیین‌نامه اخیر؛ سامانه رایانه‌ای را به این صورت تعریف کرده است: «مجموعه‌ای از نرم‌افزارها و سخت افزارهای مرتبط که از طریق یک شبکه رایانه ای جهت اجرای فرایندهای کار مشخصی، به یکدیگر متصل‌اند». امروزه سامانه‌های رایانه ای به‌عنوان ابزاری در خدمت دستگاه عدالت، بسترهای لازم را برای توسعه فناوری در مراحل مختلف دادرسی فراهم می‌نماید.

یکی از مهم‌ترین پیوندهای منفی که برای داده و سامانه می‌توان ذکر کرد، استفاده مجرمانه از آنها است. داده و سامانه می‌توانند هم به عنوان موضوع جرم و هم می‌توانند به‌عنوان وسیله ارتکاب واقع شوند. در مورد موضوع جرم بدواً باید بیان داشت که هر جرمی الزاماً باید دارای موضوع باشد و جرم بدون موضوع نمی‌تواند وجود خارجی داشته باشد. مثلاً در قتل خود انسان موضوع جرم قرار می‌گیرد و در توهین و افترا، حیثیت و آبروی وی موضوع جرم قرار می‌گیرد. در برخی از جرایم رایانه‌ای نیز موضوع جرم خود داده‌ها و سامانه‌ها هستند مثلاً در سرقت داده یا سامانه، ابزارهای اخیر موضوع جرم هستند .

از جمله تفاوت‌های بین این دو می‌توان به فرایند توقیف داده و شرایط و اصول حاکم بر آنها به عنوان ادله اثبات جرم اشاره کرد. برخلاف ادله سنتی که دارای فرایندهای تعریف شده بوده و در قوانین کشورها، مقررات مشخصی برای آنها پیش‌بینی شده برای توقیف داده و سامانه، ابهامات و مشکلات تقنینی، قضایی و اجرایی متعددی وجود دارد. با توجه به همین مشکلات موجود بر سر راه توقیف ادله رایانه ای که بیشتر سیستم‌های حقوقی کشورهای دنیا در قوانین مربوط به خود با نقصان در این رابطه مواجه می‌باشند، توصیه‌نامه شورای اروپا در خصوص مشکلات آیین دادرسی مصوب سپتامبر 2016 به‌عنوان راهنمایی، تا حدودی توانست در رفع مشکلات یاد شده موثر باشد (Dezbani,2015: 30).

**مفهوم تفتیش و توقیف:** تفتیش امری است شامل جمع‌آوری ادله که با تحقیق در مورد دلایل جرم از سوی مقام‌های مخصوص به این کار انجام می‌گیرد. صرف نظر از اراده و رضایت فرد یا صاحب مکان مورد نظر، تفتیش عملی است تحقیقی که این مقام در محل خاص یا در مورد خاصی و برای زمینه‌سازی جهت اعمال حق جامعه در مورد مجازات انجام می‌دهد :2022, (Jaafari Langroudi 5006).

توقیف داده و سامانه به معنای این است که شخص دارای صلاحیت، داده یا سامانه را در موارد پیش‌بینی شده در قانون توقیف نماید و این اجازه را به مالک یا متصرف ندهد که در داده و سامانه توقیف شده دخل و تصرفی نماید.

در قانون آیین دادرسی کیفری فرانسه در مرحله‌ی تحقیقات ابتدایی، افسران پلیس قضائی می‌توانند اقدام به توقیف اسناد، مدارک یا داده‌های رایانه‌ای نمایند. «ضبط و توقیف اطلاعات و داده‌های رایانه‌ای ضروری برای کشف حقیقت و قرار دادن آن در اختیار دادگستری، از طریق ضبط سخت‌افزار این اطلاعات و داده‌ها یا کپی آنها، در حضور اشخاصی که به جرم بازرسی کمک کرده‌اند، صورت می‌گیرد. در صورت تهیه کپی از داده‌های رایانه‌ای، براساس تعلیمات و دستورات دادستان شهرستان، اطلاعات موجود بر روی سخت‌افزارهایی که در اختیار دادگستری نیست و نگهداری یا استفاده از آنها مضر به امنیت اشخاص یا اموال باشد، به‌صورت قطعی پاک می‌شود (Casey, 2008: 85). در کنوانسیون اروپایی جرایم سایبر اصل تناسب برگزیده شده و همانطور که حساسیت‌های ناشی از مصون ماندن حریم داده‌های الکترونیکی افراد در قبال تعرض از سوی مجریان قانون را پذیرفته، در عین حال قبول دارد که اگر مجریان قانون از اختیار عمل جهت انجام وظایف مقرره برخوردار نباشند، مجرمین بدون واهمه از تعقیب و دستگیری، بیشتر به ارتکاب اعمال مجرمانه سوق می‌یابند. به همین دلیل اختیاراتی برای آنها قائل شده است Jalali ) . (Farahani,2007: 90علاوه بر قانون، پیش‌بینی اختیارات برای پلیس در جهت منافع عمومی است. برای نمونه باید گفت اگر توطئه ثابت شود حکم حریم خصوصی نمی‌تواند مانع اخلاقی در بالا رفتن از خانه شخص گردد(Kelsen,2020: 19) . در این‌گونه موارد و در تلاقی حقوق فرد و جمع مسلماً اولویت با جامعه است(Kubben, Dumontier & Dekker,2029: 326) .

در پایان ادبیات این پژوهش با نگاهی تطبیقی برخی اصول حاکم بر حفاظت از محتوای داده‌ها در سه کشور ایران، فرانسه و انگلیس در جدول ۱. آورده شده است.

**جدول ۱: برخی اصول حاکم بر حفاظت از محتوای داده‌ها در سه کشور ایران، فرانسه و انگلیس(نگارنده)**

| اصول | جمهوری اسلامی ایران | فرانسه | انگلستان |
|---|---|---|---|
| **اصل تناسب و ضرورت** | اصل ضرورت، در بستر مواد قانونی ۶۷۵، ۶۷۷ و ۶۷۸ قانون آیین دادرسی کیفری، حاکم بر عملکرد پلیس در مرحله انجام تفتیش داده‌ها و توقیف سامانه است؛ ولی دستورالعمل یا آیین‌نامه اجرایی در تشخیص این تناسب وجود ندارد و از طرفی اختیار پلیس در سنجش تناسب یا ضرورت، توقیف داده و سامانه، در طول و مادون تشخیص ضرورت توسط مقام قضایی می باشد. | مطابق با ماده ۸۶ و ماده ۸۹ از مقررات عمومی حفاظت از داده‌ها، رعایت اصل ضرورت، تأکید شده است. ماده ۴ از مواد عمومی مقررات حفاظت از داده فرانسه و ماده ۵۶ قانون آیین دادرسی این کشور، به طور خاص نسبت به محدود بودن قلمروی تفتیش به حد کافی برای کشف حقیقت تصریح دارند. | بندهای ۸ تا ۱۰ ازفصل سوم قانون حفاظت عمومی از داده‌های انگلستان، نسبت به اصل ضرورت در تفتیش و توقیف داده و سامانه تصریح دارد. بند ۱۳-۴ بخش سوم قانون اختیارات تحقیق، هر گونه احراز تناسب را منوط به ارزیابی میزان جدیت لطمه به حریم خصوصی اشخاص می داند. |

| | | | |
|---|---|---|---|
| اصل شفافیت و منصفانه بودن پردازش | اصل موصوف به‌عنوان یک اصل جداگانه در نظر گرفته نشده و مهمترین مصداقی که در ماهیت نزدیک به آن در حقوق ایران قابل شناسایی به نظر می رسد، حق حضور متصرف سامانه در زمان تفتیش و توقیف داده ها است. | ماده ۴ و ماده ۵ از قانون حفاظت از اطلاعات فرانسه، دستورالعمل حمایت از داده در برابر پلیس و مقامات دادرسی کیفری و مقررات عمومی حفاظت از داده‌های اتحادیه اروپا، رکن قانونی برای ضرورت اعمال اصل شفافیت و منصفانه بودن پردازش است . | ماده ۵۳ از قانون اختیارات تحقیق این کشور مقام تفتیش را ملزم به رعایت مقتضیات اصل منصفانه بودن تحقیقات می‌داند. |
| اصل پاسخگویی و نظارت | در مقررات جمهوری اسلامی ایران، مرجع نظارت مستقل، اختصاصی یا تخصصی برای نظارت بر تفتیش و توقیف داده ها در نظر گرفته نشده و مقررات مربوط به این حوزه نیز صرفا منحصر به تخلفات عمومی ضابطین دادگستری یا مقامات قضایی و یا شمول ضمانت اجراهای مقرر در قانون جرایم رایانه ای برای تحصیل یا افشای غیرمجاز داده ها است. | در فرانسه، کمیسیون ملی اطلاعات و آزادی‌ها، به موجب قانون حفاظت از داده‌های فرانسه، مسئول اصلی نظارت بر صدور تمامی قرارهای تفتیش صادره توسط مقامات قضایی یا مقامات دولتی در موارد مجاز است. . | در انگلستان، دفتر مجوز داده ارتباطات( دفتر کمیسیرهای اختیارات تحقیق) به اقدامات تفتیش و توقیف داده و سامانه نظارت دارد. مطابق با قانون حفاظت از داده های انگلستان، بر تمامی فرایندهای تفتیش داده‌ها نظارت مستمر دفتر مذکور وجود دارد. |

**روش تحقیق**

پژوهش حاضر از نظر هدف، کاربردی و از نظر نوع پژوهش توصیفی– تحلیلی و از نظر روش جمع‌آوری داده‌ها در زمره تحقیق کیفی است.. بر این اساس برای شناسایی چالش‌های پلیس در تفتیش و توقیف داده و سامانه در ایران با رویکرد پیشگیری و کشف جرم با استفاده از جامعه آماری شامل؛ منابع کتابخانه‌ای، اسنادی و مصاحبه با خبرگان دانشگاه علوم انتظامی امین، گروه حقوق، پیشگیری از جرم، گروه جرم یابی و کارشناسان حقوقی این حوزه، داده ها جمع آوری و با استفاده از روش تحلیل محتوا به مثابه تکنیکی پژوهشی، مفاهیم، مقوله ها و عوامل اصلی و فرعی شناسایی و مورد تجزیه و تحلیل قرار گرفت.

در پژوهش‌های کیفی داده‌ها از منابع متنوع و چندگانه جمع آوری می‌شود، که در این مطالعه از اسناد مرتبط با موضوع، با بررسی طیف وسیعی از اسناد و رویه ها و سایر آثار پژوهشی و مصاحبه نیمه ساختار یافته با تعداد ۱۲ نفر از جامعه آماری تاحد اشباع نظری استفاده گردید و داده های اولیه جمع آوری گردید. در این پژوهش مصاحبه با خبرگان و کارشناسان تا اشباع نظری پیش رفت و در ۱۲ نفر تثبیت و داده ها تکرار گردید. برای حصول اطمینان از روایی بخش کیفی پژوهش و به منظور اطمینان خاطر از دقیق بودن یافته ها از دیدگاه پژوهشگر، از نظرات ارزشمند اساتید آشنا با این حوزه و متخصصان حقوقی که در این حوزه خبره و مطلع بودند استفاده شد. هم چنین به طور هم زمان از مشارکت کنندگان درتحلیل و تفسیر داده ها کمک گرفته شد. داده‌ها به روش تحلیل محتوای کیفی مورد تجزیه و تحلیل قرار گرفتند.

**یافته‌ها**

یافته‌ها بیانگر این است که پلیس در تفتیش و توقیف داده و سامانه با دو دسته چالش مواجه می‌باشد. چالش نخست پیرامون حفظ حریم خصوصی اشخاص و حقوق اشخاص موضوع داده و سامانه است و چالش دوم مرتبط با محدودیت و خلاءهای تقنینی است که در جدول ۲. نشان داده می‌شود و در ادامه با تطبیق مقررات پیش‌بینی شده در نظام کیفری ایران، با مقررات کشورهای انگلستان و فرانسه به تبیین هر یک از این چالش‌ها پرداخته می‌شود.

**جدول۲. شناسایی چالش های پلیس در تفتیش و توقیف داده و سامانه در ایران با رویکرد پیشگیری و کشف جرم**

| متغیر | مقوله ها | زیر مقوله‌ها |
|---|---|---|
| چالش‌های پلیس در تفتیش و توقیف داده و سامانه | حفظ حریم خصوصی و حقوق اشخاص | عدم شفافیت حقوق اشخاص موضوع داده |
| | | عدم جامعیت حقوق اشخاص موضوع داده |
| | | عدم کفایت مقررات در حمایت از محرمانگی داده‌ها |
| | | ضعف حمایت از حریم خصوصی اشخاص ثالث |
| | | ضعف حمایت از حریم خصوصی اشخاص بزه دیده |
| | | عدم پیش‌بینی مقررات افتراقی برای تفتیش ادله شهود |
| | | عدم پیش‌بینی مقررات افتراقی برای تفتیش ادله بزه دیدگان |
| | محدودیت و خلاءهای تقنینی | محدودیت‌های ناشی از قضایی بودن تفتیش |
| | | محدودیت‌های ناشی از قضایی بودن توقیف |
| | | خلأ مقررات تفصیلی در تبیین اصول و شیوه های جمع آوری داده‌ها توسط پلیس |
| | | عدم پیش‌بینی مرجع مشاوره فنی و مقررات افتراقی برای داده‌های رمزنگاری شده |
| | | نبود مقررات شفاف پیرامون تفتیش پیشگیرانه ی داده‌ها |
| | | نبود مقررات شفاف پیرامون تفتیش کشف داده‌ها |
| | | عدم تعیین اختیارات پلیس در ارتباط با ارائه‌دهندگان خدمات دسترسی و میزبانی (رسانه‌ها) |

**الف: چالش‌های مرتبط با نقض حریم خصوصی**

با توجه به یافته‌های تحقیق، چالش‌های زیر در ارتباط با حریم خصوصی اشخاص و قواعد ناظر بر آن توضیح داده می‌شود.

**۱. عدم شفافیت و جامعیت حقوق اشخاص موضوع داده**

در یک نگاه کلی، حق حضور متصرف در زمان تفتیش، حق اعتراض نسبت به ضررهای ناشی از دستور تفتیش و توقیف، حق اخذ کپی از داده‌های توقیف یا محتوای سامانه‌های حفاظت شده در زمره معدود حقوق قابل اعمال از سوی شخص ذینفع یا مالک داده است؛ حال آنکه حقوق شخص موضوع داده در فرایند تفتیش و توقیف داده و سامانه، در دو کشور فرانسه و انگلستان، منحصر به موارد ذکر شده نیست و حقوقی مانند حق محدود کردن اطلاعات، حق اصلاح داده‌ها، حق ارتباط مستمر با افسر کنترل‌کننده یا نماینده وی، درخواست حذف داده‌ها، حق آگاهی از اهداف، مدت و فرایند تفتیش و توقیف و حق مصون بودن جان و اموال وی از

ضرر شدید در فرایند تفتیش و توقیف، در زمره مواردی است که در راستای حفاظت از حریم خصوصی اشخاص پیش‌بینی شده است. لیکن این حقوق در قانون جرائم رایانه ای مصوب ۱۳۸۸ کمتر مورد توجه قرار گرفته است. حتی در ماده ۳۴ در وظایف ضابطین در خصوص تفتیش و توقیف داده‌ها و سامانه‌ها به حقوق صدرالاشاره مالک داده توجه خاصی نشده است.

همچنین قانون آئین دادرسی کیفری ایران از شفافیت کافی در ارتباط با حقوق اشخاص موضوع داده برخوردار نیست و همین موضوع، امکان برخورد سلیقه‌ای منجر به نقض حقوق شخص موضوع داده یا ایجاد غیرتعمدی مسئولیت برای ضابطین دادگستری را ایجاد می‌کند. بنابراین باوجود اینکه در ماده ۶۷۲ آئین دادرسی کیفری، تأکید گردیده تفتیش و توقیف داده‌ها یاسامانه‌های رایانه‌ای و مخابراتی در حضور متصرفان قانونی یا اشخاصی که به نحوی آنها درتحت کنترل قانونی دارند، اما برخی حقوق اشخاص از قبیل حق اعتراض نسبت به ضررهای ناشی از دستور تفتیش و توقیف و غیره مورد توجه قرار نگرفته است.

### ۲. عدم کفایت مقررات در حمایت از محرمانگی داده‌ها

در حقوق ایران، اولاً هیچ‌گونه تفکیکی میان نوع داده‌ها (به‌عنوان مثال، تفکیک داده‌های حساس مانند پزشکی و جنسی یا ممتاز از حیث فرایند تفتیش و حقوق اشخاص) وجود ندارد و ارائه‌دهندگان خدمات دسترسی و میزبانی نیز مکلف هستند بدون تبعیض داده‌های مورد درخواست را در اختیار مقام قضایی و عمدتا ضابط دادگستری قرار دهند. هر چند برابر ماده ۷ آیین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیکی مصوب ۱۳۹۳ داده‌های محتوا و ترافیک و اطلاعات کاربران باید مطابق مقررات این آیین‌نامه به نحوی نگهداری، حفاظت، توقیف و ارائه شود که صحت و تمامیت، محرمانگی، اعتبار و انکارناپذیری آنها محفوظ بماند. اما به تفکیک داده‌های حساس و حقوق اشخاص توجه جدی نشده است. از سوی دیگر، حمایتی که از اقشار خاص، مانند وکلا، روزنامه نگاران و مؤسسات خبری، سردفتران، پزشکان و ... به واسطه در اختیار داشتن اسناد محرمانه یا اطلاعات فردی اشخاص ثالث در مقررات عمومی حفاظت از داده‌ها (مصوب اتحادیه اروپا)، قانون اختیارات تحقیق انگلستان و به‌ویژه قانون آیین دادرسی کیفری فرانسه به عمل آمده است، در مقررات ایران پیش‌بینی نشده است که خود این موضوع دلالت بر احتمال بیشتر نقض اصل محرمانگی و حریم خصوصی اشخاص در عملکرد مأمورین پلیس را دارد.

از دیگر موارد با اهمیت در این زمینه، وضع ضوابط تعیین‌کننده و راهنمای پلیس در نحوه تفتیش و استخراج اطلاعات است که در قوانین فرانسه و انگلستان، به صورت نسبی، در نظر گرفته شده، ولی در حقوق ایران، به‌ویژه در پرتوی عدم وضع آیین نامه موضوع ماده ۶۸۴ قانون آیین دادرسی کیفری، مغفول و محدود به بیان اصل کلی حفاظت از داده‌ها مانده است.

### ۳. عدم پیش‌بینی مقررات افتراقی برای تفتیش ادله شهود و بزه دیدگان

یکی از موارد با اهمیت در شناسایی جرایم، تفتیش ادله الکترونیکی موجود در سامانه‌های شهود و بزه دیده‌های جرایم است. با بررسی قانون جرائم رایانه ای مصوب ۱۳۸۸ و آیین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیکی مصوب ۱۳۹۳ و همچنین قسمت دادرسی الکترونیکی آیین دادرسی مصوب ۱۳۹۲ پیش‌بینی مقررات افتراقی برای تفتیش ادله شهود و بزه دیدگان به عمل نیامده است. در شرایطی که تضمین‌های لازم برای اعمال مقررات افتراقی، رعایت محرمانگی و عدم لطمه به حریم خصوصی این اشخاص وجود نداشته باشد، اساساً این اشخاص نسبت به گزارش جرم نیز با تردید مواجه شده و به‌ویژه در خصوص شهود، چه بسا از در اختیار قرار دادن داده‌های سامانه‌های الکترونیکی و مخابراتی به پلیس خودداری نمایند یا برخی داده‌ها را حذف نمایند و مشکل بازیابی داده‌ها را برای پلیس ایجاد کنند. حال آن که مطابق با تبیین صورت گرفته، مقررات برخی کشورها همچون کشور انگلستان در این خصوص، توام با یک قانون خاص (قانون پلیس، جرم، مجازات و دادگاه‌های قانونی (مصوب ۲۰۲۲) هست که مقررات ویژه و افتراقی برای تفتیش و توفیف داده و سامانه شهود و بزه دیده‌ها پیش‌بینی نموده است.

**۴. ضعف حمایت از حریم خصوصی اشخاص ثالث و بزه دیده**

در این خصوص، قانون اختیارات تحقیق کشور انگلستان، تصریح نموده است که اگر قرار صادره موضوعی نباشد و ناظر بر شخص یا سازمان خاصی باشد، برای رهگیری داده‌های مربوط به شخص ثالث باید مجوز جدید صادر شود، ولی اگر اصلاح به صورت جزیی باشد، مانند حذف یک نام یا توصیف یک شخص، دیگر نیازی به صدور تصمیم جدید نیست. در حقوق ایران، هر چند چنین حکم مصرحی راجع به این موضوع وجود ندارد، ولی از آنجا که اساسا صدور حکم تفتیش و توقیف مستلزم تعیین داده‌ها و سامانه‌ها توسط مقام قضایی شده است، بنابراین حق تفتیش اطلاعات اشخاص ثالث در نظام کیفری ایران نیز نیازمند صدور دستور جداگانه است.

با این وصف، چالش حقوق اشخاص ثالث زمانی بیشتر نمود می‌یابد که اطلاعات شخص ثالث بر سامانه‌هایی باشد که مقام قضایی دستور توقیف آن‌ها را داده است. در این ارتباط قانون آیین دادرسی کیفری جمهوری اسلامی ایران به‌ویژه دادرسی الکترونیکی ساکت است و در نتیجه هیچ‌گونه منع یا ملاحظه خاصی نسبت به این اشخاص در نظر نگرفته است، ولی بند ۸ ماده واحده قانونی احترام به آزادی‌های مشروع و حفظ حقوق شهروندی مصوب ۱۳۸۳، مقرر نموده « بازرسی‌ها و معاینات محلی، جهت دستگیری متهمان فراری یا کشف آلات و ادوات جرم براساس مقررات قانونی و بدون مزاحمت و در کمال احتیاط انجام شود و از تعرض نسبت به اسناد و مدارک و اشیایی که ارتباطی به جرم نداشته و یا به متهم تعلق ندارد و افشای مضمون نامه ها و نوشته ها و عکس های فامیلی و فیلم های خانوادگی و ضبط بی‌مورد آنها خودداری گردد».

**ب: چالش‌های تقنینی فراروی جمع‌آوری و پردازش داده توسط پلیس**

در این قسمت با توجه به یافته‌های تحقیق، اهم چالش‌هایی که پلیس را برای اقدام به موقع و کارآمد در تفتیش و توقیف داده و سامانه محدود یا تضعیف می‌کند، توضیح داده می‌شود.

**۱. محدودیت‌های ناشی از قضایی بودن تفتیش و توقیف**

یکی از وظایف ذاتی ضابطین دادگستری، پایبندی به دستورات قضایی صادره توسط مراجع قضایی است که ضابطین دادگستری صرفاً مجری آن محسوب می‌شوند. هر چند در بسیاری موارد، تشخیص نقض دستورات توسط ضابطین و به تبع آن ایجاد مسئولیت کیفری، مدنی و انتظامی برای ضابطین، مشخص و قابل شناسایی است، ولی در برخی موارد، مانند تحصیل ادله الکترونیک، تشخیص پایبندی به دستورات مقام قضایی مشکل می‌نماید. بنابراین اصل قضایی بودن، با شدتی که در نظام آئین دادرسی کیفری ایران مشاهده می شود، با ماهیت تفتیش و توقیف داده که سرشار از مسائل فنی و غیرقضایی است، سازگار به نظر نمی‌رسد؛ حال آنکه چالش‌های اجرایی فراروی پلیس اقصی نقاط جهان نیزدر پایبندی به دستورات مقام قضایی، در مقام تفتیش یا توقیف داده و سامانه وجود دارد و بر همین اساس، برخی کشورها یا ایالت‌ها، مبادرت به تفویض اختیار گسترده تر به پلیس به منظور تحصیل ادله الکترونیک درصدد رفع یا کاهش چالش برآمده‌اند که نمونه آن نه تنها در کشورهای کامن لا، بلکه در کشورهای پیشرو در حقوق مدون، مانند فرانسه هم قابل مشاهده است(Purtova,2018: 14) .

در خصوص تطبیق این وضعیت با محدودیت‌های وارد شده به اختیارات پلیس ایران از حیث تبعیت از مقام قضایی، باید گفت که در قانون آیین دادرسی کیفری جمهوری اسلامی ایران، تمام تلاش مقنن بر این قرار گرفته که وظایف ضابطین دادگستری را محدود به تبعیت از مقام قضایی نموده و از حیث تقنینی، تنها زمانی که ضابطین دادگستری رأسا امکان اقدام دارند، در صدور دستور حفاظت، آن هم محدود به احراز فوریت و ضرورت است و حتی در زمانی که ضابطین با سامانه ای مواجه شوند که در دستور مقام قضایی نمی‌گنجد، برای تفتیش یا توقیف داده و سامانه‌هایی که دستور شامل آن نمی‌شود، نیازمند اخذ دستور مجدد قضایی هستند.

**۲. خلأ مقررات تفصیلی در تبیین اصول و شیوه‌های جمع‌آوری داده‌ها توسط پلیس**

در تمام امور مربوط به تفتیش و توقیف داده و سامانه، نیاز هست اصول و شیوه‌های جمع‌آوری یا نگهداری از داده‌های الکترونیک وجود داشته باشد. در قانون ایران نسبت به مقررات ناظر بر کنترل داده‌های در حال انتقال یا مقررات راجع به رهگیری انبوه ساکت است. چنانچه در آیین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیکی، جمع آوری داده‌ها به‌عنوان فرایندی تعریف شه است که طی آن ادله الکترونیکی به تنهایی یا به همراه سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده، نگـــــــهداری، حفظ فوری، تفتیش و توقیف و شنود می‌شوند، درحالی‌که اصول و شیوه‌های انجام این فرایند مغفول ماده است و بعضا فرایند و چگونگی جمع‌آوری دلایل الکترونیکی برای ضابطین چالش‌های مدنی و کیفری ایجاد می‌نماید.

**۳. عدم پیش‌بینی مرجع مشاوره فنی و مقررات افتراقی برای داده‌های رمزنگاری شده**

یکی از تهدیدهای فراروی تفتیش و توقیف داده و سامانه، داده‌های رمزنگاری شده و داده‌های ابری است که صعوبت در پردازش داده‌ها ایجاد می‌کند. بر همین مبنا، در قوانین برخی کشورها، به موضوع استفاده از مشاوره‌های فنی و قابلیت ارائه اخطار فنی نسبت به ارائه‌دهندگان خدمات دسترسی و خدمات میزبانی، تصریح گردیده و استفاده از شرکت‌های ارائه کننده خدمات ابری صراحتا مورد پذیرش قرار گرفته است. همچنین در این بستر، برای پلیس فرانسه حق تحمیل الزاماتی به ارائه‌دهندگان خدمات دسترسی و میزبانی پیشبینی شده که در قانون جرائم رایانه ای ایران ، آیین نامه جمع‌آوری و استنادپذیری ادله الکترونیکی ، آیین دادرسی کیفری و دادرسی الکترونیکی نسبت به آن مسکوت بوده و توجه خاصی نگردیده و مشاوره فنی و مقررات افتراقی برای بررسی داده‌های رمزنگاری شده تعیین نگردیده است.

**۴. نبود مقررات شفاف پیرامون تفتیش پیشگیرانه و کشف داده‌ها**

یکی از اهداف تفتیش، نبودپیش‌بینی مقررات راجع به تفتیش پیشگیرانه و کشف داده‌ها است. این مهم در قوانین ایران مغفول مانده است. هر چند در وجود این خلاء قانونی، مصوبات کمیسیون امنیت ملی در دفاع از امنیت ملی یا مصوبات شورای عالی فضای مجازی یا تبادل اطلاعات کشور و کارگروه تعیین مصادیق محتوای مجرمانه، جایگزین مقررات تفنینی پیرامون تفتیش پیشگیرانه در جمهوری اسلامی ایران شده است، ولی نمی‌توان این واقعیت را نادیده انگاشت که تداوم این وضعیت، هم ابتکار عمل را از ضابطین انتظامی و پلیس فتا در تفتیش پیشگیرانه و دسترسی به اهداف کنترل دامنه جرم در فیشینگ یا جلوگیری از حملات سایبری سلب می‌کند و هم حقوق اشخاص خصوصی از جمله احترام به حریم خصوصی آن‌ها مبهم باقی می‌ماند و تعیین وظایف پیشگیرانه پلیس در این حوزه در چارچوب ضوابط و ملاحظات قانونی می‌تواند خلاء موجود را رفع نماید.

**۵. عدم تعیین اختیارات پلیس در ارتباط با ارائه‌دهندگان خدمات دسترسی و میزبانی (رساها)**

یکی دیگر از ابهاماتی که مقررات جمهوری اسلامی ایران در حوزه تفتیش با آن مواجه است، عدم شفافیت در حدود اختیارات پلیس با ارائه‌دهندگان خدمات دسترسی و خدمات میزبانی است؛ زیرا در قانون آیین دادرسی کیفری صرفاً ارائه‌دهندگان خدمات میزبانی داخلی و ارائه دهندگان خدمات دسترسی را مشمول الزام به نگهداری حداقل ۶ ماه از داده‌ها، پس از خاتمه اشتراک دانسته است؛ بدون آنکه نسبت به نوع داده‌ها، الزامات کنترلی و حفاظتی ارائه دهندگان خدمات موصوف یا تعیین ضمانت اجرای تخلف از این تعهد تصریح شده باشد. ماده ۲۴ آیین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیکی تفتیش و توقیف ادله الکترونیکی، ضابطین را صرفا منوط به درخواست تفتیش و توقیف داده‌های الکترونیکی و ذکر دلایل ضرورت تفتیش و توقیف ، تعیین زمان تقریبی لازم برای تفتیش و توقیف و غیره نموده است و این اساسا بر اقدام پلیس در فرایند بعد از وقوع جرم دلالت می‌نماید و پلیس اختیارات کافی و لازم برای ارتباط و اشراف بر فعالیت ارائه‌دهندگان خدمات الکترونیکی در مرحله قبل از وقوع جرم و اقدامات پیشگیرانه ندارد و توان عملیاتی و اشراف آن چالشی و تصمیمات آن دچار تردید قرار می‌گیرد. دیگر مقررات موجود در

این زمینه که ضوابط و آیین‌نامه‌های مصوب شورای عالی انقلاب فرهنگی است نیز به مسأله پلیس پرداخت نکرده و چنانچه تقریر شد، صرفاً اختیار را به وزارت پست، تلفن و تلگراف (وزارت ارتباطات) تفویض نموده که آن هم با حکم مرجع قضایی، اطلاعات را در اختیار وزارت اطلاعات (و نه نیروی پلیس) قرار دهد.

## بحث و نتیجه گیری

این پژوهش با هدف شناسایی چالش‌های پلیس ایران در تفتیش و توقیف داده و سامانه در پیشگیری وکشف جرم انجام پذیرفت. پلیس در مقام ضابط و فرماندهی انتظامی کشور به عنوان نیروی امنیتی که وظیفه برقراری نظم و امنیت اجتماعی را به عهده دارد، از یک سو وظیفه تضمین بخش مهمی از حقوق شهروندی، مانند حفاظت از جان و مال و حقوق و امنیت شهروندان را متقبل می‌شود و از سوی دیگر، به هنگام انجام وظایف خود، بنا به ارتباط مستقیم با شهروندان، ممکن است اقداماتی صورت دهد که به حق یا ناحق، به عنوان تضییع حقوق شهروندی تلقی گردد. قسمت عمده دغدغه پلیس با شهروندان، در ایفای نقش پلیس به عنوان ضابط قضایی بروز می‌کند. حقوق شهروندی شخصی که به عنوان متهم در اختیار پلیس قرار می‌گیرد، محل چالش است. از یک سو، متهم و حتی مجرم، دارای حقوق ویژه‌ای است که برآمده از حقوق شهروندی است. از سوی دیگر، متهم ممکن است مجرم نباشد و نمی‌توان به صرف اتهام شخص، حقوق شهروندی وی را نادیده‌گرفت .

نتایج این پژوهش بیانگر آن است که یکی از چالش‌های ضابطین پلیس، ابهامات و تداخل وظایف آن در تفتیش و توقیف ادله برای پیشگیری و کشف جرم، «چالش‌های پیرامون حریم خصوصی اشخاص» است. چرا که پلیس در هنگام اقدامات مرتبط با ضابطان، در تفتیش و توقیف ادله در فضای سایبر یا کسب اطلاعات باید تمامیت و محرمانگی داده‌ها را هم به‌صورت قانونی و هم به‌صورت عملی رعایت کند. محتوای داده‌های ارتباطی یا الکترونیکی باید بدون نظارت و پایش به دست گیرنده برسد. بدین‌ترتیب در راستای حمایت از حریم خصوصی اشخاص، اقداماتی نظیر کنترل، شنود، ضبط و ... ممنوع گردیده است. چالشی که در این راستا متوجه پلیس بوده این است که اگر پلیس برای انجام وظایف خود در دو مرحله پیشگیری و کشف جرایم در اقداماتی نظیر تفتیش و توقیف اختیار عمل نداشته باشد، در عمل مجرمانی که می‌توان آنان را از رهگذر آثار و پیشینه‌های الکترونیکی شناسایی کرد، از اجرای عدالت به دور خواهند ماند. بنابراین چنانچه گردآوری و پردازش داده‌ها از سوی پلیس از جمله برای منافع عمومی، امنیت ملی، دفاع ملی، مبارزه با جرایم سازمان یافته یا تروریسم اجتناب‌ناپذیر باشد، اساساً رضایت شخص ذینفع نباید ضرورت داشته باشد.

بدین‌ترتیب می‌توان نتیجه گرفت که تفتیش و توقیف در محیط سایبر همانند محیط فیزیکی جامعه نیست. زیرا این اقدام مستلزم دارا بودن ابزار و دسترسی به زیرساخت‌هایی است تا بتواند پلیس را در نظارت و کنترل در فضای مجازی یاری کند. درست است که پلیس به بانک‌های اطلاعاتی موجود در کشور همچون ثبت احوال، گذرنامه، تشخیص هویت، سازمان زندان‌ها، راهنمایی و رانندگی، سامانه ۱۱۸، سیستم قضایی و تشخیص هویت دسترسی دارد، ولی این دسترسی از آنجایی که بعد از شناسایی مظنون و آی پی[1] او کاربرد دارد، در فضای سایبر که اولا: متهم قابل شناسایی نیست و اقدامات صورت گرفته از سوی پلیس، قبل از شناسایی مرتکب است و ثانیا: حتی بعد از پیدا کردن یکی از ظرفیت‌های دسترسی به مرتکب همچون نام، شماره تلفن و یا سایر اطلاعات جزئی دیگر احتمال دارد وی با مشخصات غیرحقیقی و هویت جعلی به شبکه‌های ارتباطی ورود کرده باشد، دردی را درمان نمی‌کند و در این زمان پلیس نیازمند دستیابی به ابزارهای پیشرفته و زیرساخت‌هایی است تا بتواند نسبت به شناسایی مرتکب اقدام کند. پلیس در این راستا یکی از مراجع ذی‌صلاح است. به عبارت دیگر مراجع دیگری همچون وزارت ارتباطات و فن‌آوری که از دسترسی به سرورها و پایگاه‌های داده بهره‌مند هستند، می‌توانند اقدامات لازم را در زمینه پایش فضای سایبری چه در حوزه پیشگیری و چه در حوزه تعقیب و تحقیق و کشف جرم انجام دهند و پلیس را در پیشگیری و کشف جرم در حوزه تفتیش و توقیف داده و سامانه یاری رساند.

1 . Internet Protocol (ip)

از سوی دیگر عملاً اختیارات پلیس در این حد نیست که بتواند در فضای سایبر اشخاص ورود کند. زیرا در حال حاضر تا شکایتی صورت نگیرد مراجع قضایی و مراکز مربوطه، اجازه دخالت به پلیس را نمی‌دهند. بنابراین پلیس صرفاً بخشی از مراجع ذیصلاح است که نقش همکاری دارد و به تنهایی و بدون در اختیار گذاشتن امکانات لازم نمی‌تواند نسبت به رفع تمام امور اقدام کند. در اینجا می‌توان این‌گونه نتیجه‌گیری کرد با توجه به نظریه خطر، از آنجا که شرکت‌های ارائه کننده خدمات (آی اس پی) [1] ملزم به پیشگیری و نظارت بر کاربران خود هستند و این شرکت‌ها موظفند حداقل نسبت به فعالیت کاربران خود در این محیط جرم‌زا، کنترل لازم را داشته باشند و نسبت به تغییرات در داده‌های جرم انگاری شده که از سوی کاربران ایجاد می‌شود اقدام کنند. زیرا در اختیار داشتن گلوگاه ارتباطی کاربران با دنیای مجازی از اهمیت بسیار زیادی برخوردار است و متصدیان آن از اختیار عمل فراوانی برخوردارند. از سوی دیگر اگر قصد هرگونه سوءاستفاده وجود داشته باشد، هم از لحاظ کیفی و هم از لحاظ کمی بیش از همه کشف آن برای ارائه‌کنندگان خدمات میسر است و به راحتی می‌توانند انواع بسیاری از داده‌های الکترونیکی خصوصی در مکالمات دونفره و نیمه خصوصی در شبکه‌های اجتماعی افراد را در مقیاس بالا جمع‌آوری کنند و نسبت به سایرین دارای محدودیت فنی و نیروی انسانی متخصص نیستند. این شرکت‌ها درباره کلیه کاربران خود اطلاعات ارزشمندی دارند که بخش عمده‌ای از آن ماهیت خصوصی دارند و آنها حق ندارند بدون مجوز قانونی یا رضایت صاحب اطلاعات مبادرت به افشای آنها کند. زیرا این وضعیت حساس و تعیین‌کننده هرگز مجوز عمل خودسرانه و تعرض‌آمیز را صادر نمی‌کند. خدمات دهندگان صرفاً موظفند فضای درخواستی را با رعایت استانداردهای فنی مقرر در اختیار متقاضیان قرار دهد و نسبت به نوع فعالیتی که متقاضی در آن فضا انجام می‌دهد حق هیچ‌گونه دخالتی ندارد.

بنابراین به طور کلی می‌توان گفت در تطبیق این وضعیت با محدودیت‌های وارد شده به اختیارات پلیس ایران از حیث تبعیت از مقام قضایی، و یا اقدامات محدود به احراز فوریت و ضرورت برای تفتیش یا توقیف داده و سامانه‌ها، عملا به جهت عدم شفافیت و جامعیت حقوق اشخاص موضوع داده دچار چالش می‌گردد.

چرا که نمی‌توان گفتمان و درک مشترک از عباراتی مانند ظن قوی، احراز فوریت و ضرورت بین ضابطین و مقام قضایی ایجاد کرد. همچنین از سوی دیگر به جهت عدم پیش‌بینی مقررات افتراقی برای تفتیش ادله شهود و بزه‌دیدگان و ضعف مقررات لازم در حمایت از حریم خصوصی اشخاص ثالث و بزه دیده در فرایند جمع‌آوری دلایل الکترونیکی برای ضابطین چالش‌های حقوقی و کیفری ایجاد می‌گردد و بعضا پرونده کیفری یا حقوقی جدیدی علیه ضابطین گشوده می‌شود. همچنین نبود مرجع مشاوره فنی و مقررات افتراقی برای داده‌های رمزنگاری شده و مقررات شفاف پیرامون تفتیش پیشگیرانه و کشف داده‌ها در بستر قوانین، مشکلات پلیس را دو چندان می‌نماید.

نتایج این مطالعه با یافته‌های (Taghi Zadeh & Kosha,2022). در توجه به ویژگی‌های جرایم سایبری و ضرورت ایجاد تحول در سیاست‌گذاری‌ها و تغییر در برنامه‌ریزی‌های مقابله جرائم سایبری، با یافته‌های Tabrizi , Aalipour & Elahi (Menesh,2022) در ضرورت اصل تناسب در توقیف داده و سامانه با جرم، با یافته‌های( Moradi Haqgo, Shamlou & Saibani,2022) در چالش‌های صلاحیت منفعل در رسیدگی به جرایم سایبری، با یافته‌های (Jaafari Langroudi,2016) در رابطه با ضرورت رویکرد افتراقی در جرائم سایبری هماهنگی و همسویی دارد. همچنین نتایج این مطالعه با نتایج تحقیقات (Ashawa and et al,2024) در رابطه با مشکلات پزشکی قانونی دیجیتال در حفاظت از داده‌ها، مالکیت و مرزهای قضایی، یافته‌های(Baraz & Montasari,2023) در خصوص چالش‌های مجریان قانون در جرائم رایانه‌ای، با نتایج تحقیقات (Rahiminejad,2023) در رابطه با اثر دیجیتالی شدن بر قانون صلاحیت اجرایی، نتایج مطالعات (Hasan,2023) در خصوص ایجاد مبانی قانونی برای پیشگیری و تعقیب جرایم دیجیتال و همچنین با یافته‌های (Khater,2023) و Ngcece & (Mkhize,2023) در رابطه با ضرورت تلاش‌های بین المللی برای تقویت مبارزه با تروریسم سایبری و ایجاد یک معاهده قانونی الزام‌آور در این زمینه و لزوم مشارکت و همکاری همه جانبه همه سهامداران مختلف از جمله دادستان‌ها و قوه قضاییه، آژانس‌های

1. Internet Service Provider (isp)

امنیتی خصوصی و ارائه دهندگان خدمات (ارائه دهندگان اینترنت)، و سایر ذینفعان در مقابله با جرایم سایبری، هماهنگی و همسویی دارد.

**پیشنهادها؛**

با عنایت به یافته‌ها ونتایج به دست آمده، پیشنهادهای ذیل به صورت کاربردی ارائه می‌شوند:

- وظایف ضابطین در خصوص درجه اهمیت جرم ارتکابی در حوزه ادله الکترونیک به طور شفاف در آیین‌نامه‌ای مجزا با عنوان «شرایط و ضوابط ضبط ادله الکترونیکی توسط ضابطین» پیش‌بینی شود.

- پیشنهاد می‌گردد؛ با توجه به سرعت و حجم وقوع جرایم رایانه‌ای همانند جرایم مشهود، اختیارات پلیس ایران در خصوص اجرای قوانین گسترش یابد.

- دستورالعمل‌ها، توصیه‌نامه‌ها یا معیارها توسط یک مرجع واحد که هدف آن تسهیل انطباق تفتیش داده‌های شخصی با مقررات حفاظت از داده‌ها و رعایت حریم خصوصی باشد، به طور شفاف و با ذکر مصادیق قانونی تعریف و تبیین شوند.

- وظایف پیشگیرانه و وظایف نظارتی و کنترلی ضابطین بر داده‌ها و سامانه‌های الکترونیکی پلیس به طور صریح در خصوص جلوگیری از ارتکاب جرائم رایانه‌ای در قانون مشخص شود.

- با توجه به نبود دادسرا و دادگاه تخصصی جرایم رایانه‌ای در استان‌ها پیشنهاد می‌گردد؛ ساختارهای قضایی جهت رسیدگی افتراقی به جرائم رایانه‌ای در کلیه استان‌ها ایجاد گردد.

**سپاس گزاری:**

در پایان نگارش این مقاله از اعضای هیئت علمی دانشگاه علوم انتظامی امین که ما را در انجام این پژوهش یاری نموده اند تشکر و قدردانی می‌گردد.

## References:

Ashawa, M., Mansour, A., Riley, J., Osamor, J., & Owoh, N. P. (2024). Digital Forensics Challenges in Cyberspace: Overcoming Legitimacy and Privacy Issues Through Modularisation. Cloud Computing and Data Science, 140-156. https://ojs.wiserpub.com/index.php/CCDS/article/view/3845

Baraz, A., & Montasari, R. (2023). Law Enforcement and the Policing of Cyberspace. In Digital Transformation in Policing: The Promise, Perils and Solutions (pp. 59-83). Cham: Springer International Publishing.

Casey, Owen (2008). Digital reasons and computer crime; Legal Science, Computers and Internet (Translators: Amir Hossein Jalali Farahani and Ali Shayan), first edition, Tehran: Selsbeil Publications. [In Persisn]

Dezbani, M. H. (2005). The beginning of computer-cyber crimes, informatics newsletter, number 93. [In Persisn]

Fazli, M. (2012). Criminal liability in cyberspace, second edition, Tehran: Khorsandi Publications. [In Persisn]

Hasan, M. S. (2023). Application of Fundamental Rights in Cyberspace: A Dissection of the Digital Security Act. Available at SSRN 4412447.

Jaafari Langroudi, M. J. (2022), expanded on legal terminology. Tehran: Ganj Danesh Publications, [In Persisn]

Jalali Farahani, A. H. (2007). Advantages and limitations of cyberspace in the fields of freedom of expression, freedom of information and privacy. Justice Journal, 71(59), 61-100. [In Persisn]https://www.jlj.ir/article_

Jovan Jafari, A. R. (2016), cyber crimes and the differential approach of criminal law with a look at the Islamic Penal Code section of computer crimes. Master's thesis, University of Mashhad. [In Persisn]

Karami, D. (2015). Differential criminal policy in cyber crimes with an emphasis on Iranian criminal law, Master's thesis, University of Qom. [In Persisn]

Kelsen, Hans (2020). The law of the United Nations, London, 5th edition, Stevens Press.

Kubben, P., Dumontier, M., & Dekker, A. (2019). Fundamentals of clinical data science.

Khater, M. H. (2023). International Perspective on Securing Cyberspace Against Terrorist Acts. International Journal of Sociotechnology and Knowledge Development (IJSKD), 15(1), 1-11. https://www.igi-global.com/article/international-perspective-on-securing-cyberspace-against-terrorist-acts/318706

Mirfallah, S.M. (2015). FATA police tactics in detecting cyber crimes, Master's thesis, Payam Noor University, Tehran province. [In Persisn]

Moradi Haqgo, F., Shamlou, B., & Saibani, A.R. (2022). Passive jurisdiction in dealing with cybercrimes: conditions; Challenges and consequences. Police Criminology Research, 3(6), 163-184. [In Persisn]doi: 10.22034/cr.2022.1266426.1060

Ngcece, S., & Mkhize, S. M. (2023). An Exploratory Study of the South African Police Services (SAPS) Systems in Combating Cybercrime. In Cybercrime and Challenges in South Africa (pp. 159-175). Singapore: Springer Nature Singapore.

Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. Law, Innovation and Technology, 10(1), 40-81. https://www.tandfonline.com/doi/pdf/10.1080/17579961.2018.1452176

Pournajafi, L., Fakhr, H. & Pourgahermani, B. (2022). Refining the cyberspace as a crime or a tool to prevent it? Research paper on criminal law. 2(3), 163-187 [In Persisn] doi: 10.22124/jol.2022.20840.2214

Rahiminejad, I. (2023). Basic challenges of crime prevention rights in Iran. Research Journal of Criminal Law, 14(1), 115-89. [In Persisn]doi: 10.22124/jol.2022.21908.2268

Rathmell, A., & Valeri, L. (2018). Handbook of legislative procedures of computer and network misuse in EU countries, Study for the European Commission Directorate General Information Society. Cambridge: Rand Europe.

Ryngaert, C. (2023). Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts. German Law Journal, 24(3), 537-550. DOI: https://doi.org/10.1017/glj.2023.24

Tabrizi, S., Aalipour, H., Elahi Menesh, M.R. (2022). The principle of proportionality in the seizure of data and the system in the criminal process. Justice Journal, 86(117), 131-152. [In Persisn] https://www.jlj.ir/article245408.pdf

Taghi Zadeh, M., & Kosha, J. (2022). the effectiveness of traditional police powers in detecting transnational cyber crimes, International Police Studies Quarterly, 13(52), 55-78 [In Persisn] doi: 10.22034/interpol.2023.1270640.1303 http://interpol.jrl.police.ir/article.pdf

Thomas, M. Chen & Davies,C. (2016), A Brief Description of Electronic Attacks, Deputy Legal Affairs and Majlis Naja, Applied Research Center, [In Persisn]

Winn, Jane K. & Wright Benjamin, (2011), Law of Electronic Commerce, Fourth Edition, Aspen Law & Business Supplement.

**استناد به این مقاله:**
درویشی، صیاد و رضایی، محسن (۱۴۰۳)، « چالش‌های پلیس ایران در تفتیش و توقیف داده و سامانه در پیشگیری وکشف جرم »، **پژوهشنامه حقوق کیفری**، دوره ۱۵، پیاپی ۲۹، صص. ۸۵-۹۸. DOI: 10.22124/jol.2024.25877.2415