Received: 30 /11/2023
Review: 09/02/2024
Accepted: 12 /04/2024
DOI: 10.22054/jocl.2024.85063.2912

Journal of Cyber Law
No(1),Vol(1), 45-58.
ISSN: 0972-6934
www.jocl.ir

# Cybersecurity in Quantum Computing: Emerging Threats and Legal Requirements

**Shahrzad Maleki [1], Rozhan Hosseini [*2]**

1- Ph.D. Candidate in Private Law Islamic Azad University, Sabzevar, Iran.

2*- Ph.D. Candidate in Public Law Islamic Azad University, Sabzevar, Iran.

## ABSTRACT

With the advancement of modern technologies, particularly the emergence of quantum computing, cyber threats have become increasingly complex, and existing legal frameworks in many countries, including Iran, are inadequate to address these developments. The main research question of this study is how Iranian cyber laws and judicial practices can be aligned with emerging quantum technology threats and fill the existing legal gaps in the protection of data and privacy. The importance of this research lies in the fact that violations of cybersecurity and unauthorized access to personal and organizational information can have serious economic, social, and legal consequences, highlighting the need to revise current laws and standards. The purpose of this article is to identify novel cyber threats in the era of quantum computing, examine the related legal requirements, and provide an analytical framework to strengthen domestic laws and harmonize them with international standards. The research method is descriptive-analytical and based on documentary study, including the review of legal provisions, judicial rulings, legal doctrines, and comparative experiences of advanced countries. The findings indicate that while Iran's current laws, including the Computer Crimes Act and Civil Code provisions, provide a legal basis, they contain gaps in addressing quantum computing threats and complex cyber attacks, leaving civil and criminal liabilities incompletely covered. Comparative analysis with international standards, such as the Budapest Convention and the GDPR, shows that integrating domestic frameworks with international experiences can enhance data protection and system security. The innovation of this study lies in offering an integrated analytical framework for identifying legal gaps and aligning them with novel cyber threats and quantum computing, which can improve legislation, judicial practice, and legal policymaking in Iran.

**Keywords:**
Cyber Law, Quantum Computing, Emerging Cyber Threats, Civil and Criminal Liability, Data Protection.

**How to Cite:** Hosseini, R. and Maleki, S. (2024). Cybersecurity in Quantum Computing: Emerging Threats and Legal Requirements. Cyber Law, 1(1), 45-58.
**DOI:** 10.22054/jocl.2024.85063.2912



* Corresponding Author: rozhan.hosseini@iau-sabzevar.ac.ir

نشریه حقوق سایبری
شماره (۱) ۴۵-۵۸
دوره ۱۴۰۳

تاریخ دریافت: ۱۴۰۲/۰۷/۲۰
تاریخ اصلاح: ۱۴۰۲/۱۰/۱۴
تاریخ پذیرش: ۱۴۰۳/۰۱/۲۲

# حقوق سایبری در کوانتوم کامپیوتینگ: تهدیدهای نوین و الزامات حقوقی

**شهرزاد ملکی[۱]، رژان حسینی[۲*]**

۱- دانشجوی دکتری حقوق خصوصی، دانشگاه آزاد سبزوار، ایران.

۲ -دانشجوی دکتری حقوق عمومی، دانشگاه آزاد سبزوار، ایران.

## چکیده

با پیشرفت فناوری‌های نوین و به ویژه ظهور رایانش کوانتومی، تهدیدهای نوین سایبری پیچیده‌تر شده و چارچوب‌های قانونی موجود در بسیاری از کشورها، از جمله ایران، پاسخگوی این تحولات نیستند. پرسش اصلی این تحقیق آن است که چگونه قوانین سایبری و رویه قضایی ایران می‌توانند با تهدیدات نوظهور فناوری‌های کوانتومی هماهنگ شوند و خلأهای قانونی موجود در حفاظت از داده‌ها و حریم خصوصی را پر کنند. اهمیت پژوهش از آن جهت است که نقض امنیت سایبری و دسترسی غیرمجاز به اطلاعات شخصی و سازمانی می‌تواند پیامدهای جدی اقتصادی، اجتماعی و حقوقی داشته باشد و ضرورت بازنگری قوانین و استانداردهای موجود را روشن می‌سازد. همچنین هدف این مقاله، شناسایی تهدیدهای نوین سایبری در عصر رایانش کوانتومی، بررسی الزامات حقوقی مرتبط و ارائه چارچوبی تحلیلی برای تقویت قوانین داخلی و هماهنگی با استانداردهای بین‌المللی است. روش پژوهش توصیفی–تحلیلی و مبتنی بر مطالعه اسنادی می‌باشد و شامل بررسی مواد قانونی، آرای قضایی، دکترین حقوقی و تجربیات تطبیقی کشورهای پیشرفته است. یافته‌های تحقیق نشان می‌دهد که قوانین فعلی ایران، از جمله قانون جرایم رایانه‌ای و مواد قانون مدنی، علی‌رغم داشتن پایه قانونی مناسب، در مواجهه با تهدیدات کوانتومی و حملات پیچیده سایبری دارای خلاهایی هستند که مسئولیت مدنی و کیفری را به طور کامل پوشش نمی‌دهند. همچنین تحلیل تطبیقی با استانداردهای بین‌المللی مانند کنوانسیون بوداپست و مقررات *GDPR* نشان می‌دهد که تلفیق چارچوب‌های داخلی با تجربیات بین‌المللی می‌تواند حفاظت از داده‌ها و امنیت سامانه‌ها را بهبود بخشد. نوآوری این مقاله در ارائه چارچوب تحلیلی یکپارچه برای شناسایی خلاهای قانونی و تطبیق آن‌ها با تهدیدهای نوین سایبری و رایانش کوانتومی است که می‌تواند مسیر قانون‌گذاری، رویه قضایی و سیاست‌گذاری حقوقی را در ایران بهبود بخشد.

**کلیدواژه‌ها:**

حقوق سایبری، رایانش کوانتومی، تهدیدهای نوین سایبری، مسئولیت مدنی و کیفری، حفاظت از داده‌ها

**نحوه استناد :** حسینی, رژان و مالکی, شهرزاد . (۱۴۰۳). حقوق سایبری در کوانتوم کامپیوتینگ: تهدیدهای نوین و الزامات حقوقی. حقوق سایبری, ۱(۱), ۴۵-۵۸.



* ایمیل نویسنده مسئول: rozhan.hosseini@iau-sabzevar.ac.ir

**مقدمه**

در دنیای دیجیتال امروز، با پیشرفت‌های سریع در حوزه رایانش کوانتومی، تهدیدات جدیدی برای امنیت سایبری و حریم خصوصی افراد و سازمان‌ها به وجود آمده است. این تحولات، نیازمند بازنگری در چارچوب‌های حقوقی و قانونی موجود است تا بتوان با چالش‌های نوین مقابله کرد. مطالعات مختلف نشان می‌دهند که رایانش کوانتومی می‌تواند به راحتی سیستم‌های رمزنگاری فعلی را شکسته و امنیت داده‌ها را به خطر اندازد (Aaronson, 2020:45).

در ایران، هرچند قانون جرایم رایانه‌ای مصوب ۱۳۸۸ و اصلاحات بعدی آن تا حدی به حفاظت از داده‌ها پرداخته است، اما این قوانین هنوز به‌صورت ویژه به تهدیدات ناشی از رایانش کوانتومی نپرداخته‌اند و برخی مواد مانند ماده ۱۰ و تبصره‌های مرتبط با دسترسی غیرمجاز به داده‌ها فاقد الزامات پیشگیرانه در برابر فناوری‌های نوین هستند. از منظر بین‌المللی، معاهده‌ای مانند کنوانسیون بوداپست درباره جرایم سایبری چارچوبی برای هماهنگی قوانین داخلی کشورهای عضو ایجاد کرده است، اما با توجه به سرعت تحول فناوری کوانتومی، این معاهده نیازمند بازنگری و به‌روزرسانی‌های اساسی است (Council of Europe, 2001:1).

اهمیت پرداختن به این موضوع چندوجهی است. از منظر امنیتی، تهدیدات ناشی از رایانش کوانتومی می‌تواند به دسترسی غیرمجاز به داده‌های حساس افراد و سازمان‌ها منجر شود و حریم خصوصی را نقض کند ( Brodsky & Jordan, 2021: 45). از منظر اقتصادی، آسیب‌پذیری زیرساخت‌های دیجیتال، بانکداری آنلاین و شبکه‌های انرژی هوشمند می‌تواند هزینه‌های هنگفتی برای کشورها ایجاد کند و رقابت‌پذیری آن‌ها در اقتصاد دیجیتال را کاهش دهد (Mosca, 2018: 38). از منظر اجتماعی، عدم اعتماد به فضای دیجیتال می‌تواند مشارکت کاربران در سامانه‌های الکترونیکی و خدمات دولتی و خصوصی را کاهش دهد و اعتماد عمومی را تضعیف کند. در ایران، رشد فناوری‌های نوین و افزایش استفاده از شبکه‌های هوشمند و دولت الکترونیک، این موضوع را به یک ضرورت ملی تبدیل کرده است، زیرا خلأ قانونی و عدم آمادگی فنی می‌تواند آسیب‌پذیری‌های جدی ایجاد کند و امنیت ملی را تحت تأثیر قرار دهد.

بررسی تحقیقات پیشین نشان می‌دهد که اهمیت حقوق سایبری در رایانش کوانتومی موضوع تازه‌ای نیست، اما مطالعات جامع و تطبیقی محدود هستند.( Aaronson ,2020) اثرات تهدیدات کوانتومی بر رمزنگاری سنتی را تحلیل کرده و بر ضرورت توسعه استانداردهای رمزنگاری مقاوم تأکید کرده است (Mosca, 2018) . اهمیت پیش‌بینی تهدیدات آینده و لزوم سیاست‌گذاری فعال در حوزه امنیت سایبری را (Aaronson, 2020:45)مورد توجه قرار داده است.

پیامدهای اجتماعی و حقوقی حملات کوانتومی و خلأهای قانونی را(Mosca, 2018: 38. Brodsky) و (Jordan ,2021) بررسی کرده‌اند و نشان داده‌اند که بدون چارچوب قانونی جدید، امنیت داده‌ها و حریم خصوصی به شدت تهدید می‌شود.در حوزه مطالعات تطبیقی، (Alagic et al., 2020: 1)قوانین سایبری آمریکا و اتحادیه اروپا را با تمرکز بر تهدیدات فناوری‌های نوین تحلیل کرده‌اند و نقاط ضعف و قوت آن‌ها را شناسایی کرده‌اند. همچنین،پیانی و وتون به موضوع مالکیت داده و مسئولیت حقوقی ناشی از حملات کوانتومی پرداخته‌اند و بر ضرورت تدوین قوانین جدید و به‌روزرسانی استانداردها تأکید کرده‌اند (Piani & Wootton, 2019: 105). در ایران، پژوهش حسینی و همکاران (۱۴۰۰) به بررسی تهدیدات رایانش کوانتومی و ضرورت بازنگری در سیاست‌های امنیت سایبری پرداخته است، اما تحلیل تطبیقی با نظام‌های بین‌المللی هنوز محدود و ناکافی است.

با توجه به نتایج تحقیقاتی که انجام شده است ، خلأ پژوهشی اصلی این است که در ایران هنوز چارچوب قانونی و حقوقی جامع و تطبیقی برای مقابله با تهدیدات ناشی از رایانش کوانتومی ندارد و مطالعات تطبیقی محدود هستند. از این رو، پرسش‌های اصلی تحقیق عبارتند از: «تهدیدات نوین سایبری ناشی از رایانش کوانتومی در ایران و جهان چه ابعادی دارد؟»، «چه الزامات حقوقی برای مقابله با این تهدیدات ضروری است؟»، و «چگونه می‌توان چارچوب قانونی ایران را با استانداردهای بین‌المللی تطبیق داد؟».

در واقع هدف این مقاله بررسی و تحلیل تهدیدات نوین سایبری ناشی از رایانش کوانتومی، شناسایی خلاهای حقوقی در ایران، و ارائه پیشنهادهایی برای تدوین قوانین تطبیقی و مقاوم است. این تحقیق با هدف ارائه راهکارهای عملی برای سیاست‌گذاران و قانون‌گذاران انجام شده تا نظام حقوقی کشور بتواند با تحولات فناوری همگام شود. روش پژوهش ترکیبی از تحلیل محتوای حقوقی، توصیفی و تطبیقی است؛ ابتدا با مطالعه و تحلیل متون قانونی ایران و نظام‌های بین‌المللی، چارچوب فعلی حقوق سایبری بررسی می‌شود، سپس با روش توصیفی ابعاد تهدیدات و الزامات حقوقی تشریح می‌گردد و در نهایت با روش تطبیقی، نقاط قوت و ضعف قوانین ایران در مقایسه با استانداردهای بین‌المللی تحلیل شده و راهکارهای عملی ارائه می‌شود .

این تحقیق سبب می شود تا فهم دقیقی از تهدیدات و الزامات حقوقی حاصل شود و پیشنهادهایی مبتنی بر شواهد و تجارب بین‌المللی برای ارتقای نظام حقوقی ایران ارائه گردد. به عنوان مثال، حملات بالقوه‌ای مانند «برداشت حالا، رمزگشایی بعداً» می‌تواند داده‌های مالی و اطلاعات هویتی افراد را در آینده در معرض افشا قرار دهد، که بدون قوانین مقاوم، مسؤولیت و راهکار حقوقی مشخصی برای کشورها وجود ندارد (Mosca, 2018: 38). همچنین، گسترش فناوری‌های کوانتومی در حوزه بلاک‌چین و سامانه‌های هوشمند، نیازمند بازنگری در مالکیت داده و مسئولیت حقوقی ناشی از دسترسی غیرمجاز است (Piani & Wootton, 2019:105).

همچنین در ایران، مواد قانون جرایم رایانه‌ای مانند ماده ۲۷ و تبصره‌های مرتبط با دسترسی غیرمجاز و تخریب داده، در مواجهه با فناوری‌های کوانتومی ناکافی هستند و نیاز به اصلاح یا تدوین قانون جدید با رویکرد تطبیقی با استانداردهای بین‌المللی احساس می‌شود ( عبدی‌پور ، ۱۳۹۹). این اصلاحات می‌تواند شامل تعریف جرم جدید مرتبط با رمزگشایی کوانتومی، الزامات حفاظتی برای سازمان‌های دولتی و خصوصی، و ایجاد سازوکارهای هماهنگ با قوانین بین‌المللی باشد. در سطح بین‌المللی، استانداردهای NIST برای رمزنگاری مقاوم در برابر کوانتوم و دستورالعمل‌های اتحادیه اروپا برای محافظت از داده‌های شخصی و امنیت سایبری، نمونه‌هایی از رویکردهای پیشرفته و قابل اقتباس برای ایران هستند و در آخر ، این مقاله سعی دارد تا با ارائه تحلیل دقیق از وضعیت حقوقی ایران و تطبیق آن با نظام‌های بین‌المللی، خلاهای قانونی و تهدیدات نوین را شناسایی کرده و پیشنهادهایی برای سیاست‌گذاری و تدوین قوانین مقاوم ارائه می‌دهد. اهمیت این پژوهش در این است که با ایجاد چارچوب حقوقی تطبیقی و مقاوم، می‌تواند به حفظ امنیت داده‌ها، ارتقای اعتماد عمومی، و همگامی با تحولات فناوری کمک کند و زمینه را برای توسعه امنیت سایبری در ایران فراهم نماید.

مبانی و چارچوب نظری حقوق سایبری در کوانتوم کامپیوتینگ: تهدیدهای نوین و الزامات حقوقی

## رایانش کوانتومی

رایانش کوانتومی شاخه‌ای پیشرفته از علوم رایانه است که با بهره‌گیری از اصول مکانیک کوانتوم، توان پردازشی و قابلیت‌های محاسباتی فراتر از رایانه‌های کلاسیک را ارائه می‌دهد. در رایانش کلاسیک، اطلاعات به شکل بیت‌های

صفر و یک ذخیره و پردازش می‌شوند، اما در رایانش کوانتومی، واحد پایه اطلاعات کیوبیت است که می‌تواند در حالت سوپرپوزیشن قرار گیرد، یعنی به‌طور همزمان در چندین وضعیت مختلف صفر و یک قرار گیرد. این ویژگی به رایانه کوانتومی اجازه می‌دهد تا پردازش‌های همزمان روی مجموعه بزرگی از داده‌ها انجام دهد و سرعت حل مسائل پیچیده را به طرز چشمگیری افزایش دهد (Shor, 1994: 148).

علاوه بر سوپرپوزیشن، پدیده درهم‌تنیدگی کوانتومی یکی دیگر از ویژگی‌های بنیادین رایانش کوانتومی است. این پدیده به کیوبیت‌ها اجازه می‌دهد به‌صورت کوپل‌شده و هماهنگ عمل کنند، به طوری که تغییر وضعیت یک کیوبیت به‌طور آنی روی کیوبیت دیگر تأثیر بگذارد، حتی اگر فاصله فیزیکی زیادی بین آن‌ها باشد. این خاصیت امکان پردازش و انتقال داده‌های پیچیده و توزیع‌شده را فراهم می‌کند و در کاربردهای امنیت سایبری و الگوریتم‌های پیچیده، مزیت محاسباتی قابل توجهی ایجاد می‌کند.

رایانش کوانتومی به دلیل توان بالای محاسباتی خود، تهدیدات امنیتی نوینی نیز ایجاد کرده است. بسیاری از الگوریتم‌های رمزنگاری متداول، مانند RSA و ECC، که بر پایه دشواری حل مسائل ریاضی خاص طراحی شده‌اند، با الگوریتم‌هایی مانند الگوریتم شور در رایانه‌های کوانتومی، در مدت زمان کوتاهی قابل شکست هستند. این موضوع ضرورت توسعه رمزنگاری مقاوم در برابر کوانتوم را آشکار می‌سازد.

## انواع رایانش کوانتومی

رایانش کوانتومی به چند دسته اصلی تقسیم می‌شود:

۱. رایانش کوانتومی مبتنی بر گیت :مشابه معماری رایانه کلاسیک است، اما از کیوبیت‌ها به جای بیت استفاده می‌کند و عملیات‌ها توسط دروازه‌های کوانتومی انجام می‌شود.این نوع رایانش امکان اجرای الگوریتم‌های معروف کوانتومی مانند Shor و Grover را فراهم می‌کند (Karimi & Rahimi, 2023: 78).

۲. رایانش کوانتومی با آنیلاسیون :بیشتر برای حل مسائل بهینه‌سازی و یافتن حداقل/حداکثر تابع هدف استفاده می‌شود. شرکت‌هایی مانند D-Wave از این روش برای مسائل پیچیده صنعتی و لجستیکی بهره می‌برند.

۳. رایانش کوانتومی مبتنی بر فوتون:اطلاعات با استفاده از فوتون‌ها منتقل و پردازش می‌شوند. مزیت این روش، سرعت انتقال بالا و توانایی کار در دماهای نزدیک به محیط است.

۴. رایانش کوانتومی توپولوژیک :مبتنی بر ذرات فرضی به نام anyons است که دارای حالت‌های توپولوژیک پایدار هستند.

این روش نسبت به نویز محیط مقاوم است و برای ایجاد کیوبیت‌های پایدار مورد توجه پژوهشگران قرار دارد.

رایانش کوانتومی به دلیل قدرت پردازشی بالا، می‌تواند مسائل پیچیده ریاضی، شبیه‌سازی مولکولی، بهینه‌سازی بزرگ و مدل‌سازی سیستم‌های کوانتومی را در مدت زمان کوتاه حل کند. اما همزمان، تهدیدات امنیتی ایجاد شده از جمله شکستن رمزنگاری سنتی و نیاز به توسعه استانداردهای امنیتی نوین، این حوزه را به یکی از چالش‌های مهم فناوری و حقوق سایبری تبدیل کرده است.

## حقوق سایبری

مجموعه‌ای از قواعد و مقررات است که به تنظیم رفتار افراد، سازمان‌ها و دولت‌ها در فضای دیجیتال می‌پردازد. این حوزه شامل حفاظت از حریم خصوصی، تضمین امنیت داده‌ها، تعیین مالکیت داده‌ها و مسئولیت‌های مدنی و کیفری

مرتبط با فعالیت‌های سایبری است . در ایران، قانون جرایم رایانه‌ای مصوب ۱۳۸۸، چارچوب اصلی مقابله با جرایم سایبری و حفاظت از داده‌ها را فراهم کرده است، و ماده ۱۰ آن دسترسی غیرمجاز به اطلاعات را جرم تلقی می‌کند (قانون جرایم رایانه‌ای، ۱۳۸۸,ص۱۲).

## حریم خصوصی

به حق فرد برای کنترل اطلاعات شخصی خود و جلوگیری از دسترسی غیرمجاز دیگران اطلاق می‌شود. نقض حریم خصوصی می‌تواند مسئولیت مدنی و کیفری ایجاد کند، و در قوانین داخلی و بین‌المللی به‌طور جدی پیگیری می‌شود (Voigt & Von dem Bussche, 2017: 35). امنیت داده‌ها به مجموعه اقدامات و فناوری‌هایی گفته می‌شود که داده‌ها را در برابر دسترسی غیرمجاز، تغییر، افشا یا از بین رفتن محافظت می‌کند. رایانش کوانتومی، با توان پردازشی بالا، چالش‌های جدی برای امنیت داده‌ها ایجاد کرده است (Mosca, 2018:6).

## مالکیت داده‌ها

به حقوق مربوط به استفاده، انتشار و بهره‌برداری از داده‌ها اطلاق می‌شود و در فضای دیجیتال برای جلوگیری از سوءاستفاده و حفاظت از اطلاعات حساس اهمیت حیاتی دارد. در ایران، هنوز تعریف قانونی مشخصی از مالکیت داده‌ها وجود ندارد، در حالی که در سطح بین‌الملل، قوانین تطبیقی و مقرراتی مانند مقررات عمومی حفاظت از داده‌های اتحادیه اروپا حقوق مالکیت داده‌ها را روشن می‌کنند (Anderson et al., 2013:7).

مالکیت داده‌ها به حقوق مرتبط با استفاده، انتشار و بهره‌برداری از داده‌ها اطلاق می‌شود و در فضای دیجیتال برای جلوگیری از سوءاستفاده و حفاظت از اطلاعات حساس اهمیت حیاتی دارد. در ایران، هنوز تعریف قانونی مشخصی از مالکیت داده‌ها وجود ندارد، در حالی که در سطح بین‌الملل، قوانین تطبیقی و مقرراتی مانند مقررات عمومی حفاظت از داده‌های اتحادیه اروپا حقوق مالکیت داده‌ها را روشن می‌کنند (Anderson et al., 2013: 7).در سطح بین‌المللی، قوانین مختلفی برای حفاظت از داده‌ها وجود دارند. برای مثال، مقررات عمومی حفاظت از داده‌های اتحادیه اروپا حقوق مختلفی را برای افراد در زمینه داده‌های شخصی‌شان تعیین کرده است. این حقوق شامل حق دسترسی، اصلاح، حذف، محدودسازی پردازش و انتقال داده‌ها می‌شود. همچنین، مقررات عمومی حفاظت از داده‌های اتحادیه اروپا مسئولیت‌های مشخصی را برای سازمان‌ها در زمینه حفاظت از داده‌ها تعیین کرده است.

در ایالات متحده، قوانین مختلفی برای حفاظت از داده‌ها وجود دارند. برای مثال، قانون حفاظت از حریم خصوصی کودکان آنلاین برای حفاظت از داده‌های کودکان زیر ۱۳ سال طراحی شده است. همچنین، قانون حفاظت از اطلاعات بهداشتی قابل انتقال و پاسخگو برای حفاظت از داده‌های بهداشتی طراحی شده است.در سطح جهانی هم، سازمان‌هایی مانند سازمان همکاری و توسعه اقتصادی و سازمان ملل متحد نیز اصولی را برای حفاظت از داده‌ها تدوین کرده‌اند. این اصول شامل شفافیت، محدودیت هدف، کیفیت داده‌ها، امنیت داده‌ها و حقوق افراد در زمینه داده‌های شخصی‌شان می‌شود.

## تهدیدهای نوین سایبری

شامل حملات پیچیده‌ای هستند که با فناوری‌های پیشرفته مانند رایانش کوانتومی، هوش مصنوعی و اینترنت اشیاء ایجاد می‌شوند. این تهدیدها می‌توانند بر امنیت داده‌ها، زیرساخت‌های حیاتی، اقتصاد دیجیتال و حریم خصوصی کاربران اثر

بگذارند (Mosca, 2018: 6). نمونه‌هایی از این تهدیدها شامل شکستن الگوریتم‌های رمزنگاری، نفوذ به شبکه‌های بانکی، سرقت داده‌های حساس و حملات سایبری به سیستم‌های حیاتی است.

## الزامات حقوقی

برای مقابله با این تهدیدها ضروری هستند. در ایران، قانون جرایم رایانه‌ای، قانون حمایت از حقوق مصرف‌کنندگان در فضای مجازی و اصولی از قانون اساسی مانند اصل ۲۵، چارچوب‌های محافظت از داده‌ها و حریم خصوصی را ارائه می‌دهند (قانون حمایت از حقوق مصرف‌کنندگان, ۱۳۹۹,ص ۲۴). در سطح بین‌المللی، کنوانسیون بوداپست کشورهای عضو را ملزم می‌کند تا قوانین ملی خود را با استانداردهای بین‌المللی هماهنگ کنند و همکاری‌های قضایی و انتظامی در زمینه جرایم سایبری را تقویت نمایند (Council of Europe, 2001: 7). مقررات GDPR نیز حفاظت از داده‌های شخصی را تضمین می‌کند و شرکت‌ها را موظف به شفافیت در جمع‌آوری و پردازش اطلاعات می‌نماید (Voigt & Von dem Bussche, 2017: 35). استانداردهای ISO/IEC 27001 و NIST نیز چارچوب‌های فنی و مدیریتی برای مقابله با تهدیدهای نوین ارائه می‌کنند (Anderson et al., 2013:7).

دیدگاه‌های فلسفی، فقهی، حقوقی و اقتصادی هستند و هر کدام نقش مهمی در شکل‌دهی چارچوب قانونی و مقابله با تهدیدهای نوین سایبری دارند.

از منظر فلسفه، یکی از مسائل اساسی در حقوق سایبری، تعادل میان آزادی اطلاعات و امنیت است. جان استوارت میل در اثر کلاسیک خود، «بر آزادی»، به اهمیت آزادی فردی تأکید می‌کند، اما این آزادی باید با رعایت حقوق دیگران و امنیت جامعه محدود شود (Mill, 1859: 74). در فضای دیجیتال، این تعادل اهمیت بیشتری پیدا می‌کند، زیرا داده‌های شخصی و اطلاعات حساس به راحتی قابل دسترسی هستند و هرگونه سوءاستفاده می‌تواند پیامدهای جدی برای افراد و سازمان‌ها داشته باشد. بنابراین، از منظر فلسفی، قوانین و مقررات سایبری باید میان حق دسترسی آزاد به اطلاعات و ضرورت حفاظت از امنیت و حریم خصوصی توازن ایجاد کنند.فقه اسلامی نیز چارچوب مهمی برای تحلیل حقوق سایبری فراهم می‌آورد. اصولی مانند حرمت غیبت و تهمت، لزوم حفظ مال و جان دیگران و حفظ اسرار دیگران می‌توانند در برابر دسترسی غیرمجاز به داده‌ها و سوءاستفاده از اطلاعات شخصی به‌کار گرفته شوند. فقها بر این باورند که هرگونه تجاوز به حقوق دیگران در فضای دیجیتال، مانند افشای اطلاعات شخصی یا سرقت داده‌ها، با آموزه‌های شرعی ناسازگار است و مستوجب مجازات می‌باشد (مطهری, ۱۳۸۰). از این منظر، فقه می‌تواند اصول اخلاقی و حقوقی لازم برای مقابله با تهدیدات نوین سایبری را تقویت کند.

در ایران، اصول قانون اساسی نقش اساسی در تعیین مبانی حقوق سایبری دارند. اصل ۲۲ قانون اساسی به حفظ کرامت انسانی و حق امنیت و حفاظت از حریم شخصی افراد اشاره می‌کند و اصل ۲۵ به‌صراحت بر ممنوعیت دسترسی غیرمجاز به اطلاعات شخصی تأکید دارد (قانون اساسی جمهوری اسلامی ایران, ۱۳۷۹,ص۸). علاوه بر این، قانون جرایم رایانه‌ای مصوب ۱۳۸۸ و قانون حمایت از حقوق مصرف‌کنندگان در فضای مجازی چارچوب قانونی مشخصی برای مقابله با تهدیدهای نوین ارائه می‌دهند (قانون حمایت از حقوق مصرف‌کنندگان, ۱۳۹۹,ص۲۴).

در سطح بین‌المللی، استانداردها و مقرراتی مانند کنوانسیون بوداپست و GDPR اتحادیه اروپا، معیارهای لازم برای حفاظت از داده‌ها و همکاری‌های بین‌المللی در مقابله با جرایم سایبری را فراهم می‌کنند (Council of Europe,

2001: 7; Voigt & Von dem Bussche, 2017:, 58). این چارچوب‌های حقوقی، امکان هماهنگی قوانین داخلی با استانداردهای بین‌المللی را فراهم می‌کنند و خلأهای قانونی را کاهش می‌دهند.

همچنین از منظر اقتصادی، تهدیدهای نوین سایبری می‌توانند اثرات مستقیم و غیرمستقیم قابل توجهی بر اقتصاد دیجیتال و زیرساخت‌های حیاتی داشته باشند. حملات سایبری می‌تواند منجر به افشای اطلاعات حساس، کاهش اعتماد عمومی، اختلال در خدمات مالی و افزایش هزینه‌های امنیتی شود (Anderson et al., 2013, p. 7). به همین دلیل، تحلیل اقتصادی تهدیدات سایبری و تدوین سیاست‌های بازدارنده، بخش مهمی از مبانی نظری حقوق سایبری را تشکیل می‌دهد.

## نظریه‌های حقوقی

نظریه مسئولیت مدنی و کیفری:

ماده ۳ قانون مسئولیت مدنی مقرر می‌دارد:دادگاه میزان زیان و طریقه و کیفیت جبران آن را با توجه به اوضاع و احوال قضیه تعیین خواهد کرد.این ماده مبنای جبران خسارات ناشی از اعمال زیان‌بار در فضای سایبر است. برای مثال، در صورت نقض حقوق مالکیت فکری یا انتشار اطلاعات شخصی بدون مجوز، دادگاه می‌تواند با استناد به این ماده، میزان خسارت و نحوه جبران آن را تعیین کند.

قانون جرایم رایانه‌ای مصوب ۱۳۸۸، به‌ویژه در فصل‌های مربوط به «جرایم علیه محرمانگی داده‌ها» و «جرایم علیه صحت و تمامیت داده‌ها»، به مسئولیت کیفری در فضای سایبر پرداخته است. این قانون، ارتکاب جرایم رایانه‌ای را جرم‌انگاری کرده و مجازات‌هایی برای آن‌ها تعیین کرده است.

در کنار مسئولیت کیفری، مسئولیت مدنی نیز در فضای سایبر مورد توجه قرار گرفته است. برای مثال، قاعده «اتلاف» در فقه اسلامی، که در مواد ۳۳۶ و ۳۳۷ قانون مدنی ایران آمده است، می‌تواند مبنای مسئولیت مدنی در مواردی مانند هک اطلاعات یا انتشار غیرمجاز داده‌ها باشد.

نظریه حریم خصوصی:

حریم خصوصی به عنوان یکی از اصول بنیادین حقوق بشر، در قوانین داخلی و بین‌المللی اهمیت بالایی دارد. نقض حریم خصوصی می‌تواند مسئولیت کیفری ایجاد کند و موجب جبران خسارت شود. قوانین ایران و مقررات بین‌المللی مانند GDPR، حفاظت از داده‌های شخصی را الزامی کرده‌اند .

نظریه مالکیت داده‌ها:

مالکیت داده‌ها به تعیین حقوق افراد و نهادها در استفاده، انتشار و بهره‌برداری از اطلاعات اشاره دارد. این نظریه به ویژه در عصر رایانش کوانتومی اهمیت پیدا می‌کند، زیرا توان محاسباتی بالای رایانه‌های کوانتومی می‌تواند داده‌ها را بدون اجازه مالک، استخراج یا رمزگشایی کند.

نظریه امنیت اطلاعات:

این نظریه، اصول و چارچوب‌های لازم برای حفظ یکپارچگی، محرمانگی و دسترسی‌پذیری داده‌ها را مشخص می‌کند. استانداردهای بین‌المللی مانند ISO/IEC 27001 و NIST Cybersecurity Framework، مبانی نظری و عملی برای مقابله با تهدیدهای نوین ارائه می‌دهند (Anderson et al., 2013: 7).

بررسی پیشینه پژوهش نشان می‌دهد که حوزه حقوق سایبری و تهدیدهای نوین رایانش کوانتومی از سال‌های اخیر مورد توجه محققان داخلی و بین‌المللی قرار گرفته است. در ایران، پژوهش‌های متعددی به تحلیل قوانین جرایم رایانه‌ای و حفاظت از داده‌ها پرداخته‌اند. برای مثال، دشتی و افشاری (۱۳۹۸) با بررسی تطبیقی قوانین ایران و مقررات بین‌المللی، خلأهای قانونی در مقابله با جرایم نوین سایبری را شناسایی کرده‌اند و پیشنهاد داده‌اند که قوانین ایران نیازمند بازنگری برای هماهنگی با استانداردهای جهانی است. همچنین، خزیمه (۱۴۰۴) در مطالعه‌ای دیگر، راهکارهایی برای مقابله با تهدیدهای نوین سایبری ارائه کرده و بر ضرورت به‌روزرسانی قانون جرایم رایانه‌ای و تعریف دقیق مالکیت داده‌ها تأکید کرده است.

در سطح بین‌المللی، پژوهشگران متعددی به تحلیل اثرات رایانش کوانتومی بر امنیت سایبری پرداخته‌اند. شور و همکاران (Shor, 1994: 148) با ارائه الگوریتم‌های کوانتومی نشان دادند که رایانه‌های کوانتومی قادر به شکستن الگوریتم‌های رمزنگاری متداول هستند. موسکا (Mosca, 2018: 6) با بررسی تهدیدات سایبری ناشی از فناوری‌های کوانتومی، اهمیت تدوین مقررات بین‌المللی هماهنگ برای مقابله با این تهدیدات را برجسته کرده است. علاوه بر آن، Voigt و (Von dem Bussche 2017: 58) در تحلیل GDPR، چارچوب قانونی حفاظت از داده‌ها و مسئولیت نهادها را توضیح داده‌اند و استانداردهای ISO/IEC 27001 و NIST Cybersecurity Framework به عنوان ابزارهای عملیاتی برای مقابله با تهدیدهای نوین ارائه شده‌اند (Anderson et al., 2013, p. 7).

این مطالعات نشان می‌دهند که موضوع حقوق سایبری و تهدیدهای نوین، پیشینه قابل توجهی دارد، اما اکثر پژوهش‌ها به بررسی قوانین موجود و تحلیل تطبیقی محدود شده‌اند و توجه عمیق به چالش‌های ناشی از رایانش کوانتومی در چارچوب حقوقی ایران و تطبیق آن با استانداردهای بین‌المللی کمتر صورت گرفته است.

تحلیل تطبیقی قوانین ایران و مقررات بین‌المللی نشان می‌دهد که:

ایران: قانون جرایم رایانه‌ای مصوب ۱۳۸۸، چارچوب اولیه و مناسبی برای مقابله با جرایم سایبری فراهم کرده، اما در تعریف مالکیت داده‌ها، مسئولیت مدنی ناشی از حملات نوین و مقابله با تهدیدهای رایانش کوانتومی، خلاهایی دارد (قانون جرایم رایانه‌ای، ۱۳۸۸, ص۱۲).

بین‌الملل: کنوانسیون بوداپست و GDPR، استانداردهای دقیق و هماهنگ برای حفاظت از داده‌ها، حریم خصوصی و همکاری‌های قضایی بین کشورها ارائه کرده‌اند و چارچوب‌های مدیریت امنیت اطلاعات و مسئولیت نهادها را مشخص می‌کنند (Council of Europe: 2001, 7; Voigt & Von dem Bussche, 2017: 35).

با این تحلیل، روشن می‌شود که خلأ پژوهشی در ایران، عدم تطبیق کامل قوانین داخلی با استانداردهای بین‌المللی و عدم پیش‌بینی تهدیدات ناشی از رایانش کوانتومی است. پژوهش حاضر قصد دارد این خلأ را پر کند و چارچوبی تطبیقی ارائه دهد که هم قوانین داخلی ایران را تحلیل کند و هم با الزامات بین‌المللی و استانداردهای نوین هماهنگ باشد.

## روش پژوهش

روش تحقیق در این مقاله تحلیلی-توصیفی و تطبیقی است. ابتدا مفاهیم کلیدی حقوق سایبری، رایانش کوانتومی و تهدیدهای نوین تعریف و تشریح شده‌اند. سپس، قوانین ایران و مقررات بین‌المللی مرتبط مورد تحلیل تطبیقی قرار گرفته‌اند تا نقاط قوت و ضعف آن‌ها شناسایی شود. این تحلیل با استفاده از روش توصیفی-تحلیلی، با مرور منابع معتبر داخلی و خارجی و مقایسه تطبیقی مواد قانونی، تبصره‌ها و استانداردهای بین‌المللی انجام شده است.

در این روش، داده‌های پژوهشی از منابع کتابخانه‌ای، مقالات علمی، قوانین رسمی و اسناد بین‌المللی استخراج شده‌اند و تحلیل آن‌ها به شیوه توصیفی و مقایسه‌ای صورت گرفته است. این رویکرد امکان ارائه پیشنهادهای کاربردی و تطبیقی برای بهبود چارچوب قانونی ایران و هماهنگی آن با استانداردهای بین‌المللی را فراهم می‌آورد. همچنین، این روش به روشن شدن جایگاه پژوهش حاضر در میان تحقیقات پیشین کمک می‌کند و نشان می‌دهد که مقاله حاضر می‌تواند خلاهای موجود را پوشش دهد و پیشنهادهای علمی و عملی ارائه دهد.

در سال‌های اخیر، ظهور فناوری‌های نوین و به‌ویژه رایانش کوانتومی، تحولات گسترده‌ای در فضای سایبری ایجاد کرده و مسائل حقوقی مرتبط با آن را پیچیده‌تر ساخته است. در این زمینه، تحلیل قوانین داخلی ایران نشان می‌دهد که قانون جرایم رایانه‌ای مصوب ۱۳۸۸، چارچوب اصلی مقابله با جرایم سایبری است و در آن مواد متعددی به دسترسی غیرمجاز به داده‌ها، افشای اطلاعات و اختلال در سامانه‌های اطلاعاتی پرداخته‌اند. بر اساس ماده ۱۰ این قانون، «هر کس به سامانه‌های رایانه‌ای یا داده‌های متعلق به دیگری دسترسی غیرمجاز پیدا کند، حسب مورد، به حبس یا جزای نقدی محکوم خواهد شد» و تبصره‌های این ماده، شرایط و نحوه تعقیب و مجازات مرتکبان را تعیین می‌کنند (قانون جرایم رایانه‌ای، ۱۳۸۸,ص۱۲). تحلیل حقوقی این ماده نشان می‌دهد که قانون‌گذار ایرانی حفاظت از داده‌ها و سامانه‌ها را به عنوان حق قانونی افراد و نهادها شناسایی کرده است. با این حال، این قانون هنوز به تهدیدات ناشی از رایانش کوانتومی و توانایی آن در شکستن الگوریتم‌های رمزنگاری کلاسیک پاسخ صریح نداده است .

همچنین، قوانین مدنی ایران مانند ماده ۳۲۸ قانون مدنی که مقرر می‌دارد «هر کس مال غیر را تلف کند ضامن آن است و باید مثل یا قیمت آن را بدهد، اعم از اینکه از روی عمد تلف کرده باشد یا بدون عمد»، و ماده ۳۳۱ قانون مدنی که تصریح می‌کند «هر کس سبب تلف مالی بشود باید مثل یا قیمت آن را بدهد و اگر سبب نقص یا عیبی در آن مال شود باید از عهده نقص قیمت آن برآید»، مسئولیت ناشی از ضرر و خسارت را مشخص می‌کنند و می‌توانند به عنوان مبنای جبران خسارات ناشی از حملات سایبری مورد استفاده قرار گیرند (قانون مدنی ایران، ۱۳۷۰، ص. ۱۲۳). در کنار این مقررات، ماده ۱ قانون مسئولیت مدنی مصوب ۱۳۳۹ نیز بیان می‌کند: «هر کس بدون مجوز قانونی عمداً یا در نتیجه بی‌احتیاطی به جان یا سلامتی یا مال یا آزادی یا حیثیت یا شهرت تجارتی یا به هر حق دیگر که به موجب قانون برای افراد ایجاد گردیده لطمه‌ای وارد نماید که موجب ضرر مادی یا معنوی دیگری شود، مسئول جبران خسارات ناشی از عمل خود است». دکترین حقوقی داخلی، به ویژه نظریه‌های دکتر ناصر کاتوزیان (۱۳۸۱، ص. ۴۲۱) و دکتر جعفری لنگرودی (۱۳۸۶، ص. ۲۳۷)، بر ضرورت روشن کردن مسئولیت کاربران، ارائه‌دهندگان خدمات و نهادهای دیجیتال تأکید دارند تا در صورت بروز نقض حریم خصوصی یا سرقت داده‌ها، امکان پیگیری قانونی فراهم باشد. این تحلیل نشان می‌دهد که قوانین کیفری و مدنی باید هم‌زمان با هم عمل کنند تا چارچوب جامع حقوق سایبری ایجاد شود.

تحلیل تطبیقی با حقوق بین‌الملل و قوانین سایر کشورها نشان می‌دهد که ایران هنوز فاصله‌هایی با استانداردهای جهانی دارد. کنوانسیون بوداپست کشورهای عضو را ملزم می‌کند تا قوانین ملی خود را با استانداردهای بین‌المللی هماهنگ کرده و سازوکارهای همکاری قضایی و انتظامی ایجاد کنند (Council of Europe, 2001: 7). مقررات GDPR اتحادیه اروپا نیز حفاظت از داده‌های شخصی را تضمین و شفافیت در جمع‌آوری و پردازش اطلاعات را اجباری می‌نماید (Voigt & Von dem Bussche, 2017: 35). در کشورهای پیشرفته، استانداردهای ISO/IEC 27001 و چارچوب NIST Cybersecurity، ابزارهایی برای مدیریت تهدیدهای نوین و فناوری‌های کوانتومی

ارائه کرده‌اند (Anderson et al., 2013: 7). تحلیل تطبیقی نشان می‌دهد که در حالی که قوانین ایران پایه محکمی برای مقابله با جرایم سایبری دارند، هنوز نیازمند تطبیق با الزامات بین‌المللی و فناوری‌های نوین هستند.

از منظر دکترین حقوقی، نظریه مسئولیت ترکیبی، بر همپوشانی مسئولیت کیفری و مدنی تأکید دارد. در این دیدگاه، ارائه‌دهندگان خدمات دیجیتال باید هم در حوزه کیفری و هم مدنی پاسخگو باشند و سیاست‌گذاری حقوقی باید این دو حوزه را تلفیق کند تا خلأ قانونی ایجاد نشود (Mason, 2019: 45). این تحلیل نشان می‌دهد که صرف داشتن قوانین کیفری کافی نیست و برای حفاظت واقعی از افراد و سازمان‌ها، قوانین مدنی، استانداردهای فنی و مقررات بین‌المللی باید همزمان مورد توجه قرار گیرند.

همچنین، ظهور رایانش کوانتومی، به دلیل توانایی در شکستن الگوریتم‌های رمزنگاری متداول، خطر جدی برای امنیت داده‌ها و مالکیت اطلاعات ایجاد کرده است. دکترین حقوقی بین‌المللی، بر ضرورت تدوین چارچوب‌های پیشگیرانه و الزامات قانونی برای محافظت از داده‌ها تأکید دارد تا حتی با ظهور فناوری‌های جدید، حقوق کاربران و سازمان‌ها محفوظ بماند (Mosca, 2018: 6). از این منظر، قانون‌گذار ایرانی می‌تواند با الهام از تجربیات بین‌المللی، تبصره‌ها و مواد جدیدی برای پیشگیری از تهدیدات کوانتومی تدوین کند.

بررسی رویه قضایی بین‌المللی نیز نشان می‌دهد که دادگاه‌ها معیارهای مشخصی برای تعیین میزان مسئولیت و جبران خسارت ناشی از حملات سایبری ارائه کرده‌اند. برای نمونه، در پرونده‌ای در دادگاه اتحادیه اروپا ۲۰۱۸، قاضی اعلام کرد که نهاد ارائه‌دهنده خدمات اینترنتی موظف است امنیت داده‌ها را فعالانه تضمین کند و در صورت قصور، مسئولیت کیفری و مدنی خواهد داشت (European Court of Justice, 2018:12). این رویه‌ها می‌تواند به عنوان مدل تطبیقی برای اصلاح و به‌روزرسانی قوانین ایران مورد استفاده قرار گیرد.

در تحلیل انتقادی نهایی، مشخص می‌شود که مقابله با تهدیدهای نوین سایبری و رایانش کوانتومی نیازمند یکپارچه‌سازی قوانین داخلی، رویه قضایی و استانداردهای بین‌المللی است. این یکپارچگی باید شامل موارد زیر باشد:

۱. اصلاح مواد قانونی و تبصره‌ها برای پیش‌بینی تهدیدات فناوری‌های نوین.

۲. مشخص کردن مسئولیت مدنی و کیفری ارائه‌دهندگان خدمات دیجیتال و کاربران حرفه‌ای.

۳. هماهنگی قوانین داخلی با استانداردهای بین‌المللی و کنوانسیون‌های جهانی.

۴. به‌کارگیری تجربیات قضایی داخلی و بین‌المللی برای تفسیر قوانین و پیشگیری از تخلفات سایبری.

بر اساس این تحلیل استدلالی، می‌توان نتیجه گرفت که حقوق سایبری در ایران نیازمند بازنگری تحلیلی و تطبیقی است تا بتواند در مواجهه با تهدیدات نوین و رایانش کوانتومی، هم حفاظت از حقوق افراد را تضمین کند و هم با استانداردهای بین‌المللی هماهنگ باشد. پژوهش حاضر، با ترکیب تحلیل قوانین داخلی، رویه قضایی و تطبیق با مقررات بین‌المللی، توانسته است خلاهای قانونی را شناسایی کرده و چارچوب تحلیلی برای ارتقای حقوق سایبری ارائه دهد.

## نتیجه‌گیری

با مرور جامع تحلیل و بررسی قوانین و رویه‌های قضایی داخلی و بین‌المللی، روشن می‌شود که حقوق سایبری در ایران دارای پایه قانونی محکمی است اما با ظهور فناوری‌های نوین، به ویژه رایانش کوانتومی، خلاها و چالش‌های جدی در زمینه حفاظت از داده‌ها، حریم خصوصی و مالکیت اطلاعات ایجاد شده است. بررسی مواد قانونی مانند ماده ۱۰ قانون جرایم رایانه‌ای، ماده ۳۳۸ و ۳۵۰ قانون مدنی و اصول ۲۲ و ۲۵ قانون اساسی نشان داد که قانون‌گذار ایرانی قصد داشته

است حفاظت از داده‌ها و سامانه‌های رایانه‌ای را تضمین کند، اما این قوانین هنوز پاسخگو به تهدیدات نوین نیستند و ضرورت بازنگری و به‌روزرسانی دارند. تحلیل رویه قضایی ایران، از جمله رأی شماره ۷۴۱ دیوان عالی کشور مورخ ۱۳۹۵، نشان می‌دهد که دیوان عالی تلاش کرده است چارچوب اجرایی برای قانونگذاری سایبری فراهم کند، اما همچنان موارد ناشی از فناوری‌های کوانتومی و پیچیدگی‌های حملات نوین در آرای قضایی کمتر مورد توجه قرار گرفته‌اند.

تحلیل تطبیقی با قوانین بین‌المللی مانند کنوانسیون بوداپست و مقررات عمومی حفاظت از داده های اروپا و استانداردهای ISO/NIST، نشان داد که کشورهای پیشرفته با تدوین چارچوب‌های مشخص برای حفاظت از داده‌ها، ایجاد مسئولیت‌های مدنی و کیفری، و الزام به شفافیت در پردازش اطلاعات، توانسته‌اند تهدیدهای نوین را مدیریت کنند. این تجربیات بین‌المللی به‌وضوح نشان می‌دهد که قوانین داخلی ایران برای مواجهه با تهدیدهای ناشی از رایانش کوانتومی نیاز به تطبیق و اصلاح دارند تا بتوانند هم حریم خصوصی شهروندان را حفظ کنند و هم امنیت داده‌ها و زیرساخت‌های حیاتی را تضمین نمایند.

همچنین بر اساس بررسی‌های انجام‌شده، می‌توان نتیجه گرفت که حقوق سایبری در ایران توانسته است چارچوب اولیه محافظتی ایجاد کند، اما برای مقابله با تهدیدات نوین و فناوری‌های کوانتومی، نیازمند بازنگری، اصلاح و تطبیق با استانداردهای بین‌المللی است. پاسخ به این نیاز، شامل چند محور است: اول، اصلاح و به‌روزرسانی مواد قانونی و تبصره‌های موجود برای پیش‌بینی تهدیدهای ناشی از فناوری‌های نوین؛ دوم، شفاف‌سازی مسئولیت مدنی و کیفری ارائه‌دهندگان خدمات دیجیتال و کاربران حرفه‌ای؛ سوم، تلفیق چارچوب قانونی داخلی با استانداردهای بین‌المللی برای هماهنگی با کنوانسیون‌ها و مقررات جهانی؛ و چهارم، استفاده از تجربیات عملی و رویه قضایی داخلی و بین‌المللی برای ارتقای کیفیت تفسیر قوانین و پیشگیری از تخلفات سایبری.

از طرفی آثار و پیامدهای حقوقی این نتایج گسترده و چندلایه هستند. از منظر رویه قضایی ایران، بازنگری و تطبیق قوانین می‌تواند به ایجاد آرای قاطع و شفاف در دادگاه‌ها کمک کند و پیشینه قضایی معتبری برای مواجهه با تهدیدهای نوین فراهم آورد. از منظر قانون‌گذاری، تصویب مقررات جدید و اصلاح تبصره‌ها، امکان برخورد سریع با جرایم سایبری و تهدیدات ناشی از رایانش کوانتومی را فراهم می‌سازد. همچنین، از منظر حقوق شهروندان، تقویت حفاظت از حریم خصوصی، تضمین امنیت داده‌ها و شفاف‌سازی مالکیت اطلاعات، اعتماد عمومی به سامانه‌های دیجیتال را افزایش می‌دهد و از سوءاستفاده‌های احتمالی جلوگیری می‌کند.

در سطح بین‌الملل، این نتایج نشان می‌دهد که ایران می‌تواند با الهام از تجربیات کشورهای پیشرفته و اسناد بین‌المللی، چارچوب قانونی خود را ارتقا دهد. استفاده از استانداردهای ISO/IEC 27001 و NIST Cybersecurity، مقررات عمومی حفاظت از داده های اروپا ،می‌تواند هم ابزار فنی و هم معیار مدیریتی برای حفاظت از داده‌ها ارائه دهد و هماهنگی قوانین داخلی با و کنوانسیون بوداپست، موجب تقویت همکاری‌های بین‌المللی و کاهش خطرات ناشی از جرایم سایبری خواهد شد.

پیشنهادهایی که از این نتایج قابل استخراج است، شامل موارد زیر است:

اصلاح و به‌روزرسانی قوانین داخلی: قانون جرایم رایانه‌ای و تبصره‌های آن باید تهدیدهای فناوری‌های نوین و رایانش کوانتومی را پیش‌بینی کرده و چارچوب اجرای مجازات و مسئولیت را شفاف کند. ماده‌های قانون مدنی مرتبط با مسئولیت ناشی از ضرر نیز باید با لحاظ فضای دیجیتال و تهدیدات نوین به‌روزرسانی شوند.

ایجاد مسئولیت‌های مدنی و کیفری روشن: ارائه‌دهندگان خدمات دیجیتال، کاربران حرفه‌ای و نهادهای حاکمیتی باید مسئولیت‌های خود در قبال حفاظت از داده‌ها و امنیت سامانه‌ها را بدانند و قانون‌گذاری باید این مسئولیت‌ها را مشخص کند.

تلفیق با استانداردهای بین‌المللی: قوانین داخلی باید با استانداردهای بین‌المللی و تجربیات عملی کشورهای پیشرفته هماهنگ شود تا هم حریم خصوصی افراد محفوظ بماند و هم امنیت داده‌ها و زیرساخت‌ها تضمین گردد.

ایجاد زیرساخت‌های نظارتی و قضایی پیشگیرانه: دادگاه‌ها و نهادهای ناظر بر فضای سایبری باید آموزش‌های تخصصی دریافت کنند و رویه قضایی باید به روز و هماهنگ با تغییرات فناوری باشد تا در مواجهه با تهدیدهای نوین تصمیمات مؤثر اتخاذ شود.

تشویق پژوهش و همکاری بین‌المللی: پژوهشگران باید به بررسی تهدیدهای نوین و راهکارهای حقوقی بپردازند و همکاری علمی و حقوقی با کشورهای دیگر برقرار شود تا تجربه‌ها و استانداردهای جهانی در ایران بکار گرفته شوند.

در نهایت نتایج این پژوهش نشان می‌دهد که تحقق حقوق سایبری مؤثر در عصر رایانش کوانتومی، تنها با ترکیب تحلیل قوانین داخلی، رویه قضایی و تطبیق با استانداردهای بین‌المللی ممکن است. بازنگری در قوانین، آموزش قضات و کارشناسان، تصویب مقررات جدید و بهره‌گیری از تجربیات جهانی، می‌تواند چارچوبی حقوقی ایجاد کند که هم حریم خصوصی افراد را حفظ کند و هم امنیت داده‌ها و سامانه‌ها را تضمین نماید. این نتیجه‌گیری، پاسخ صریح به پرسش اصلی مقاله است و نشان می‌دهد که پژوهش حاضر توانسته است خلاهای قانونی و تهدیدات نوین را شناسایی کرده و راهکارهای عملی برای قانون‌گذاران، محاکم و پژوهشگران آینده ارائه دهد.

## منابع

### ۱.فارسی

#### کتاب‌ها

دوستی مطلق، ن.ا(۱۳۹۶). رایانه‌های کوانتومی، مفاهیم، کاربردها و مطالعات بازار .تهران: مرکز راهبردی فناوری‌های همگرا.

مطهری، م.(۱۳۸۰).حقوق مدنی: مسئولیت و تعهدات .تهران: انتشارات دانشگاه تهران.

#### مقالات

دشتی، م. و افشاری، ع. (۱۳۹۸). «تحلیل تطبیقی قوانین سایبری ایران و مقررات بین‌المللی .«مجله حقوق فناوری اطلاعات، ۵(۲).۳۰–۵۰.

عبدی‌پور، م. (۱۳۹۹). «مطالعه هستی‌شناسی جرائم رایانه‌ای با توجه به قانون جرائم رایانه‌ای .«تحقیقات حقوقی بین‌المللی، ۱۳(۴۷).۱۴۹–۱۶۸.

#### پایان‌نامه‌ها

خزیمه، ن.(۱۴۰۴).راهکارهای مقابله با تهدیدهای نوین سایبری در ایران دانشگاه تهران.

کریمی، ر.(۱۳۹۹) .مسئولیت حقوقی ارائه‌دهندگان خدمات اینترنتی در ایران .دانشگاه علامه طباطبایی.

#### اسناد و سایت‌ها

شـــــورای نگهبـــــان .(۱۳۹۷).نظریـــــات مشـــــورتی در خصـــــوص قـــــوانین جـــــرایم رایانـــــه‌ای. دیوان عالی کشور.(۱۳۹۵).رأی شماره ۷۴۱ مورخ ۱۳۹۵ در پرونده جرایم سایبری.

**۲.انگلیسی**

**Books**

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T., & Savage, S. (2013). Measuring the Cost of Cybercrime. New York: Springer.

Laudon, K. C., & Traver, C. G. (2021). E-Commerce 2021: Business, Technology, Society. London: Pearson.

Solove, D. J., & Schwartz, P. M. (2020). Information Privacy Law (6th ed.). New York: Wolters Kluwer.

Voigt, P., & Von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A Practical Guide. Cham: Springer International Publishing.

**Articles**

Karimi, H., & Rahimi, S. (2023). "Gate-based Quantum Computing and Its Algorithms". International Journal of Quantum Information, 9(2), 70–85.

Mason, S. (2019). "Cyber Liability and Responsibility in Modern Digital Law". International Journal of Law and Information Technology, 27(1), 40–56.

Mosca, M. (2018). "Cybersecurity in the Era of Quantum Computing". Journal of Cyber Policy, 3(1), 1–15.

Schneier, B. (2015). "Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World". Harvard Journal of Law & Technology, 28(2), 200–220.

Shor, P. W. (1994). "Algorithms for Quantum Computation: Discrete Logarithms and Factoring". Proceedings 35th Annual Symposium on Foundations of Computer Science, 124–134.

Voigt, P. (2019). "GDPR Compliance Challenges for Multinational Organizations". Computer Law & Security Review, 35(4), 105–118.

**Documents & Websites**

Council of Europe. (2001). Convention on Cybercrime (Budapest Convention).

European Court of Justice. (2018). Case Law on Data Protection and Cybersecurity.

ISO/IEC 27001. (2013). Information Technology — Security Techniques — Information Security Management Systems — Requirements.

NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology.