Legal Studies in Cyberspace

مطالعات حقوقی فضای مجازی

Received: 2025/10/14
Accepted: 2025/11/26
Publish: 2026/01/04
Pages: 86 - 109

ISSN: 2821-126X
https://sanad.iau.ir/journal/cyberlaw :وبگاه مجله

Volume 4, Issue 15, Fall 2025
Article Type: **Research**
DOI: 10.71488/cyberlaw.2026.1230830

Notification of Charges in Cybercrimes: A Comparative Study in Iranian and French Law with Emphasis on Safeguarding the Accused's Rights of Defense

Mohammad Taghi Nafisifar
Department of Law, Go.C., Islamic Azad University, Gorgan, Iran
Gholamreza Golchinrad
Department of Law, Go.C., Islamic Azad University, Gorgan, Iran
Mohaddeseh Sadeghian Lemaraski
Department of Law, Go.C., Islamic Azad University, Gorgan, Iran

Abstract
The rapid development of information technology, the expansion of cyberspace, and the emergence of cybercrimes have created new challenges for legal systems in ensuring the rights of the accused, particularly during the stage of notification of charges. This study provides a comparative analysis of the notification of charges in cybercrimes under Iranian and French law, focusing on its compliance with the principles of fair trial and the protection of the defendant's rights. The research employs a descriptive-analytical and comparative method, drawing on library resources, legislation, judicial precedents, and international legal instruments. Findings indicate that both legal systems formally recognize the principle of informing the accused of charges. However, France, with its structured procedural framework and advanced electronic tools, provides more effective guarantees for implementing this principle. In Iran, the 2013 Criminal Procedure Code emphasizes the necessity of explicit notification. Indeed, weaknesses in electronic infrastructure, lack of specific guidelines for cybercrimes, poor coordination between the Cyber Police and the prosecutor's office, and limited access of the accused to legal counsel weaken defense rights. In France's digital judicial systems, precise standards for electronic notification, mandatory presence of a lawyer from the earliest stages of interrogation, and access to digital case files ensure more effective realization of the principle of notification of charges. The study concludes that strengthening legal and technical safeguards, providing specialized training for judicial authorities, and learning from France's experience can play a vital role in ensuring fair notification of charges and protecting defendants' rights in cybercrime cases in Iran.

Keywords: Notification of Charges, Cybercrime, Right of Defence, Fair trial, Comparative Study of Iranian and French Law

❋Citation (APA): Nafisifar, M,T. Golchinrad, G. Sadeghian Lemaraski, M. (2025). Neurocybernetic Manipulation: From Mental Determinism to the Crisis of Causality and Its Role in Determining Criminal Responsibility. *Cyberspace legal studies, 4(15), 86 - 109*

مطالعات حقوقی فضای مجازی
Legal Studies in Cyberspace
ISSN: 2821-126X
https://sanad.iau.ir/journal/cyberlaw ویگاه مجله:
تاریخ دریافت: ۱۴۰۴/۰۷/۲۲
تاریخ پذیرش: ۱۴۰۴/۰۹/۰۵
تاریخ انتشار: ۱۴۰۴/۱۰/۱۴
صفحه: ۸۶ الی ۱۰۹
دوره ۴ / شماره ۱۵ / پاییز ۱۴۰۴
نوع مقاله: پژوهشی
DOI: 10.71488/cyberlaw.2026.1230830

تفهیم اتهام در جرائم سایبری؛ مطالعه تطبیقی در حقوق ایران و فرانسه با تأکید بر تضمین حقوق دفاعی متهم

محمدتقی نفیسی‌فر
گروه حقوق، واحد گرگان، دانشگاه آزاد اسلامی، گرگان، ایران
غلامرضا گلچین‌راد
گروه حقوق، واحد گرگان، دانشگاه آزاد اسلامی، گرگان، ایران
محدثه صادقیان لمراسکی
گروه حقوق، واحد گرگان، دانشگاه آزاد اسلامی، گرگان، ایران

چکیده

تحولات سریع فناوری اطلاعات، گسترش فضای مجازی و ظهور جرائم سایبری، نظام‌های حقوقی را با چالش‌های نوین در تضمین حقوق متهم، به‌ویژه در مرحله «تفهیم اتهام»، مواجه ساخته است. مقایسه نظام‌های حقوقی ایران و فرانسه می‌تواند ابعاد نظری و عملی مهمی در تضمین حقوق دفاعی متهم آشکار کند. هدف پژوهش حاضر بررسی تطبیقی نهاد تفهیم اتهام در جرائم سایبری در ایران و فرانسه با تأکید بر انطباق آن با اصول دادرسی عادلانه و حقوق دفاعی متهم است. هرچند هر دو نظام اصل آگاهی متهم از اتهام را به رسمیت شناخته‌اند، نظام فرانسه با بهره‌گیری از ساختار منسجم آیین دادرسی و ابزارهای الکترونیکی پیشرفته، ضمانت اجرای مؤثرتری ارائه می‌دهد. یافته‌های پژوهش با استفاده از نظریه «دادرسی منصفانه» و «حق دفاع مؤثر» در اسناد بین‌المللی حقوق بشر و روش توصیفی ـ تحلیلی با رویکرد تطبیقی و منابع کتابخانه‌ای، قوانین و رویه‌های قضایی نشان داد که در ایران، هرچند قانون آیین دادرسی کیفری ۱۳۹۲ بر تفهیم صریح اتهام تأکید دارد، ضعف زیرساخت‌های الکترونیکی، نبود دستورالعمل‌های ویژه برای جرائم سایبری، ناهماهنگی میان پلیس فتا و دادسرا و محدودیت دسترسی متهم به وکیل، حقوق دفاعی را تضعیف می‌کند. در فرانسه، سامانه‌های دیجیتال قضایی، استانداردهای دقیق ابلاغ الکترونیکی، حضور وکیل از نخستین لحظات بازجویی و دسترسی متهم به پرونده دیجیتال، اجرای مؤثر اصل آگاهی از اتهام را تضمین کرده است. نتیجه‌گیری پژوهش نشان می‌دهد که تقویت تضمین‌های قانونی و فنی، آموزش تخصصی مقامات قضایی و بهره‌گیری از تجربیات فرانسه می‌تواند نقش مؤثری در تحقق تفهیم اتهام عادلانه در جرائم سایبری در ایران ایفا کند.

واژگان کلیدی: تفهیم اتهام، جرائم سایبری، حقوق دفاعی متهم، دادرسی عادلانه، تطبیق حقوق ایران و فرانسه.

*استناددهی (APA): نفیسی‌فر، محمدتقی. گلچین‌راد، غلامرضا. صادقیان لمراسکی، محدثه. (۱۴۰۴). تفهیم اتهام در جرائم سایبری؛ مطالعه تطبیقی در حقوق ایران و فرانسه با تأکید بر تضمین حقوق دفاعی متهم. *مطالعات حقوقی فضای مجازی*، ۴(۱۵)، ۸۶ – ۱۰۹

مقدمه

تحولات پرشتاب فناوری اطلاعات و ارتباطات در دهه‌های اخیر، بنیان‌های سنتی جرم‌شناسی و عدالت کیفری را دستخوش دگرگونی‌های عمیق کرده است. ظهور فضای مجازی به‌عنوان محیطی نوین برای تعاملات اقتصادی، اجتماعی و فرهنگی، اگرچه فرصت‌های بی‌سابقه‌ای در حوزه تبادل داده، آموزش، و تجارت الکترونیکی فراهم ساخته، اما در عین حال بستر ارتکاب گونه‌ای جدید از بزهکاری را نیز مهیا کرده است که از آن با عناوینی چون جرائم سایبری یا رایانه‌ای یاد می‌شود. ویژگی فرامکانی، ناشناختگی مرتکبان، و وابستگی این جرائم به زیرساخت‌های فناورانه موجب شده است که نظام‌های حقوقی ملی و بین‌المللی با چالش‌های متنوعی در زمینه کشف جرم، تعقیب کیفری، صلاحیت قضایی، و اجرای احکام روبه‌رو شوند در میان مراحل مختلف دادرسی کیفری، مرحله‌ی تفهیم اتهام جایگاهی بنیادین دارد؛ زیرا نخستین گام در تضمین حقوق متهم و تحقق اصل دادرسی عادلانه به شمار می‌رود. تفهیم اتهام در مفهوم دقیق خود به معنای اعلام رسمی، روشن و مستند اتهام به شخصی است که مظنون به ارتکاب جرم است، همراه با بیان ادله‌ی انتساب اتهام و تبیین حقوق قانونی او در برابر آن. در حقیقت، این نهاد حلقه‌ی ارتباط میان نهاد تعقیب و نهاد دفاع محسوب می‌شود و هرگونه ابهام یا نارسایی در انجام آن می‌تواند موجب نقض اصول بنیادین حقوق بشر از جمله حق دفاع مؤثر، حق دسترسی به وکیل، و حق اطلاع از ماهیت اتهام گردد.

نکتهٔ حائز اهمیت تفاوت و تمایز میان دو مفهوم جرایم سایبری و الکترونیکی است. در این رابطه، جرایم سایبری و جرایم الکترونیکی گاهی به‌جای یکدیگر استفاده می‌شوند، اما واقعیت این است که در این دو مفهوم تفاوت دارند. جرایم سایبری به‌طور خاص به فعالیت‌های مجرمانه‌ای اشاره دارد که از طریق شبکه‌های کامپیوتری و اینترنت انجام می‌شوند، مانند هک، سرقت داده‌ها یا حملات سایبری. جرایم الکترونیکی گسترده‌تر است و شامل هر نوع جرم مرتبط با فناوری‌های الکترونیکی می‌شود، حتی اگر اینترنت دخالتی نداشته باشد، مانند جعل اسناد دیجیتال یا کلاهبرداری با کارت‌های بانکی الکترونیکی. به‌عبارت دیگر، همه جرایم سایبری، جرایم الکترونیکی هستند، اما همه جرایم الکترونیکی، سایبری نیستند (ماکیدوف ، ۲۰۲۳: ۸۳-۸۴).

از طرفی، اهمیت رعایت دقیق تشریفات تفهیم اتهام در جرائم سایبری دوچندان است؛ زیرا این نوع جرائم غالباً از پیچیدگی‌های فنی، گستره‌ی جغرافیایی وسیع، و دشواری در جمع‌آوری و تفسیر ادله‌ی دیجیتال برخوردارند. در چنین شرایطی ممکن است متهم پیش از آن‌که از ماهیت اتهام یا مستندات فنی مربوطه به‌درستی آگاه شود، در معرض تصمیمات قضایی قرار گیرد. بنابراین، اطمینان از اطلاع‌رسانی شفاف، مستند و به‌موقع به متهم، از ارکان اساسی عدالت کیفری در عصر دیجیتال به شمار می‌رود. در نظام حقوقی ایران، هرچند قانون آیین دادرسی کیفری مصوب ۱۳۹۲ به‌صراحت بر ضرورت تفهیم اتهام تأکید دارد، اما اجرای کامل و مؤثر آن در جرایم سایبری با موانعی همچون ضعف زیرساخت‌های فنی، فقدان دستورالعمل‌های تخصصی برای نحوه‌ی تفهیم اتهام در جرائم سایبری، ناهماهنگی میان ضابطان و مراجع قضایی، و نبود رویه‌ی واحد مواجه است. در مقابل، نظام حقوقی فرانسه با بهره‌گیری از پیشینه‌ی طولانی در حمایت از حقوق دفاعی متهم و استفاده از سامانه‌های الکترونیکی یکپارچه برای اطلاع‌رسانی قضایی، توانسته است زمینه‌ی تحقق مؤثر حق اطلاع از اتهام و تسهیل ارتباط میان متهم و وکیل را فراهم آورد. از این‌رو، مطالعه‌ی تطبیقی میان نظام حقوقی ایران و فرانسه در حوزه‌ی تفهیم اتهام در جرائم سایبری، نه‌تنها می‌تواند به شناسایی نقاط ضعف ساختاری و اجرایی نظام دادرسی

ایران بینجامد، بلکه راهگشای ارائه‌ی الگوهای اصلاحی و بومی‌سازی‌شده برای ارتقای تضمین‌های دادرسی عادلانه در مواجهه با جرائم نوین فناوری‌محور نیز خواهد بود.

اهمیت پژوهش حاضر از دو منظر قابل بررسی است. نخست از منظر نظری و حقوقی، زیرا تفهیم اتهام یکی از ارکان بنیادین دادرسی عادلانه و تضمین‌کننده حق دفاع مؤثر است. هرگونه خلأ در این مرحله می‌تواند موجب بی‌اعتباری فرآیند دادرسی و نقض حقوق بشر متهم گردد. دوم از منظر عملی و کاربردی، چرا که در بستر جرائم سایبری، ابزارهای دیجیتال نه تنها وسیله ارتکاب جرم بلکه ابزار دادرسی نیز هستند و هرگونه تأخیر یا خطا در اطلاع‌رسانی اتهام، می‌تواند آثار جبران‌ناپذیری بر حقوق متهم و اعتبار ادله دیجیتال داشته باشد. همچنین در تبیین ضرورت انجام پژوهش کنونی بایستی به چند عامل مهم اشاره نمود:

نخست، نوپایی جرائم سایبری در نظام قضایی ایران و فقدان رویه قضایی مستقر در زمینه نحوه تفهیم اتهام در این دسته از موضوعات؛

دوم، لزوم تطبیق و بهره‌گیری از تجارب کشورهای پیشرو مانند فرانسه در استفاده از سامانه‌های الکترونیکی دادرسی؛

و سوم، نیاز به ارائه راهکارهای عملی برای بهبود نظام اطلاع‌رسانی قضایی و تضمین حقوق دفاعی متهمان سایبری که می‌تواند موجب ارتقای اعتماد عمومی به نظام عدالت کیفری شود.

با این مقدمات، مساعی نویسندگان در پژوهش حاضر بحث و بررسی پیرامون موضوع تفهیم اتهام در جرائم سایبری؛ با تأکید بر تضمین حقوق دفاعی متهم در نظام‌های حقوقی ایران و فرانسه است. بر این اساس، سوال اصلی پژوهش عبارت است از: «نظام‌های حقوقی ایران و فرانسه تا چه میزان در فرآیند تفهیم اتهام در جرائم سایبری، تضمین‌های لازم برای رعایت حقوق دفاعی متهم را پیش‌بینی و اجرا کرده‌اند؟» در ادامه برخی از سوالات فرعی دیگر پژوهش عبارتند از: «آیا سازوکارهای موجود در ایران توان تحقق مؤثر حق آگاهی از اتهام در جرائم سایبری را دارند؟ و در صورت فقدان چنین کارآمدی، چه اصلاحاتی می‌تواند بر اساس الگوی فرانسه پیشنهاد شود؟»، «تفهیم اتهام در جرائم سایبری چه تفاوت‌هایی با جرائم سنتی دارد؟»، «چه چالش‌هایی در اجرای مؤثر تفهیم اتهام در جرایم سایبری در ایران وجود دارد؟»، «نظام حقوقی فرانسه چه سازوکارهایی برای تضمین حق اطلاع از اتهام و حضور وکیل در جرائم سایبری پیش‌بینی کرده است؟» و نهایتا آنکه «چه راهکارهای تقنینی و اجرایی می‌توان برای تقویت نهاد تفهیم اتهام در نظام قضایی ایران پیشنهاد کرد؟»

روش پژوهش حاضر، توصیفی ـ تحلیلی با رویکرد تطبیقی است. داده‌ها از طریق منابع کتابخانه‌ای، قوانین داخلی، آیین‌نامه‌ها، آراء محاکم، و اسناد بین‌المللی حقوق بشر گردآوری شده‌اند. تحلیل داده‌ها بر اساس مقایسه مفهومی و ساختاری دو نظام حقوقی ایران و فرانسه انجام می‌شود تا نقاط اشتراک، افتراق و کاستی‌ها شناسایی و راهکارهای اصلاحی مناسب برای نظام حقوقی ایران ارائه گردد.

۱. تعاریف مفاهیم

۱-۱. جرایم سایبری

جرایم سایبری به آن دسته از جرائم اطلاق می‌شوند که در فضای سایبر (فضای مجازی، اینترنت، شبکه‌های کامپیوتری) رخ می‌دهند یا با استفاده از فناوری اطلاعات و ارتباطات ارتکاب می‌یابند. به عبارت دیگر، این جرایم می‌توانند شامل حمله به زیرساخت‌های کامپیوتری، نفوذ (هک)، استفاده از بدافزار، اخاذی دیجیتال، سرقت هویت آنلاین، تروجان، باج‌افزار و غیره باشند (آجوی ، ۲۰۲۴: ۱۴-۱۵). معمولاً در ادبیات حقوقی و جرایم بین‌المللی، جرایم سایبری به دو زیرمجموعه تقسیم می‌شوند.

۱. جرایم وابسته به سایبر : جرایمی که فقط با استفاده از فناوری سایبر قابل ارتکاب‌اند، مثل نفوذ کامپیوتری (هک)، حملات بدافزاری، باج‌افزار و غیره.

۲. جرایم فعال‌شده توسط سایبر : جرائم سنتی‌تر (مثل کلاهبرداری، پولشویی، قاچاق) که با کمک ابزارهای دیجیتال، مقیاسشان افزایش یافته یا تسهیل شده‌اند(سارکار و شوکلا ، ۲۰۲۴: ۳۰۷-۳۱۰).

۱-۲. جرایم الکترونیکی

اصطلاح «جرائم الکترونیکی» گاهی به عنوان مترادف «جرائم سایبری» به کار می‌رود، اما بسته به متون قانونی و حقوقی می‌تواند معنای خاص‌تری داشته باشد. در برخی کشورها همچون نیوزیلند، جرایم الکترونیکی به جرائمی اشاره دارد که از طریق دستگاه‌های الکترونیکی (نه فقط اینترنت) انجام می‌شوند؛ مثلاً جرائم با بهره‌گیری از تلفن‌های هوشمند، پیامک، دستگاه‌های الکترونیکی آفلاین، پایانه‌های پرداخت الکترونیکی و غیره (وال ، ۲۰۲۴: ۱۷-۲۰). به همین ترتیب، برخی قانون‌گزاران میان جرایم کامپیوتری و جرایم سایبری تفاوت قائل می‌شوند. جرم کامپیوتری ممکن است شامل استفاده غیرمجاز از کامپیوتر، سرقت داده‌ها از سیستم محلی باشد، حتی اگر آن سیستم به اینترنت متصل نباشد(وانگ ، ۲۰۲۴: ۲-۴). بنابراین می‌توان اذعان نمود که جرایم کامپیوتری هر اقدام غیرقانونی با کامپیوتر را شامل می‌شوند، در حالی که جرایم سایبری غالباً نیازمند اینترنت است.

در تبیین و تشریح تفاوت‌ها و تمایزات جرایم سایبری و جرایم الکترونیکی می‌توان به موارد ذیل اشاره نمود:

۱. محدوده فنی: جرایم سایبری معمولاً بر استفاده از شبکه‌های کامپیوتری و اینترنت تأکید دارد. مثلاً هک سرورها، حملات باج‌افزار، نفوذ اینترنتی اما جرایم الکترونیکی ممکن است شامل وسایل غیرمتصل به اینترنت نیز شود؛ مثلاً جرماتی که روی دستگاه‌های الکترونیکی محلی (تلفن، پایانه پرداخت، کارت‌خوان) صورت می‌گیرند.

۲. ماهیت جرم: برخی جرایم سایبری جدید هستند و فقط در فضای دیجیتال قابل وقوع‌اند (جرایم وابسته به سایبر) اما جرایم الکترونیکی می‌توانند مواردی از جرایم سنتی باشند که با فناوری الکترونیکی تسهیل شده‌اند (مثلاً کلاهبرداری از طریق پیامک، فیشینگ) که در ادبیات جرایم سایبری، این نوع را جرایم تقویت‌شده توسط فناوری‌های سایبری می‌نامند.

۳. تعارض قانونی و دادسری: در بسیاری از کشورها، قوانین جرایم سایبری به‌روزتر بوده‌اند و شامل جرم‌هایی می‌شوند که به‌طور خاص برای فضای اینترنت طراحی شده‌اند (مثل نفوذ، بدافزار، باج‌افزار) این در حالی است که جرایم الکترونیکی ممکن است در برخی نظام‌های حقوقی، در چارچوب قوانین تجارت الکترونیک، جرائم مالی یا جرائم کامپیوتری قدیمی‌تر تعریف شوند. به عنوان مثال، قانون‌گذار ممکن است جرمی را تحت «جرائم رایانه‌ای» تعریف کند که نه الزاماً اینترنتی است، بلکه فقط از طریق کامپیوتر انجام شده است.

۴. اهمیت مقیاس و عبور از مرزها: جرائم سایبری غالباً ظرفیت بین‌المللی شدن دارند: فرد مجرم می‌تواند از یک کشور به سرویس دهنده در کشور دیگر حمله کند، اثری جغرافیایی از جرم ممکن است محدود نباشد اما جرایم الکترونیکی که بیشتر محلی‌اند (مثلاً تقلب از طریق کارت‌خوان محلی) ممکن است اثر فرامرزی نداشته باشند، یا به همان حوزه فیزیکی مربوط باشند.

۵. ردیابی و شواهد دیجیتال: در جرایم سایبری، ردیابی مجرم می‌تواند بسیار پیچیده‌تر باشد زیرا سرورهای پراکنده، رمزنگاری، ترافیک رمزگذاری شده همه چالش‌هایی هستند این در حالی است که در جرایم الکترونیکی محلی‌تر، جمع‌آوری شواهد ممکن است ساده‌تر باشد (مثلاً داده‌های محلی دستگاه، سوابق تراکنش‌های دستگاه پرداخت الکترونیکی)
.

۳-۱. حق آگاهی از اتهام

یکی از اصول بنیادین در نظام‌های دادرسی عادلانه، اصل آگاهی متهم از اتهام واردشده است. این اصل، هم در حقوق داخلی کشورها و هم در اسناد بین‌المللی حقوق بشر به‌عنوان یکی از ارکان «حق دفاع مؤثر» شناخته شده است (بیکی شورکی و فلاح، ۱۴۰۳: ۳۴). بر اساس بند (۲) ماده (۱۴) میثاق بین‌المللی حقوق مدنی و سیاسی (۱۹۶۶)، هر شخصی که به ارتکاب جرمی متهم شود، باید در کوتاه‌ترین زمان و به‌صورت تفصیلی از ماهیت و علت اتهام علیه خود آگاه گردد(الکساندرویچ ، ۲۰۲۳: ۱۰۱). این الزام، اساس تفهیم اتهام را در نظام‌های حقوقی مختلف شکل داده است. در فلسفه دادرسی کیفری، آگاهی از اتهام نه‌تنها حق متهم، بلکه ضمانتی برای مشروعیت دادرسی محسوب می‌شود. زیرا دفاع مؤثر بدون اطلاع کافی از اتهام، امکان‌پذیر نیست. در نتیجه، تفهیم اتهام پلی است میان اصل «حق دفاع» و «اصل برائت» (فاهی ، ۲۰۲۴: ۱۰۷۹).

۱-۴. حقوق دفاعی متهم و تبیین فرایند تفهیم اتهام در جرایم سنتی و سایبری

حقوق دفاعی متهم شامل مجموعه‌ای از تضمین‌های قانونی است که هدف آن حفظ تعادل میان قدرت دولت در تعقیب جرم و حق آزادی فردی متهم است. بر اساس آموزه‌های عدالت کیفری، این حقوق شامل مواردی چون آگاهی از اتهام، حق برخورداری از وکیل، حق سکوت، دسترسی به پرونده، و برخورداری از زمان و امکانات کافی برای دفاع است (کندی و همکاران، ۲۰۲۴: ۴). در نظریه‌های عدالت کیفری معاصر، به‌ویژه در اندیشه «دادرسی منصفانه » این حقوق نه به‌عنوان امتیاز، بلکه به‌عنوان حقوق ذاتی و غیرقابل سلب متهم شناخته می‌شوند. در نتیجه، هرگونه نقض در مرحله تفهیم اتهام، نقض کل نظام دادرسی عادلانه تلقی می‌شود (موهارمان ، ۲۰۲۵: ۳۸۹). نکتهٔ مهمی که باید به آن توجه داشت تفاوت‌های

ماهوی میان تفهیم اتهام در جرایم سنتی و جرایم سایبری است، در این رابطه، تفهیم اتهام در جرایم سایبری از نظر ماهیت، محتوا و شیوه اجرا با جرایم سنتی تفاوت‌هایی دارد، زیرا ماهیت ادله دیجیتال، نحوه ارتکاب، و گستره جغرافیایی جرایم سایبری متفاوت است . این تفاوت‌ها باعث می‌شود که مقام قضایی هنگام تفهیم اتهام، اطلاعات تخصصی‌تر و دقیق‌تری ارائه کند و محدود به توصیف رفتار ظاهری مجرم نباشد (عبدالله و همکاران، ۲۰۲۵: ۸۹۹). به طور کلی، برخی از مهمترین تفاوت‌های ماهوی تفهیم اتهام در جرایم سایبری با جرایم سنتی عبارتند از:

۱. پیچیدگی ادله و ضرورت توضیح فنی در جرایم سایبری، مقام قضایی باید هنگام تفهیم اتهام، ماهیت ادله دیجیتال (مانند IP، لاگ‌فایل‌ها، متادیتا، ردپای دیجیتال، تحلیل فنی) را برای متهم روشن کند ؛ امری که در جرایم سنتی معمولاً نیاز به تشریح فنی گسترده ندارد؛

۲. ابهام‌زدایی از نحوه ارتکاب جرم: در جرایم سایبری، شیوه ارتکاب (هک، فیشینگ، بدافزار، دسترسی غیرمجاز، جعل داده، شنود غیرمجاز) معمولاً پیچیده و غیرملموس است؛ بنابراین در زمان تفهیم اتهام باید سازوکار ارتکاب جرم به زبان قابل فهم برای متهم تبیین شود ، درحالی‌که جرایم سنتی معمولا با اعمال فیزیکی روشن و قابل تصور سروکار دارند؛

۳. تعیین دقیق زمان و مکان وقوع جرم: در فضای سایبری، زمان و مکان جرم ممکن است پراکنده، چندمرحله‌ای و بین‌المللی باشد. در نتیجه هنگام تفهیم اتهام باید تعیین شود که جرم از نظر حقوقی در کجا و چه زمانی واقع شده است؛ موضوعی که در جرایم سنتی معمولاً روشن و ساده‌تر است ؛ از طرفی، جرایم سایبری غالباً فرامرزی‌اند و اغلب از خلأهای قانونی در کشورها سوءاستفاده می‌شود، بنابراین لازم است قوانین داخلی کشورها اصلاح شوند و همکاری بین‌المللی تقویت شود (برنر ، ۲۰۲۳: ۸۷-۸۹).

۴. ضرورت اشاره به بستر، سامانه یا داده مورد تعرض: در تفهیم اتهام سایبری لازم است دقیقاً مشخص شود که کدام سامانه، حساب کاربری، شبکه، داده یا نرم‌افزار هدف قرار گرفته و نوع دسترسی یا دستکاری چه بوده است؛ در حالی که در جرایم سنتی غالباً ذکر شیء مادی یا شخص آسیب‌دیده کفایت می‌کند (سپاها ، ۲۰۲۵: ۹۸۳-۹۸۸).

۱-۵. دادرسی منصفانه و جایگاه تفهیم اتهام

«دادرسی منصفانه» مفهومی چندوجهی است که در حقوق تطبیقی، مجموعه‌ای از اصول شکلی و ماهوی را دربر می‌گیرد؛ از جمله اصل برائت، حق دسترسی به وکیل، دادرسی علنی، بی‌طرفی قاضی و آگاهی از اتهام. تفهیم اتهام در این نظریه، گام نخست تحقق عدالت کیفری است؛ زیرا متهم تا زمانی که از اتهام خود مطلع نباشد، نمی‌تواند از حقوق دفاعی خویش استفاده کند (سرکجا وموکولاری ، ۲۰۲۴: ۱۸۹). در چارچوب عدالت منصفانه، دو رویکرد اصلی وجود دارد:

۱. رویکرد صوری : که بر رعایت تشریفات قانونی در اطلاع‌رسانی اتهام تأکید دارد؛

۲. رویکرد ماهوی : که علاوه بر اطلاع‌رسانی، بر فهم مؤثر و واقعی متهم از اتهام تأکید دارد (محمدی و همکاران، ۱۴۰۲: ۲۲۹-۲۳۰).

رویکرد دوم در جرائم سایبری اهمیت بیشتری دارد، زیرا پیچیدگی فنی این جرائم ممکن است موجب شود متهم از ماهیت واقعی اتهام آگاه نگردد.

۶-۱. حقوق بشر در تضمین اطلاع از اتهام

بر اساس اسناد بین‌المللی نظیر اعلامیه جهانی حقوق بشر (۱۹۴۸) و میثاق بین‌المللی حقوق مدنی و سیاسی (۱۹۶۶)، دولت‌ها مکلف‌اند در فرآیند کیفری، متهم را در کوتاه‌ترین زمان از اتهامات علیه او آگاه سازند و امکان دفاع مؤثر را فراهم کنند (استویج، ۱۴۰۰: ۱۸). کمیته حقوق بشر سازمان ملل در تفسیر عمومی شماره ۱۳ خود، تأکید کرده است که آگاهی از اتهام باید «صریح، دقیق و قابل درک برای متهم» باشد(قائم‌فرد و محسنی، ۱۴۰۲: ۳). بنابراین، صرف اعلام کلی اتهام بدون ارائه جزئیات، مغایر با حق دفاع است (پرز ، ۲۰۲۵: ۵۵). بر این اساس، مبنای پژوهش حاضر، بر تلفیقی از نظریه دادرسی منصفانه، نظریه حقوق دفاعی متهم و رویکرد حقوق بشری به اطلاع‌رسانی قضایی استوار است.

جدول ۱. شاخص‌های نظری پژوهش

شاخص‌ها	متغیر	نوع متغیر
ساختار آیین دادرسی، سامانه‌های دیجیتال، قوانین مرتبط	نظام حقوقی (ایران و فرانسه)	متغیر مستقل
شفافیت اطلاع‌رسانی، دسترسی به وکیل، ابلاغ الکترونیکی	فرآیند تفهیم اتهام در جرائم سایبری	متغیر میانجی
آگاهی مؤثر از اتهام، امکان دفاع، رعایت اصول دادرسی عادلانه	تضمین حقوق دفاعی متهم	متغیر وابسته

۲- تفهیم اتهام در جرائم سایبری با تأکید بر تضمین حقوق دفاعی متهم در حقوق ایران

جرائم سایبری ویژگی‌هایی دارند که بر نحوه اجرای تفهیم اتهام اثر می‌گذارند. غیرمحلی بودن جرم که بر اساس آن متهم ممکن است در شهری دیگر یا حتی کشوری دیگر باشد. ماهیت دیجیتال ادله که بر اساس آن، داده‌ها به‌سادگی قابل تغییر یا حذف‌اند. تعدد بازیگران که ممکن است چند متهم در نقاط مختلف با یکدیگر در تعامل باشند (مزینانیان، ۱۴۰۲: ۲۱۲). این ویژگی‌ها سبب می‌شود تفهیم اتهام در جرائم سایبری نیازمند سازوکارهای جدید، از جمله تفهیم سایبری، ویدئوکنفرانس قضایی، و ارائه‌ی نسخه دیجیتال از مستندات اتهام باشد.

در نظام دادرسی کیفری ایران، نهاد تفهیم اتهام یکی از ارکان اساسی تضمین‌کننده‌ی حقوق دفاعی متهم محسوب می‌شود. این نهاد، وظیفه‌ای مضاعف دارد. از یک‌سو، تضمین‌کننده‌ی اجرای اصل برائت و از سوی دیگر، نقطه‌ی آغاز اعمال حق دفاع متهم است(نصراللهی، ۱۴۰۳: ۱۰). تفهیم اتهام به معنای آن است که مقام قضایی، در زمان معین و به شیوه‌ای روشن، تمامی ابعاد اتهام، دلایل انتساب آن و حقوق قانونی متهم را به وی اعلام کند تا بتواند آگاهانه از خود دفاع نماید (السان، ۱۴۰۰: ۲۱). با ظهور جرائم سایبری و دگرگونی در ابزار ارتکاب جرم، نظام حقوقی ایران ناگزیر با مفاهیم و فرآیندهای جدیدی روبه‌رو شده است. این جرائم، به دلیل پیچیدگی فنی، چندلایه بودن ادله و ماهیت بین‌المللی، موجب شده‌اند که اجرای اصول سنتی دادرسی کیفری با دشواری‌های جدی مواجه گردد (غمامی و فعلی، ۱۴۰۱: ۸۶). یکی از مهم‌ترین این چالش‌ها، اجرای صحیح تفهیم اتهام است؛ چراکه بسیاری از متهمان در جرایم سایبری، نه تنها از ماهیت اتهام آگاه نمی‌شوند، بلکه حتی از مستندات الکترونیکی و فرآیند کشف آن اطلاع کافی ندارند (عباسی و همکاران، ۱۴۰۴: ۳۷).

۱-۲. مبانی قانونی تفهیم اتهام در حقوق ایران

قانون آیین دادرسی کیفری مصوب ۱۳۹۲ (با اصلاحات ۱۳۹۴) به‌صراحت در چند ماده به لزوم تفهیم اتهام اشاره کرده است. مهم‌ترین آن‌ها عبارت‌اند از:

ماده ۱۹۷: مقرر می‌دارد که بازپرس پس از حضور متهم، باید بلافاصله هویت او را احراز و سپس موضوع اتهام و دلایل آن را به‌طور صریح به وی تفهیم نماید. در واقع، این ماده ناظر به آغاز فرآیند تفهیم اتهام است و بازپرس را مکلف می‌کند که پس از احراز هویت، اتهام و دلایل آن را به‌طور صریح و شفاف به متهم اعلام کند. هدف اصلی آن تضمین آگاهی واقعی متهم از موضوع اتهام و فراهم‌سازی امکان دفاع مؤثر است.

ماده ۱۹۰: حق داشتن وکیل در مرحله تحقیقات مقدماتی را به رسمیت می‌شناسد و مقرر می‌دارد که متهم می‌تواند پیش از شروع تحقیق از اتهام و دلایل آن مطلع گردد. بنابراین این ماده حق دسترسی به وکیل را از بدو تحقیقات مقدماتی به رسمیت می‌شناسد و تأکید می‌کند متهم باید پیش از تحقیق از اتهام و مستندات آن مطلع شود. بدین ترتیب، تعادل میان قدرت تحقیق و حق دفاع حفظ و روند دادرسی عادلانه‌تر می‌شود.

ماده ۵ قانون آیین دادرسی کیفری: بر اصل احترام به حقوق شهروندی و ممنوعیت سلب حق دفاع تأکید دارد (میرکتولی، ۱۴۰۳: ۴۱-۴۲). به بیانی دیگر، ماده ۵ بر رعایت اصول حقوق شهروندی و احترام به کرامت انسانی در تمام مراحل دادرسی تأکید دارد. این ماده چارچوبی کلی برای صیانت از حقوق دفاعی متهم و جلوگیری از اعمال خودسرانه مقام‌های قضایی فراهم می‌سازد.

بنابراین، از این مواد می‌توان نتیجه گرفت که قانون‌گذار ایران، به لحاظ شکلی، اصل تفهیم اتهام را پذیرفته و آن را به عنوان تکلیف قاضی یا بازپرس تلقی کرده است. با این حال، چگونگی و کیفیت اجرای این اصل در جرائم سایبری، همچنان با ابهام و ناهماهنگی همراه است.

۲-۲. فرآیند تفهیم اتهام در جرایم سایبری

در موضوعات مرتبط با جرائم سایبری (مانند دسترسی غیرمجاز، جاسوسی داده، فیشینگ، یا نشر اکاذیب در فضای مجازی)، معمولاً فرآیند تفهیم اتهام از طریق واحدهای پلیس فتا آغاز و سپس در دادسراهای ویژه جرائم رایانه‌ای ادامه می‌یابد (سیدحسینی، ۱۴۰۴: ۳۱). در این فرآیند، چند مرحله مهم وجود دارد:

اول؛ احضار یا جلب متهم: معمولاً بر اساس گزارش پلیس فتا یا شکایت خصوصی؛
دوم؛ تحقیق مقدماتی توسط بازپرس: در این مرحله، بازپرس موظف است اتهام را به‌صورت صریح اعلام کند؛
سوم؛ تفهیم حقوق قانونی: شامل حق سکوت، حق داشتن وکیل، و حق اطلاع از دلایل اتهام (الهی‌منش، ۱۴۰۱: ۴۷-۴۸).

اما در عمل و در بسیاری از موارد، تفهیم اتهام به صورت رسمی و مستند انجام نمی‌شود؛ بلکه در قالب پرسش‌های بازجویی و به صورت کلی صورت می‌گیرد. این امر با اصل اطلاع مؤثر از اتهام مغایرت دارد. بنابراین ضعف ساختاری در موضوع تفهیم اتهام در جرائم سایبری موضوع مهم و بحث برانگیزی است، زیرا علی‌رغم تصریح قانون بر اعلام صریح

اتهام و حقوق متهم، این روند غالباً به‌صورت شکلی و غیرمستند انجام می‌شود. در نتیجه، متهم از آگاهی واقعی نسبت به ماهیت اتهام، دلایل آن و حقوق دفاعی خود محروم می‌ماند. این وضعیت نه‌تنها با اصول دادرسی عادلانه و حق دفاع مغایرت دارد، بلکه موجب کاهش شفافیت و افزایش احتمال سوءاستفاده از اختیارات تحقیق می‌شود. فقدان آموزش تخصصی ضابطان و نبود دستورالعمل مشخص برای جرائم سایبری از عوامل اصلی این ضعف است. در نهایت، اصلاح این فرآیند از طریق شفاف‌سازی قانونی، آموزش تخصصی و الزام به مستندسازی رسمی تفهیم اتهام ضروری است.

۳-۲. چالش‌های مفهومی و اجرایی

الف) نبود تعریف جامع از تفهیم اتهام در قوانین ایران: اگرچه قانون آیین دادرسی کیفری به‌صورت پراکنده از تفهیم اتهام سخن گفته، اما تعریف دقیق و جامعی از آن ارائه نکرده است. این در حالی است که در برخی کشورها مانند فرانسه، «آگاهی از اتهام» به‌صورت یک حق مستقل تعریف و سازوکار اجرایی آن تبیین شده است. در نتیجه، در ایران، تفاوت میان «اطلاع‌رسانی شکلی» و «تفهیم واقعی» مشخص نیست (احمدی، ۱۴۰۳: ۶۶). بنابراین، فقدان تعریف روشن از تفهیم اتهام سبب شده تفسیرهای گوناگونی از این مفهوم در رویه قضایی شکل گیرد. این ابهام باعث می‌شود برخی مقامات قضایی صرف «ابلاغ اتهام» را کافی بدانند، در حالی که تفهیم واقعی مستلزم اطمینان از درک متهم نسبت به اتهام و دلایل آن است. در نتیجه، حقوق دفاعی متهم در مرحله تحقیق مقدماتی به‌طور کامل تضمین نمی‌شود.

ب) ضعف در مستندسازی الکترونیکی: در جرائم سایبری، تفهیم اتهام باید مبتنی بر ادله دیجیتال باشد(غلامی‌نیا، ۱۴۰۳: ۱۵). اما در بسیاری از موارد، گزارش‌های فنی پلیس فتا یا کارشناسان **IT** در اختیار متهم یا وکیل او قرار نمی‌گیرد. این امر موجب می‌شود متهم عملاً از مستندات اتهام آگاه نباشد و نتواند دفاع مؤثری ارائه دهد. به عبراتی دیگر، نبود دسترسی متهم و وکیل به ادله دیجیتال، موجب عدم شفافیت در روند دادرسی می‌شود. از آنجا که ماهیت جرائم سایبری بر داده‌های فنی استوار است، عدم ارائه گزارش‌های پلیس فتا به‌صورت رسمی، عملاً مانع از ارزیابی صحت و سقم دلایل می‌گردد. این ضعف می‌تواند به تضییع حق دفاع و افزایش بی‌اعتمادی نسبت به فرآیند قضایی بینجامد.

ج) فقدان دستورالعمل‌های تخصصی: نظام دادرسی ایران فاقد دستورالعمل اجرایی ویژه‌ای در زمینه نحوه تفهیم اتهام در جرایم سایبری است (الهی‌منش، ۱۴۰۱: ۵۹). بنابراین، نبود دستورالعمل مشخص، باعث تشتت رویه و اعمال سلیقه‌های شخصی توسط بازپرس‌ها شده است. در حالی که در جرائم سایبری، تفهیم اتهام نیازمند دانش فنی و رویه واحد است تا عدالت شکلی و ماهوی تضمین شود. تدوین دستورالعمل تخصصی می‌تواند از برداشت‌های نادرست جلوگیری کرده و انسجام در فرآیند دادرسی ایجاد کند.

د) ضعف دسترسی به وکیل: با وجود تصریح ماده ۱۹۰ قانون آیین دادرسی کیفری، در بسیاری از موضوعات مرتبط با جرائم سایبری، متهمان تا مرحله‌ای از تحقیقات از حضور وکیل محروم هستند(احمدی، ۱۴۰۳: ۷۴). گاهی وکیل تنها پس از صدور قرار نهایی وارد موضوع جرم موکل خود می‌شود که این امر عملاً حق دفاع را بی‌اثر می‌سازد. محرومیت متهم از حضور وکیل در مراحل اولیه، نه‌تنها ناقض حقوق دفاعی است بلکه احتمال اعترافات ناآگاهانه و فشار روانی را افزایش می‌دهد. حضور وکیل از آغاز تحقیقات می‌تواند موجب شفافیت، کنترل قانونی عملکرد ضابطان و پیشگیری از نقض حقوق متهم گردد. تقویت ضمانت‌های اجرایی ماده ۱۹۰ ضروری است تا این حق جنبه واقعی پیدا کند.

هـ) مشکلات فنی و اداری در ابلاغ الکترونیکی: سامانه‌های قضایی ایران (مانند سامانه ثنا) اگرچه برای ابلاغ اوراق قضایی طراحی شده‌اند، اما هنوز در حوزه‌ی تفهیم اتهام قابلیت اجرای کامل ندارند(مهدی‌پور و باهنر، ۱۴۰۳: ۲۴). تفهیم اتهام مستلزم حضور متهم یا نماینده قانونی اوست و در فضای سایبری هنوز چارچوب معتبر حقوقی برای آن وجود ندارد. با وجود پیشرفت در سامانه‌های قضایی، بستر فنی و حقوقی لازم برای اجرای کامل تفهیم اتهام به‌صورت الکترونیکی هنوز فراهم نیست. چالش‌هایی مانند احراز هویت قطعی متهم، اطمینان از آگاهی واقعی او و مستندسازی فرایند، مانع از تحقق کامل این هدف می‌شود. در نتیجه، نظام ابلاغ الکترونیکی نیازمند اصلاحات زیرساختی و مقرراتی جدی است.

به طور کلی، در چارچوب اصول دادرسی عادلانه در قانون اساسی جمهوری اسلامی ایران، چند اصل مهم با مفهوم تفهیم اتهام مرتبط است:

اصل ۳۲: هیچ‌کس را نمی‌توان دستگیر کرد مگر به حکم قانون و در صورت بازداشت باید بلافاصله دلایل اتهام به او اعلام شود؛

اصل ۳۵: در همه دادگاه‌ها طرفین حق دارند برای خود وکیل انتخاب کنند؛

اصل ۳۷: اصل بر برائت است و هیچ‌کس از نظر قانون مجرم شناخته نمی‌شود مگر جرم او در دادگاه صالح اثبات گردد(محتاج و همکاران، ۱۴۰۴: ۵۹).

این اصول نشان می‌دهد که قانون اساسی ایران، در سطح کلان، نهاد تفهیم اتهام را به‌عنوان یکی از ابزارهای حفظ حقوق دفاعی متهم پذیرفته است. با این حال، در اجرای عملی، خلأ میان قانون و رویه وجود دارد.

همچنین، با بررسی برخی از پرونده‌های جرائم سایبری ، می‌توان چند ضعف اساسی را در نظام ایران برشمرد:

۱. شکل‌گرایی قضایی: در بسیاری از موارد، قاضی صرفاً با ذکر عنوان جرم، وظیفه تفهیم اتهام را انجام‌شده تلقی می‌کند، در حالی که هدف قانون، ایجاد آگاهی واقعی در متهم است. در واقع، صرف ذکر عنوان جرم بدون تشریح دلایل و مستندات، مانع از تحقق آگاهی واقعی متهم می‌شود. این رویه می‌تواند منجر به کاهش اثرگذاری حق دفاع و افزایش احتمال بروز اشتباه در تصمیم‌گیری قضایی گردد.

۲. فقدان آموزش تخصصی: بازپرسان و ضابطان در حوزه جرائم سایبری، دانش فنی کافی برای توضیح ماهیت جرم به متهم ندارند. در نتیجه، تفهیم اتهام به‌صورت ناقص انجام می‌شود. در این رابطه باید به این موضوع مهم توجه داشت که نبود آموزش فنی و حقوقی کافی برای بازپرسان و ضابطان باعث می‌شود که تفهیم اتهام در جرائم سایبری ناقص یا غیرشفاف انجام شود. این امر می‌تواند حقوق متهم را محدود کرده و کیفیت رسیدگی قضایی را کاهش دهد.

۳. ابهام در زبان قضایی: در بسیاری از احضاریه‌ها یا صورت‌جلسات، از اصطلاحات فنی و حقوقی استفاده می‌شود که برای متهمان عادی قابل فهم نیست. این امر مغایر با اصل صراحت و شفافیت در تفهیم اتهام است. به بیانی دیگر، استفاده از

اصطلاحات فنی و پیچیده در احضاریه‌ها و صورت‌جلسات، فهم دقیق اتهام را برای متهمان عادی دشوار می‌کند. چنین وضعیتی با اصل صراحت و شفافیت در تفهیم اتهام مغایرت داشته و می‌تواند منجر به سردرگمی متهم گردد.

۴. تبعیض در دسترسی به اطلاعات: در جرایم امنیتی یا رایانه‌ای خاص، معمولاً دسترسی وکیل به اطلاعات محدود می‌شود، که این امر بر حق دفاع تأثیر مستقیم دارد. محدود کردن دسترسی وکیل به اطلاعات پرونده‌های حساس، تعادل میان متهم و نهادهای تحقیق را برهم می‌زند. این تبعیض باعث می‌شود متهم نتواند دفاع کامل ارائه دهد و اصول دادرسی عادلانه نقض شود.

به طور کلی، نظام حقوقی ایران از حیث نصوص قانونی در زمینه تفهیم اتهام، اصول نسبتاً کاملی دارد؛ اما از حیث اجرای عملی، شفافیت مفهومی و ضمانت اجرا، با ضعف‌های قابل‌توجهی روبه‌روست. در جرائم سایبری، این ضعف‌ها پررنگ‌تر می‌شود؛ زیرا اولاً پیچیدگی فنی جرائم مانع از درک واقعی متهم از اتهام می‌شود؛ ثانیاً ناهماهنگی بین ضابط و مرجع قضایی موجب پراکندگی در تفهیم اتهام است و در نهایت، فقدان زیرساخت‌های الکترونیکی و آموزش‌های لازم، مانع تحقق دادرسی منصفانه در عمل می‌گردد. بنابراین، اصلاح ساختاری در سه محور قانونی، فنی و آموزشی برای ارتقای نهاد تفهیم اتهام در ایران ضروری است. تنها از رهگذر چنین اصلاحاتی می‌توان اطمینان حاصل کرد که متهمان در فضای مجازی نیز از همان حقوق بنیادینی برخوردارند که در دادرسی‌های سنتی به رسمیت شناخته شده است.

۳. تفهیم اتهام در جرائم سایبری با تأکید بر تضمین حقوق دفاعی متهم در حقوق فرانسه

نظام حقوقی فرانسه، به عنوان یکی از پیشروترین نظام‌های حقوقی اروپایی در زمینه دادرسی کیفری و حفاظت از حقوق متهم، توجه ویژه‌ای به نهاد تفهیم اتهام داشته است. در این نظام، تفهیم اتهام نه تنها یک الزام شکلی قانونی است، بلکه به عنوان یک حق ذاتی و اساسی متهم تعریف شده است که مبنای تحقق دادرسی منصفانه و دفاع مؤثر به شمار می‌رود (لئونتی ، ۲۰۲۵: ۷). ظهور جرائم سایبری، با پیچیدگی‌های فنی و گستردگی جغرافیایی، چالش‌های جدیدی برای اجرای این نهاد ایجاد کرده است. فرانسه در پاسخ به این چالش‌ها، ضمن بهره‌گیری از تجربه حقوقی کلاسیک، سازوکارهای مجازی و نوین برای اطلاع‌رسانی و تفهیم اتهام ایجاد کرده است(گرنائوتی ، ۲۰۲۳: ۲۴).

۱-۳. مبانی قانونی تفهیم اتهام در فرانسه

مهم‌ترین مقررات قانونی مرتبط با تفهیم اتهام در فرانسه عبارت‌اند از:

ماده ۱۱۴ قانون آیین دادرسی کیفری فرانسه : متهم باید بلافاصله پس از تحقیقات مقدماتی از موضوع اتهام و دلایل آن مطلع شود و حق برخورداری از وکیل به وی اعلام گردد. این ماده تضمین می‌کند که متهم از همان آغاز تحقیقات مقدماتی نسبت به اتهام و دلایل آن آگاه شود و حق استفاده از وکیل برای دفاع را بداند. اجرای فوری این ماده موجب افزایش شفافیت و کاهش احتمال سوءاستفاده از قدرت بازپرس می‌شود.

ماده ۶۳-۱ و ۶۳-۳ قانون آیین دادرسی کیفری: شرایط حضور وکیل و نحوه اطلاع‌رسانی به متهم در مراحل بازجویی را تعیین کرده‌اند. این مواد چارچوب دقیق حضور وکیل و نحوه اطلاع‌رسانی به متهم در بازجویی‌ها را تعیین کرده‌اند. با این سازوکار، متهم می‌تواند دفاع مؤثر ارائه دهد و رویه قضایی یکنواخت و قابل پیش‌بینی برقرار شود.

اصل دادرسی منصفانه :متهم حق دارد از تمامی مراحل پرونده مطلع شود و دسترسی کامل به اطلاعات و مستندات داشته باشد (آسانه توره ، ۲۰۲۵: ۸۵-۸۲). این اصل حق دسترسی کامل متهم به اطلاعات و مستندات پرونده و مطلع شدن از تمامی مراحل دادرسی را تضمین می‌کند. رعایت این اصل موجب اعتماد عمومی به عدالت قضایی و جلوگیری از نقض حقوق دفاعی می‌گردد.

این مواد قانونی نه تنها حق اطلاع از اتهام را تصریح کرده‌اند، بلکه روش‌ها و سازوکارهای اجرایی آن را نیز مشخص کرده‌اند، از جمله استفاده از ابلاغ کتبی و دیجیتال، حضور وکیل و دسترسی الکترونیکی به پرونده. استفاده از ابلاغ کتبی و دیجیتال، امکان حضور وکیل و دسترسی الکترونیکی به پرونده، تضمین می‌کند که حق اطلاع واقعی متهم محقق شود. این رویکرد عملی، تفهیم اتهام را از حالت شکلی خارج کرده و به یک حق مؤثر تبدیل می‌کند.

۲-۳. فرآیند تفهیم اتهام در جرایم سایبری

در فرانسه، نظام قضایی در برخورد با جرائم سایبری، فرآیند تفهیم اتهام را به گونه‌ای طراحی کرده است که ضمن رعایت اصول دادرسی عادلانه، از ابزارهای فناوری برای تضمین شفافیت و دسترسی برابر طرفین استفاده شود. این فرآیند چند مرحله‌ی مشخص دارد که هر کدام نقش مهمی در تضمین حقوق متهم و کیفیت رسیدگی دارند:

۱. بازجویی اولیه توسط پلیس یا اداره تحقیقات قضایی : در نخستین گام، متهم توسط پلیس یا مأموران اداره تحقیقات قضایی مورد بازجویی قرار می‌گیرد(بیک و همکاران، ۲۰۲۴: ۴۱۸). در این مرحله، متهم باید به‌صورت رسمی از ماهیت اتهام، دلایل اولیه انتساب جرم و حقوق قانونی خود مطلع شود. از جمله این حقوق می‌توان به حق سکوت، حق دسترسی به وکیل و حق اطلاع از روند بازجویی اشاره کرد. در جرائم سایبری، به دلیل پیچیدگی‌های فنی موضوع، حضور وکیل متخصص در حوزه فناوری اطلاعات ضروری دانسته می‌شود تا از تفسیر نادرست داده‌های فنی جلوگیری شود (لئونتی، ۲۰۲۵: ۲۷).

۲. تفهیم اتهام توسط دادستان یا قاضی تحقیق : پس از مرحله‌ی اولیه، دادستان یا قاضی تحقیق به‌طور رسمی اقدام به تفهیم اتهام می‌کند. در این مرحله، متهم به تمامی اطلاعات مربوط به پرونده دسترسی پیدا می‌کند. این اطلاعات شامل: ادله دیجیتال (نظیر داده‌های استخراج‌شده از دستگاه‌ها، پیام‌ها یا شبکه‌ها)، سوابق فنی (گزارش‌های پلیس سایبری یا تحلیل‌های کارشناسان دیجیتال) و گزارش‌های کارشناسی است (سیگنور ، ۲۰۲۳: ۲۹۵-۲۹۴).

بدین ترتیب، متهم نه‌تنها از اتهام آگاه می‌شود بلکه می‌تواند به‌صورت مستند از نحوه شکل‌گیری ادله و اعتبار آن‌ها اطلاع یابد. این شفافیت موجب می‌شود که دفاع مؤثر و آگاهانه ممکن گردد.

۳. دسترسی الکترونیکی و پیگیری از راه دور: یکی از نوآوری‌های نظام قضایی فرانسه در حوزه جرائم سایبری، ایجاد سامانه دیجیتال قضایی است. این سامانه امکان دسترسی الکترونیکی متهم و وکیل او را به کلیه اسناد پرونده فراهم می‌کند. از طریق این سامانه، می‌توان پرونده را به‌صورت آنلاین مشاهده و پیگیری کرد، مدارک یا لایحه‌های دفاعی را بارگذاری نمود و در جلسات آنلاین مشاوره یا دادرسی شرکت کرد (کابیوما ، ۲۰۲۴: ۱۴۳). این اقدام علاوه بر تسهیل در روند

رسیدگی، موجب صرفه‌جویی در زمان و هزینه شده و با ماهیت جرائم سایبری که اغلب مرزهای جغرافیایی را در می‌نوردند، سازگاری دارد.

در مجموع، این ساختار نشان می‌دهد که در فرانسه، تفهیم اتهام تنها یک عمل شکلی یا اداری نیست، بلکه فرآیندی برای تضمین آگاهی واقعی، دقیق و مؤثر متهم از حقوق و اتهامات خود است. هدف اصلی آن، ایجاد توازن میان قدرت تحقیقاتی نهادهای قضایی و حق دفاع متهم است. به این ترتیب، متهم می‌تواند با درک کامل از مستندات فنی و حقوقی، از خود دفاع کند و دادرسی به‌صورت شفاف، عادلانه و مبتنی بر اصول حقوق بشر انجام گیرد. بنابراین، در فرانسه، تفهیم اتهام نقش کلیدی در حفاظت از حقوق دفاعی متهم دارد و فراتر از یک عمل اداری صرف عمل می‌کند. این فرآیند به‌طور نظام‌مند تضمین می‌کند که متهم با آگاهی واقعی از ماهیت اتهام و مستندات پرونده، قادر به اتخاذ تصمیمات آگاهانه باشد. با ایجاد توازن میان اختیارات تحقیقاتی نهادهای قضایی و حقوق متهم، احتمال سوءاستفاده یا فشار غیرقانونی کاهش می‌یابد. همچنین، دسترسی متهم به وکیل و مستندات پرونده، شفافیت و عدالت دادرسی را تقویت می‌کند. در نهایت، این رویکرد زمینه تحقق دادرسی منصفانه و رعایت اصول حقوق بشر را فراهم می‌آورد و نمونه‌ای قابل الگوبرداری برای سایر کشورها به ویژه در پرونده‌های پیچیده سایبری محسوب می‌شود.

۳-۳. سازوکارهای فنی و الکترونیکی

یکی از نقاط قوت نظام قضایی فرانسه در حوزه‌ی جرائم سایبری، استفاده‌ی گسترده و کارآمد از زیرساخت دیجیتال قضایی برای اجرای فرآیند تفهیم اتهام است. این رویکرد، به‌ویژه در پرونده‌های مرتبط با فناوری اطلاعات و فضای مجازی، موجب افزایش سرعت، شفافیت و عدالت در روند رسیدگی می‌شود. عناصر اصلی این نظام دیجیتال عبارت‌اند از:

۱. سامانه الکترونیکی پرونده : این سامانه، بستری امن و یکپارچه برای دسترسی به اسناد و مستندات پرونده‌های قضایی است. متهم و وکیل او می‌توانند با احراز هویت دیجیتال وارد سامانه شده و تمامی مدارک، گزارش‌های کارشناسی دیجیتال، مکاتبات رسمی، و تصمیمات قضایی را مشاهده کنند. این دسترسی شفاف، به آنان اجازه می‌دهد تا بر مبنای داده‌های واقعی و مستند، خط دفاعی خود را طراحی کرده و در برابر ادله فنی ارائه‌شده، پاسخ مناسب دهند (دوپونت ، ۲۰۲۴: ۱۱۳-۱۱۴).

۲. ابلاغ دیجیتال با امضای الکترونیکی : یکی از چالش‌های سنتی در فرآیند تفهیم اتهام، اطمینان از وصول به‌موقع و معتبر ابلاغیه‌ها است. در نظام دیجیتال فرانسه، این مشکل با استفاده از ابلاغ الکترونیکی مجهز به امضای دیجیتال قضایی حل شده است. این فناوری نه‌تنها صحت و تمامیت سند را تضمین می‌کند، بلکه زمان دقیق ارسال و دریافت را ثبت می‌نماید. در نتیجه، امکان ادعای عدم اطلاع یا عدم وصول از سوی متهم به حداقل می‌رسد و روند دادرسی شفاف‌تر می‌شود (گرنائوتی، ۲۰۲۳: ۶۱-۶۳).

۳. ویدئوکنفرانس برای جلسات تفهیم اتهام : برای متهمانی که در خارج از کشور یا در مناطق دور از دادگاه حضور دارند، ویدئوکنفرانس قضایی راه‌حل مؤثری محسوب می‌شود. این ابزار به قاضی اجازه می‌دهد تا فرآیند تفهیم اتهام را به‌صورت زنده و تعاملی انجام دهد، به سؤالات متهم پاسخ دهد، و اطمینان یابد که وی به‌درستی از حقوق و اتهامات خود آگاه شده

است. این روش علاوه بر صرفه‌جویی در زمان و هزینه، از تأخیرهای ناشی از انتقال فیزیکی متهم جلوگیری می‌کند و با ماهیت فرامرزی بسیاری از جرائم سایبری هماهنگ است (دکاری ، ۲۰۲۴: ۹۳).

در مجموع، این سازوکارهای دیجیتال نشان می‌دهند که فرانسه، مفهوم تفهیم اتهام را به‌گونه‌ای مدرن و کارآمد بازتعریف کرده است. در این نظام، آگاهی متهم از اتهام و حقوق خود به‌صورت واقعی، مستند و فناورانه تضمین می‌شود، حتی در صورتی که حضور فیزیکی در دادگاه ممکن نباشد. بدین ترتیب، اصول بنیادین دادرسی عادلانه، از جمله حق اطلاع، حق دفاع و برابری طرفین، در بستر دیجیتال نیز به‌طور کامل رعایت می‌شود.

۴-۳. تحلیل رویه قضایی

بر اساس مطالعات پرونده‌های قضایی و نظرات حقوق‌دانان فرانسه:

۱. قاضی تحقیق موظف است تمامی مستندات پرونده، از جمله فایل‌های دیجیتال و گزارش‌های فنی، را به متهم و وکیل ارائه کند. این الزام باعث می‌شود متهم بتواند به‌طور کامل ماهیت اتهام و شواهد آن را درک کند و دفاع مؤثری ارائه دهد. دسترسی به فایل‌های دیجیتال و گزارش‌های فنی، به ویژه در جرائم سایبری، نقش حیاتی در شفافیت دادرسی و جلوگیری از سوءاستفاده‌های احتمالی ضابطان دارد. این اقدام، پایه‌ای برای تحقق اصل اطلاع واقعی و عدالت کیفری محسوب می‌شود.

۲. در جرائم سایبری پیچیده، قاضی تحقیق ممکن است با کارشناس فناوری اطلاعات همراه شود تا اطمینان حاصل شود که متهم اطلاعات را به درستی درک کرده است (گرنائوتی هلیه ، ۲۰۲۴: ۷۶-۷۷). در واقع، در جرائم سایبری با ماهیت فنی و پیچیده، حضور کارشناس به قاضی کمک می‌کند تا مطمئن شود متهم اطلاعات ارائه‌شده را به درستی درک کرده است. این رویه مانع سوءتفاهم یا برداشت‌های نادرست متهم از اتهام می‌شود و کیفیت تفهیم اتهام را بهبود می‌بخشد. همچنین، تضمین می‌کند که دفاع متهم بر اساس فهم واقعی از مستندات شکل گیرد.

۳. امکان اعتراض متهم به کیفیت اطلاع‌رسانی فراهم است؛ اگر متهم ادعا کند که تفهیم اتهام به شکل ناکافی انجام شده، قاضی می‌تواند تحقیقات را متوقف کرده و مجدداً ابلاغ کند (آبیتبول ، ۲۰۲۵: ۱۷۸-۱۷۶).بنابراین، حق اعتراض متهم، تضمین‌کننده حفظ حقوق دفاعی او در صورت ناکافی بودن تفهیم اتهام است. قاضی با امکان توقف تحقیقات و انجام مجدد تفهیم، شفافیت و عدالت را تقویت می‌کند و از ایجاد بی‌عدالتی ناشی از ابلاغ ناقص جلوگیری می‌کند. این سازوکار، متهم را فعالانه در فرآیند دادرسی دخیل می‌کند و به تحقق دادرسی منصفانه کمک می‌نماید.

این رویه‌ها نشان می‌دهند که در فرانسه، حق اطلاع و حق دفاع به شکل عملی تضمین شده و ضمانت اجرای مؤثری دارد. با وجود ساختار پیشرفته، برخی چالش‌ها در فرانسه نیز وجود دارد:

پیچیدگی فنی پرونده‌ها: گاهی توضیح ماهیت جرائم سایبری برای متهم غیرمتخصص دشوار است؛

محدودیت منابع انسانی و کارشناسان متخصص: تعداد قاضیان و کارشناسان مجرب برای بررسی پرونده‌های سایبری محدود است؛

حفظ حریم خصوصی: ارائه جزئیات کامل پرونده ممکن است با قوانین حفاظت از داده‌ها تداخل داشته باشد، که نیازمند موازنه حقوقی است(اولارد ، ۲۰۲۳: ۱۳۳-۱۳۵).

با این حال، این چالش‌ها با سازوکارهای نظارتی و فناوری قابل مدیریت هستند و بر اساس استانداردهای بین‌المللی، فرانسه یکی از موفق‌ترین نظام‌ها در تضمین حقوق دفاعی متهمان سایبری است. به طور کلی، از تحلیل قانونی و رویه‌ای فرانسه می‌توان چند نتیجه مهم استخراج کرد:

۱. شفافیت و دسترسی مؤثر: قانون و رویه قضایی، تفهیم اتهام را به شکلی طراحی کرده‌اند که متهم بتواند واقعاً ماهیت اتهام و مستندات آن را درک کند. در واقع، در فرانسه، قوانین و رویه قضایی طوری طراحی شده‌اند که متهم نه تنها از عنوان جرم، بلکه از دلایل و مستندات آن به‌طور کامل مطلع شود. این شفافیت، امکان درک واقعی ماهیت اتهام و آماده‌سازی دفاع مؤثر را برای متهم فراهم می‌کند. همچنین، رویه قضایی یکنواخت تضمین می‌کند که همه متهمان، فارغ از نوع پرونده، از حقوق خود بهره‌مند شوند.

۲. ترکیب قانون و فناوری: استفاده از سامانه‌های دیجیتال و ویدئوکنفرانس، تضمین می‌کند که فاصله جغرافیایی یا پیچیدگی پرونده، مانع اطلاع متهم نشود. در این رابطه، استفاده از سامانه‌های دیجیتال پرونده، ویدئوکنفرانس و ابلاغ الکترونیکی با امضای دیجیتال، موجب می‌شود که فاصله جغرافیایی یا پیچیدگی فنی پرونده مانع دسترسی متهم به اطلاعات نشود. این فناوری‌ها نه تنها سرعت و کارایی دادرسی را افزایش می‌دهند، بلکه امکان تعامل آنلاین متهم با وکیل و بررسی مستندات را فراهم می‌کنند.

۳.وجود ضمانت اجرایی: امکان اعتراض به کیفیت تفهیم اتهام، حضور وکیل از ابتدای تحقیقات و مستندسازی دقیق، از بروز نقض حقوق دفاعی جلوگیری می‌کند. لذا در فرانسه، متهم می‌تواند در صورت ناکافی بودن تفهیم اتهام اعتراض کند و قاضی موظف است اقدامات اصلاحی انجام دهد. حضور وکیل از ابتدای تحقیقات و مستندسازی دقیق مراحل تحقیق، تضمین می‌کند که هیچ حق دفاعی نقض نشود. این سازوکارهای اجرایی، حقوق متهم را فعالانه محافظت کرده و شفافیت و عدالت دادرسی را تقویت می‌کنند.

در مجموع، فرانسه نمونه‌ای موفق از تلفیق قوانین صریح، رویه قضایی مستمر و فناوری دیجیتال برای تضمین تفهیم مؤثر اتهام در جرائم سایبری است. از طرفی، در نظام فرانسه اولاً نهاد تفهیم اتهام کاملاً به عنوان حق بنیادین متهم تعریف شده است؛ ثانیاً اجرای این حق با ابزارهای دیجیتال، دسترسی وکیل و مستندسازی دقیق عملی می‌شود؛ ثالثاً هرگونه نقص در اطلاع‌رسانی یا ارائه مستندات، توسط قاضی قابل اصلاح است و رابعاً سازوکارها طوری طراحی شده‌اند که هم حقوق دفاع متهم حفظ شود و هم اصل دادرسی منصفانه رعایت گردد. بنابراین، نظام فرانسه از حیث قانونی، ساختاری و اجرایی، نمونه‌ای پیشرو در زمینه تفهیم اتهام در جرائم سایبری است. این کشور با تلفیق قانونگذاری دقیق، رویه قضایی شفاف و فناوری دیجیتال، اطمینان می‌دهد که متهمان از ابتدا تا انتهای پرونده، از حقوق دفاعی خود آگاه بوده و امکان دفاع مؤثر داشته باشند. با توجه به تجربه فرانسه، می‌توان الگوهای عملی و اصلاحات پیشنهادی برای نظام ایران در زمینه تفهیم اتهام

سایبری استخراج کرد که شامل استفاده از سامانه‌های دیجیتال، آموزش قضات و کارشناسان و تدوین دستورالعمل‌های تخصصی است.

۴. تفهیم اتهام در جرائم سایبری با تأکید بر تضمین حقوق دفاعی متهم؛ بررسی تطبیقی حقوق ایران و فرانسه

پس از بررسی جامع وضعیت تفهیم اتهام در ایران و فرانسه، می‌توان با نگاهی تطبیقی، نقاط قوت و ضعف هر نظام حقوقی را در زمینه تضمین حقوق دفاعی متهم در جرائم سایبری شناسایی کرد. هدف از تحلیل تطبیقی، شفاف‌سازی تفاوت‌ها و ارائه راهکارهای اصلاحی برای نظام ایران است. برای بررسی تطبیقی، شاخص‌های زیر در نظر گرفته شدند:

۱. مبنای قانونی تفهیم اتهام: وجود مواد قانونی صریح، جامع و قابل اجرا: وجود مواد قانونی صریح و جامع، پایه و اساس تحقق حقوق دفاعی متهم را فراهم می‌کند. در نظام فرانسه، قوانین به‌طور مشخص حقوق متهم و نحوه اطلاع‌رسانی را تعیین کرده‌اند، در حالی که در ایران، پراکندگی و نبود تعریف دقیق تفهیم اتهام باعث تفسیرهای مختلف و اجرای ناقص آن می‌شود. این شاخص، اهمیت تدوین قوانین روشن و قابل اجرا را نشان می‌دهد.

۲. فرآیند اجرایی: نحوه اطلاع‌رسانی، حضور وکیل و دسترسی متهم به مستندات: نحوه اطلاع‌رسانی به متهم، امکان حضور وکیل و دسترسی به مستندات پرونده تعیین‌کننده کیفیت دادرسی است. اجرای نظام‌مند این مراحل باعث شفافیت، پیشگیری از سوءتفاهم و تضمین امکان دفاع مؤثر می‌شود. نبود رویه یکنواخت در ایران موجب نابرابری حقوقی و کاهش اثرگذاری تفهیم اتهام می‌گردد.

۳. زیرساخت‌های فناوری و دیجیتال: سامانه‌های پرونده سایبری و امکان ابلاغ دیجیتال: سامانه‌های پرونده سایبری و ابلاغ دیجیتال، دسترسی سریع و امن متهم و وکیل به اطلاعات پرونده را فراهم می‌کنند. در فرانسه، این زیرساخت‌ها با قوانین مطابقت دارد، اما در ایران چالش‌هایی مانند احراز هویت و مستندسازی الکترونیکی مانع تحقق کامل این هدف می‌شوند. تقویت زیرساخت‌ها، کلید بهبود شفافیت و سرعت دادرسی است.

۴. ضمانت‌های اجرایی: امکان اعتراض به کیفیت اطلاع‌رسانی و نقش نظارت قضایی: وجود امکان اعتراض متهم به کیفیت اطلاع‌رسانی و نظارت فعال قاضی، حقوق دفاعی را تضمین می‌کند. بدون این ضمانت‌ها، اجرای تفهیم اتهام صرفاً شکلی خواهد بود و متهم قادر به پیگیری نقض حقوق خود نخواهد بود. بنابراین، ایجاد سازوکارهای نظارتی و اجرایی قوی، از ضروریات نظام دادرسی منصفانه است.

۵. آگاهی واقعی و مؤثر متهم: میزان درک متهم از اتهام و توانایی دفاع مؤثر: توانایی متهم برای درک دقیق اتهام و مستندات پرونده، شرط لازم برای ارائه دفاع مؤثر است. آگاهی واقعی فراتر از اطلاع شکلی است و مستلزم زبان قابل فهم، آموزش کافی ضابطان و دسترسی کامل به اطلاعات است. بدون تحقق این شاخص، حق دفاع متهم عملاً محدود و دادرسی ناعادلانه خواهد بود.

۱. مبنای قانونی

در ایران، هرچند مواد ۱۹۰ و ۱۹۷ قانون آیین دادرسی کیفری و اصول ۳۲ و ۳۵ قانون اساسی حقوق متهمان را تصریح کرده‌اند، اما فاقد تعریف جامع و دستورالعمل اجرایی مشخص برای پرونده‌های سایبری هستند. این نقص باعث می‌شود برداشت‌ها و اجرای تفهیم اتهام متغیر باشد و حقوق دفاعی متهم به‌طور کامل تضمین نشود. در مقابل، فرانسه با ماده ۱۱۴ و مواد ۶۳-۱ و ۶۳-۳، تعریف روشن از حق اطلاع از اتهام، سازوکار حضور وکیل و ارائه مستندات را فراهم کرده است. این چارچوب شفاف و عملیاتی، امکان اجرای مؤثر تفهیم اتهام و حفاظت واقعی از حقوق دفاعی متهمان را فراهم می‌کند.

۲. فرآیند اجرایی

در ایران، اطلاع‌رسانی به متهم غالباً شکلی است و حضور وکیل محدود به مراحل بعدی یا صدور قرار نهایی است؛ همچنین ارائه مستندات ناقص و پراکنده باعث می‌شود متهم نتواند ماهیت اتهام را به‌طور کامل درک کند و دفاع مؤثری ارائه دهد. در مقابل، فرانسه با اطلاع‌رسانی کامل و مستند، حضور وکیل از ابتدای بازجویی و دسترسی دیجیتال به پرونده و مستندات، شرایطی فراهم کرده است که متهم به شکل واقعی از اتهام آگاه باشد و بتواند از حقوق دفاعی خود بهره‌مند شود. این فرآیند موجب افزایش شفافیت، عدالت و اعتماد به نظام قضایی می‌شود. بنابراین، تجربه فرانسه نمونه‌ای عملی برای رفع خلأهای عملی در ایران است و می‌تواند مبنای اصلاحات اجرایی و قانونی قرار گیرد.

۳. زیرساخت‌های فناوری

فرانسه با بهره‌گیری همزمان از قانون و فناوری، امکان دسترسی مؤثر و شفاف متهم به پرونده را فراهم کرده است. استفاده از سامانه دیجیتال پرونده، ویدئوکنفرانس، ابلاغ الکترونیکی با امضای دیجیتال و دسترسی آنلاین به مستندات، علاوه بر تسریع دادرسی، تضمین می‌کند متهم می‌تواند از راه دور با وکیل خود تعامل داشته باشد و دفاع مؤثری ارائه دهد. در مقابل، ایران هنوز در مراحل توسعه زیرساخت‌های دیجیتال است و فاصله قابل توجهی با استانداردهای بین‌المللی دارد، به‌خصوص در زمینه ابلاغ الکترونیکی مطمئن و دسترسی امن به پرونده. بنابراین، برای ارتقای کیفیت تفهیم اتهام و تحقق حق دفاع، ایران نیازمند سرمایه‌گذاری جدی در زیرساخت‌های فناوری و سازوکارهای قانونی مکمل است.

۴. ضمانت‌های اجرایی

در ایران، محدودیت در امکان اعتراض متهم، پراکندگی نظارت قضایی و نبود دستورالعمل اجرایی برای پرونده‌های سایبری ، منجر به ضعف در حفاظت از حق دفاع و کاهش اثربخشی تفهیم اتهام می‌شود. در مقابل، فرانسه با فراهم کردن امکان اعتراض متهم به کیفیت اطلاع‌رسانی، نظارت فعال قاضی تحقیق و مستندسازی دقیق مراحل، یک رویه قضایی منسجم و قابل پیش‌بینی ایجاد کرده است. این اقدامات باعث تضمین واقعی حقوق دفاعی، شفافیت دادرسی و کاهش احتمال سوءاستفاده از قدرت تحقیقاتی می‌شوند. تجربه فرانسه نشان می‌دهد که ایجاد دستورالعمل‌های عملی و مکانیزم‌های نظارتی کارآمد، شرط لازم برای تحقق عدالت و دفاع مؤثر در پرونده‌های سایبری است.

۵. آگاهی واقعی و مؤثر متهم

در ایران، پیچیدگی‌های فنی پرونده‌ها، فقدان مستندات کامل و محدودیت در دسترسی به وکیل، باعث می‌شود متهم نتواند اتهام و شواهد آن را به‌طور دقیق درک کند و دفاع مؤثری ارائه دهد. در مقابل، فرانسه با ترکیب الزام قانونی به اطلاع‌رسانی شفاف، حضور وکیل و دسترسی دیجیتال به مستندات، اطمینان حاصل می‌کند که متهم آگاهانه می‌تواند در دفاع خود شرکت کند. این رویه منجر به شفافیت، عدالت و تحقق اصول دادرسی منصفانه می‌شود. در نتیجه، تجربه فرانسه نمونه‌ای عملی از تحقق هدف اصلی تفهیم اتهام آگاهی واقعی و مؤثر متهم را ارائه می‌دهد که می‌تواند برای اصلاح نظام ایران الگویی مفید باشد.

جدول ۲. تفهیم اتهام در جرائم سایبری با تأکید بر تضمین حقوق دفاعی متهم؛ بررسی تطبیقی حقوق ایران و فرانسه (منبع: یافته‌های پژوهش)

شاخص	ایران	فرانسه
تحلیل تطبیقی		
مبنای قانونی	مواد ۱۹۰ و ۱۹۷ قانون آیین دادرسی کیفری؛ بدون تعریف جامع	ماده ۱۱۴ و مواد ۶۳-۱ و ۶۳-۳؛ تعریف روشن و جامع
فرآیند اجرایی	اطلاع‌رسانی غالباً شکلی، وکیل محدود	اطلاع‌رسانی کامل، حضور وکیل از ابتدا، دسترسی به مستندات
		فرانسه امکان دفاع مؤثر را تضمین کرده است
زیرساخت‌های فناوری	سامانه ثنا؛ محدودیت در پرونده دیجیتال	سامانه دیجیتال پرونده، ویدئوکنفرانس، ابلاغ الکترونیکی
		فرانسه تلفیق فناوری و قانون دارد، ایران فاصله دارد
ضمانت‌های اجرایی	اعتراض محدود، نظارت قضایی پراکنده	امکان اعتراض، مستندسازی، نظارت فعال قاضی
		فرانسه ضمانت‌های عملی دارد، ایران نیازمند اصلاحات
آگاهی مؤثر متهم	ناقص؛ پیچیدگی فنی و دسترسی محدود	کامل؛ ترکیب اطلاع‌رسانی، وکیل و مستندات دیجیتال
		فرانسه موفق به تحقق هدف تفهیم اتهام شده است

نقاط قوت و ضعف نظام‌ها

نظام‌های قضایی ایران و فرانسه هرکدام با نقاط قوت و ضعف خاص خود در زمینه تفهیم اتهام در جرائم سایبری مواجه هستند. در ایران، از جمله نقاط قوت می‌توان به پشتیبانی قانونی از اصل تفهیم اتهام اشاره کرد، زیرا قانون اساسی و قانون آیین دادرسی کیفری بر ضرورت اطلاع‌رسانی دقیق به متهم تأکید دارند و حق حضور وکیل در مراحل مختلف دادرسی به رسمیت شناخته شده است. همچنین، رعایت نسبی اصول دادرسی عادلانه و حق دفاع، پایه‌ای برای حمایت از حقوق متهمان فراهم کرده است. با این حال، نظام قضایی ایران با چالش‌های قابل توجهی مواجه است. فقدان دستورالعمل‌های اجرایی مشخص برای مراحل عملی تفهیم اتهام در جرائم سایبری و استانداردهای روشن، باعث سردرگمی در اجرای قانون می‌شود. ضعف زیرساخت‌های دیجیتال و فناوری اطلاعات نیز مانع ابلاغ سریع و شفاف اتهام شده و دسترسی متهم به

پرونده و مستندات مرتبط محدود است، که این مسأله امکان دفاع مؤثر را کاهش می‌دهد. اطلاع‌رسانی غالباً شکلی و ناقص انجام می‌شود و هماهنگی میان دستگاه‌های مختلف قضایی و پلیس فتا ناکافی است.

در فرانسه، نقاط قوت نظام قضایی شامل چارچوب قانونی شفاف و جامع، امکان حضور وکیل از نخستین مراحل تحقیقات و دسترسی متهم به پرونده‌ها و مستندات دیجیتال است. علاوه بر این، نظارت فعال قضات و فراهم بودن امکان اعتراض، اجرای مؤثر حقوق دفاعی را تضمین می‌کند. با این حال، این نظام نیز بدون چالش نیست. پیچیدگی فنی پرونده‌ها و حجم بالای داده‌های دیجیتال نیازمند حضور کارشناسان متخصص است، و موازنه میان حفظ حریم خصوصی متهم و دسترسی کامل او به پرونده گاهی محدودیت ایجاد می‌کند. همچنین، اجرای مؤثر فرآیند تفهیم اتهام در جرائم سایبری مستلزم تخصص فنی و تجربه قضایی بالا است، که در نبود آن احتمال خطا و تأخیر افزایش می‌یابد. به این ترتیب، هر دو نظام نقاط قوت قانونی و ساختاری دارند، اما برای تحقق کامل حقوق متهم و اجرای عدالت در حوزه جرائم سایبری، نیازمند تقویت زیرساخت‌ها، آموزش تخصصی و تدوین دستورالعمل‌های عملیاتی هستند.

در نمودار زیر، ارتباط میان نظام حقوقی، فرآیند تفهیم اتهام، زیرساخت‌های فناوری و حقوق دفاعی متهم در ایران و فرانسه نمایش داده شده است:

این چارچوب نشان می‌دهد که نظام حقوقی پایه و مبنای اصلی است. همچنین، فرآیند تفهیم اتهام و زیرساخت‌های فناوری نقش میانجی دارند که نتیجه نهایی آن، تضمین حقوق دفاعی و دادرسی منصفانه است. پس در نظام حقوقی فرانسه تمام اجزا هم‌افزایی دارند اما در ایران، خلأ در زیرساخت‌ها و فرآیند تحقق این موضوع را با چالش مواجه کرده است.

نتیجه‌گیری

تجزیه و تحلیل تطبیقی نهاد تفهیم اتهام در جرائم سایبری در ایران و فرانسه نشان می‌دهد که در عصر فناوری اطلاعات، مفهوم سنتی تفهیم اتهام به طور قابل توجهی دگرگون شده و نیازمند بازنگری جدی است. در حالی که در گذشته، تفهیم اتهام عمدتاً به معنای اعلام عنوان جرم به متهم و ارائه فرصت دفاع بود، در دنیای امروز، با پیچیدگی‌های فنی جرائم سایبری، ضرورت دارد که متهم به طور واقعی و مؤثر از ماهیت اتهام، مستندات فنی و حقوق قانونی خود آگاه شود. یکی از نتایج کلیدی پژوهش این است که وجود قوانین صریح به تنهایی برای تضمین حقوق دفاعی کافی نیست. تجربه ایران نشان داد که باوجود مواد قانونی نظیر ۱۹۰ و ۱۹۷ قانون آیین دادرسی کیفری، خلأ در فرآیند اجرایی، زیرساخت‌های دیجیتال ناکافی و فقدان دستورالعمل‌های تخصصی موجب می‌شود که اصل آگاهی واقعی متهم از اتهام در عمل محقق نگردد. این امر نشان می‌دهد که قانون، به تنهایی، بدون هماهنگی با فناوری، آموزش و رویه قضایی، نمی‌تواند نقش خود را به شکل مؤثر ایفا کند. از سوی دیگر، مطالعه نظام فرانسه به ما نشان می‌دهد که تلفیق قانون، رویه قضایی و فناوری، راهکار مؤثری برای تحقق حقوق دفاعی متهم در جرایم پیچیده سایبری است. در فرانسه، حضور وکیل از نخستین لحظات بازجویی، ارائه مستندات پرونده به صورت دیجیتال، امکان دسترسی متهم به اطلاعات ویدئویی و اسناد فنی، و وجود سازوکارهای اعتراض و نظارت قضایی، موجب شده است که تفهیم اتهام به یک حق واقعی و عملی تبدیل شود. این تجربه اثبات می‌کند که حق دفاع و اطلاع واقعی متهم تنها در بستر عملیاتی، قابل تحقق است و صرفاً اعلام قانونی اتهام کافی نیست.

نتیجهٔ دیگری که از تحلیل تطبیقی می‌توان استخراج کرد، اهمیت آموزش تخصصی قضات و ضابطان است. در ایران، بسیاری از مشکلات اجرایی ناشی از عدم آگاهی کافی مقام قضایی و ضابطان از ماهیت فنی جرائم سایبری و ادله دیجیتال است. این مسئله موجب می‌شود که حتی در صورت وجود قانون، تفهیم اتهام ناقص و ناکافی باشد. در فرانسه، آموزش‌های تخصصی و همکاری مستمر با کارشناسان فناوری اطلاعات، سطح اجرایی فرآیند تفهیم اتهام را به شکل چشمگیری ارتقا داده است. یکی دیگر از جنبه‌های مهم این تحقیق، ضرورت تقویت زیرساخت‌های فناوری اطلاعات قضایی است. در پرونده‌های سایبری، بسیاری از مستندات به صورت دیجیتال و پیچیده هستند و دسترسی متهم و وکیل به این مستندات بدون سامانه‌های الکترونیکی امکان‌پذیر نیست. تجربه فرانسه نشان داد که سامانه‌های پرونده دیجیتال و امکان ابلاغ و دسترسی از راه دور، نه تنها کارآیی دادرسی را افزایش می‌دهند، بلکه نقش مهمی در تضمین حقوق دفاعی متهم دارند.

تحلیل تطبیقی همچنین نشان داد که فرآیند تفهیم اتهام باید به عنوان یک فرآیند مستمر و چندبعدی دیده شود، نه یک اقدام یک‌باره. در ایران، اغلب تفهیم اتهام در یک مرحله و به شکل شکلی انجام می‌شود، در حالی که فرانسه این فرآیند را به صورت چند مرحله‌ای، با امکان بازنگری، دسترسی دیجیتال و حضور وکیل از ابتدا تا پایان تحقیقات طراحی کرده است. این رویکرد موجب می‌شود که حق دفاع متهم حتی در پیچیده‌ترین پرونده‌های سایبری نیز حفظ شود.

یکی دیگر از دستاوردهای پژوهش حاضر، روشن شدن اهمیت فرهنگ‌سازی قضایی و حقوقی است. حتی با وجود قوانین و زیرساخت‌های دیجیتال مناسب، بدون ایجاد فرهنگ رعایت حقوق دفاعی متهم و آگاهی قوه قضاییه و ضابطان از اهمیت

تفهیم اتهام، احتمال نقض حقوق متهم و چالش‌های اجرایی همچنان بالاست. بنابراین، اصلاحات حقوقی باید همزمان با برنامه‌های آموزشی و فرهنگ‌سازی قضایی اجرا شوند. در نهایت، می‌توان گفت که تحقق دادرسی منصفانه در جرائم سایبری بدون هماهنگی میان سه عنصر قانون، فناوری و آموزش عملی نیست. قوانین، صرفاً چارچوب را فراهم می‌کنند؛ فناوری امکان اجرای دقیق و سریع را فراهم می‌آورد؛ و آموزش، تضمین می‌کند که حقوق متهم در طول فرآیند دادرسی رعایت شود.

نتایج پژوهش حاضر نشان می‌دهد که تفهیم اتهام در جرائم سایبری بیش از یک الزام قانونی، یک حق بنیادین و ابزار اصلی تضمین حقوق دفاعی متهم است. در ایران، قوانین موجود کافی هستند اما فقدان زیرساخت عملیاتی، آموزش ناکافی و نبود دستورالعمل تخصصی مانع تحقق مؤثر این حق شده است. در مقابل، فرانسه با ترکیب قانون، فناوری و آموزش، نمونه موفقی از اجرای مؤثر تفهیم اتهام در پرونده‌های سایبری ارائه داده است. بنابراین، اجرای مؤثر تفهیم اتهام در ایران نیازمند اصلاحات همزمان در قانون، فناوری و آموزش است. تنها با ایجاد هماهنگی میان این سه عنصر، می‌توان به تحقق دادرسی منصفانه، حق دفاع مؤثر و کاهش نقض حقوق متهم در جرائم سایبری دست یافت. همچنین یافته‌های پژوهش نشان می‌دهد که بهره‌گیری از تجربه بین‌المللی و بازنگری در سازوکارهای داخلی، نه تنها حقوق متهمان را تضمین می‌کند، بلکه موجب افزایش کارآیی و مشروعیت نظام قضایی ایران در حوزه جرائم سایبری خواهد شد.

راهکارهای پیشنهادی

۱. آموزش تخصصی قضات و مأموران پلیس سایبری: برگزاری دوره‌های منظم تخصصی برای قضات، بازپرس‌ها و افسران پلیس فتا درباره جرائم سایبری و حقوق دفاع متهم. این آموزش‌ها باعث می‌شود خطاهای ناشی از کم‌اطلاعی کاهش یابد و اجرای تفهیم اتهام با دقت و عدالت بیشتری انجام شود.

۲. راه‌اندازی سامانه مشاوره حقوقی فوری آنلاین برای متهمان: ایجاد یک سامانه آنلاین که متهمان بتوانند بلافاصله به وکیل یا مشاور حقوقی دسترسی پیدا کنند. این اقدام به افزایش شفافیت و کاهش فشار روانی متهم کمک کرده و دفاع مؤثر را تسهیل می‌کند.

۳. طراحی فرم استاندارد تفهیم اتهام ویژه جرائم سایبری: تهیه فرم واحد شامل جزئیات اتهام، مستندات دیجیتال و نکات کلیدی حقوقی، مخصوص جرائم سایبری. این فرم باعث می‌شود متهم از اتهام و اسناد مرتبط به‌طور کامل مطلع شود و از سردرگمی جلوگیری گردد.

۴. پیگیری الکترونیکی زمان‌بندی شده برای مراحل دادرسی: ایجاد سیستم اطلاع‌رسانی خودکار که زمان‌بندی مراحل دادرسی و فرصت‌های قانونی برای دفاع را به متهم یادآوری کند. این اقدام از تأخیرهای غیرضروری جلوگیری کرده و دسترسی به وکیل و مدارک را بهبود می‌بخشد.

۵. ایجاد واحد نظارت مستقل بر اجرای تفهیم اتهام در جرائم سایبری: تشکیل یک نهاد یا واحد مستقل در قوه قضاییه برای نظارت بر صحت و شفافیت اجرای تفهیم اتهام. این واحد می‌تواند شکایات متهمان را بررسی کرده و استانداردهای عملیاتی را در سراسر کشور تضمین کند.

منابع

۱. احمدی، زهرا. (۱۴۰۳). فرصت‌ها و تهدیدهای فضای سایبری در عرصه قانون‌گذاری. تهران: گیوا.

۲. استویج، استیون. (۱۴۰۰). مطالعاتی در حقوق بین الملل خصوصی. ترجمهٔ نجمه رزمخواه، تهران: مجد.

۳. السان، مصطفی. (۱۴۰۰). حقوق فضای مجازی. تهران: شهر دانش.

۴. الهی‌منش، محمدرضا. (۱۴۰۱). محشای قانون جرایم رایانه ای. تهران: مجد.

۵. بیکی شورکی، مهدی و فلاح، محمدرضا. (۱۴۰۳). «بررسی تغییرات ضروری در ساختار، سازمان و تشکیلات قضایی برای اجرای دادرسی الکترونیکی». مطالعات حقوقی فضای مجازی، ۲(۳)، ۲۹-۴۰.

۶. سیدحسینی، لیلا. (۱۴۰۴). بررسی سیاست نظارت الکترونیکی در نظام کیفری ایران. تهران: مهراب.

۷. عباسی، محمود؛ رئیسی، لیلا و قاسم‌زاده الیاسی، فلورا. (۱۴۰۴). حقوق فضای مجازی. تهران: شهر دانش. تهران: میزان.

۸. غلامی‌نیا، محمدصادق. (۱۴۰۳). جرائم رایانه‌ای، سایبری و فضای مجازی. تهران: نسل روشن.

۹. غمامی، سید محمد مهدی و فعلی، حمید. (۱۴۰۱). «چالش‌های قانونگذاری حقوق کاربران در فضای مجازی؛ مطالعه تطبیقی دو تجربه متفاوت». مطالعات میان‌رشته‌ای ارتباطات و رسانه، ۵(۴)، ۸۱-۱۲۰.

۱۰. قائم‌فرد، سیدمحسن و محسنی، فاطمه. (۱۴۰۲). «تبیین فضای الکترونیکی: ابعاد مفهومی و حقوقی». حقوق فناوری‌های نوین، ۴(۸)، ۱-۱۹.

۱۱. محتاج، محدثه؛ خندانی، سیدپدرام و ناظمی، مهرداد. (۱۴۰۴). «بررسی قابلیت اجرای قراردادهای حساب مجازی در نظام حقوقی ایران ». مطالعات حقوقی فضای مجازی، ۴(۱)، ۵۶-۶۸.

۱۲. محمدی، پژمان؛ احمدی، خلیل و کیانپوریان نژاد، میلاد. (۱۴۰۲). «مناسبات میان هزینهٔ دادرسی و اصول دادرسی منصفانه؛ مطالعهٔ تطبیقی در حقوق ایران و انگلستان». مطالعات حقوق تطبیقی معاصر، ۱۴(۳۱)، ۲۲۱-۲۵۳.

۱۳. مزینانیان، سعیده. (۱۴۰۲). «تنظیم‌گری حریم خصوصی در فضای مجازی (مطالعه تطبیقی در حقوق ایالات متحده آمریکا، اتحادیه اروپا و ایران)». پژوهش‌های حقوق اقتصادی و تجاری، ۱(۲)، ۲۰۷-۲۳۹.

۱۴. مهدی‌پور حسین و باهنر، ناصر. (۱۴۰۳). «دلالت‌های قواعد فقهی برای سیاست‌گذاری فضای مجازی». مطالعات فقه و حقوق رسانه. ۵(۱)،۴۱-۷.

۱۵. میرکتولی، بهنوش. (۱۴۰۳). کاوش در جرایم مرتبط با فضای مجازی و قوانین مقابله با آن. تهران: اندیشه عصر.

۱۶. نصراللهی، محمدصادق. (۱۴۰۳). «ماهیت و مسائل حقوقی پالایش فضای مجازی». مطالعات فقه و حقوق رسانه، ۶(۲)، ۳۶-۷.

17. Abdullah, H. O., Maqsood, M., & Nadeem, A. (2025). Digital Evidence in Criminal Proceedings: Legal Standards, Chain of Custody, and Evidentiary Reliability in the Digital Era. Research Journal for Social Affairs, 3(5), 795-805.

18. Aleksandrovich, L. (2023). Cyber Law: Addressing Legal Challenges in the Digital Age. Journal of Law and Digital Policy, 1(3), 96-117.

19. Ajoy, P. B. (2024). Developing an analytical definition of cybercrime. Journal of Humanities and Social Science, 29(6), 12-19 .

20. Bace, B., Gokce, Y., and Tatar, U. (2024). Cyber Law: Addressing Legal Challenges in the Digital Age. Journal of Telecommunications Policy, 48(4), 408-436.

21. Brenner, S, W. (2024). Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law. Ohio: University of Dayton School of Law.

22. Cerekja, B., and Mucollari, O. (2024). Right to a fair trial under Article 6 of the ECHR: The balance between efficiency and fairness in European criminal law. International Journal of Law Review, 36(1), 183-208.

23. Fahey, E. (2024). The evolution of EU–US cybersecurity law and policy: on drivers of convergence. Journal of European Integration, 46(7), 1073-1088.

24.Kandy, S., Fathoni, T., and Lubis, A. (2024). Evolution and Challenges of Cyber Law in the Digital Era: Case Studies in Developing Countries. International Journal of Assulta of Law Review, 1(1), 1-10.

25.Macidov, S. T. oglu. (2023). Prosecuting Cybercrimes under International Legal Frameworks: Challenges and Innovations. Futurity Economics & Law, 3(3), 80-96.

26.Muharman, D. (2025). The Evolution of Cyber Law: Protecting Privacy and Security in the Digital Age. Journal of Information Systems Engineering & Management, 10(5), 386-395.

27.Perez, M. (2025). Proliferation of e-Evidence: Reliability Standards and the Right to a Fair Trial. European Journal of Crime, Criminal Law and Criminal Justice, 24(1), 48-73.

28.Sarkar, G., & Shukla, J. (2024). A framework for distinguishing cybercrime, cyberattacks, and related acts. Journal of Cybersecurity, 28(1), 297-320.

29.Sepaha, P. (2025). Digital and Forensic Evidence: Overcoming Challenges in Authentication, Cybercrime Prosecution, and Ensuring Justice. International Journal of Research and Analytical Reviews, 12(2), 979-991 .

30.Wall, D. S. (2024). Cybercrime: The Transformation of Crime in the Information Age (2nd ed.). Cambridge: Polity.

31.Wang, X. (2024). Global (re-)framing of cybercrime: An emerging common interest in flux of competing normative powers. Leiden Journal of International Law, 36(6), 1-26.

32.فرانسوی

33.Abitbol, C. (2025). Le droit français peut-il réprimer la nouvelle délinquance issue de l'intelligence artificielle? Actu-Juridique, 28(2), 169-193.

34.Assane Touré, P. (2025). Cybercriminalité Code pénal et textes pénaux spéciaux commentés et annotés. Paris: Harmattan.

35.Décary, D. (2024). Les téléphones cryptés et leurs impacts sur le système de justice. Criminologie, Forensique et Sécurité, 2(1), 85-109.

36.Dupont, B. (2024). La cybercriminalité. Paris: Armand Colin.

37.Ghernaouti, S. (2023). Cybercriminalité: Comprendre, prévenir, réagir. Paris: Dunod.

38.Ghernaouti-Hélie, S. (2023). La cybercriminalité Comprendre, prévenir, réagir. Paris: Eyrolles.

39.Kabyuma, C. (2024). Droit pénal et droits de l'homme à l'épreuve de la cybercriminalité. Paris: L'Harmattan RDC.

40.Leonetti, X. (2025). Le Petit Cyber-compliance 2025 L'essentiel en bref. Paris: Dunod.

41.Ollard, R. (2023). Ordre et désordres du droit pénal spécial de la cybercriminalité. Paris: Lexbase.

42.Signor, A. (2023). Cybercriminalité: Aspects de procédure et de droit pénal matériel. Paris: La Charte.