

## نقش پلیس در جمع‌آوری ادله الکترونیکی در فضای مجازی در نظام حقوقی ایران، فرانسه و کنوانسیون جرائم سایبری<sup>۱</sup>

تاریخ دریافت: ۹۷/۱۰/۱۲ تاریخ پذیرش: ۹۸/۰۲/۰۵

از صفحه ۱۳۱ تا ۱۴۸

رامین دلخون اصل<sup>۲</sup>، ایرج گلدوزیان<sup>۳</sup>، کیومرث کلانتری<sup>۴</sup>

### چکیده

**زمینه و هدف:** امروزه فناوری اطلاعات ابزاری در دست تبهکاران و رایانه‌ها باعث تسهیل وقوع جرائم در دنیای مجازی و حتی دنیای واقعی شده است. پژوهش حاضر با هدف بررسی تطبیقی نقش و اختیارات پلیس در جمع‌آوری ادله الکترونیکی در نظام حقوقی ایران و کشور فرانسه و کنوانسیون جرائم سایبری انجام شده است. **روش:** پژوهش حاضر از نظر هدف، کاربردی و براساس روش، توصیفی-تحلیلی است که بر پایه منابع کتابخانه‌ای با استفاده از منابع موجود، به بررسی، توصیف و تحلیل ابعاد و زوایای گوناگون موضوع پژوهش پرداخته شده و تجزیه و تحلیل اطلاعات جمع‌آوری شده به صورت کیفی و مبتنی بر استنتاج محقق از منابع و متون بوده است.

**یافته‌ها:** یافته‌های پژوهش بیانگر آن است که فرآیند تحقیق، کشف و جمع‌آوری ادله در فضای مجازی براساس قوانین ایران، فرانسه و کنوانسیون جرائم سایبری بر عهده پلیس گذاشته شده است. تفاوت‌ها و شباهت‌های فراوانی بین مقررات دو کشور و کنوانسیون وجود دارد و در ایران در بحث تفتیش و توقیف و حفاظت از ادله، پلیس نقش محوری دارد.

**نتیجه‌گیری:** نتایج نشان می‌دهد که پلیس در جمع‌آوری ادله در فضای مجازی به جهت بی‌هویتی افراد و همچنین سرعت ناپدید شدن صحنه جرم، با چالش جدی مواجه است و تحصیل اینگونه ادله، مستلزم تخصص کافی در زمینه فناوری اطلاعات و رعایت قواعد و اصول فنی است. در نظام حقوقی هر دو کشور ایران و فرانسه، پلیس اولین کسی است که با ادله الکترونیک برخورد می‌کند و در جمع‌آوری، مستندسازی و حتی ارزیابی ادله، نقش کلیدی دارد.

**کلید واژه‌ها:** ادله الکترونیکی، فضای مجازی، پلیس، ایران، فرانسه، کنوانسیون جرائم سایبری.

**استناد:** دلخون اصل، رامین؛ گلدوزیان، ایرج و کلانتری، کیومرث (تابستان ۱۳۹۸). نقش پلیس در جمع‌آوری ادله الکترونیکی در فضای مجازی در نظام حقوقی ایران، فرانسه و کنوانسیون جرائم سایبری. فصلنامه پژوهش‌های اطلاعاتی و جنایی، ۱۴(۵)، صص ۱۴۸-۱۳۱.

۱. برگرفته از رساله دکتری حقوق کیفری دانشگاه آزاد اسلامی واحد گرگان با عنوان «تحصیل دلیل کیفری در فضای مجازی در حقوق ایران و با بررسی تطبیقی آن در حقوق فرانسه».

۲. دانشجوی دکتری حقوق کیفری و جرم‌شناسی دانشگاه آزاد اسلامی واحد گرگان، delkhood@ramin@yahoo.com

۳. استاد حقوق کیفری و جرم‌شناسی دانشگاه آزاد اسلامی واحد گرگان، نویسنده مسئول: miramts@yahoo.com

۴. دانشیار حقوق کیفری و جرم‌شناسی دانشگاه آزاد اسلامی واحد گرگان، kalantar@nit.ac.ir

## مقدمه

کشف حقیقت و اجرای عدالت در فرآیند کیفری صرفاً با استناد به دلیل امکان‌پذیر است، بنابراین دلیل در فرآیند دادرسی کیفری، نقش اساسی دارد. یکی از مباحث نوین در نظام حقوقی، بحث ادله الکترونیکی و جمع‌آوری دلایل در فضای مجازی است؛ بحثی که همپای تحولات در عرصه فناوری اطلاعات، در نظام حقوقی در حال دگرگون شدن است. با توسعه فناوری اطلاعات و تغییر روش ارتکاب جرم، جمع‌آوری ادله الکترونیکی به عنوان مهم‌ترین مرحله در فرایند رسیدگی کیفری محسوب می‌شود. پلیس در زمینه ارتکاب جرائم در فضای مجازی با حجم انبوهی از ادله روبرو می‌شود، جمع‌آوری و تفکیک ادله، مراحل پیچیده‌ای دارد که توسط پلیس انجام و پس از مستندسازی به عنوان ادله وقوع جرم به مراجع قضایی ارائه و توسط مقام قضایی مورد استناد قرار می‌گیرد. در کشور ما پس از تصویب قانون جرائم رایانه‌ای در سال ۱۳۸۸، به دلیل تخصصی بودن حوزه فناوری اطلاعات و لزوم تعیین ضابط برای این قانون، پلیس فضای تولید و تبادل اطلاعات (فتا) در بهمن‌ماه ۱۳۸۹ با هدف ایجاد امنیت و پیشگیری از وقوع جرم و جمع‌آوری ادله تشکیل شد.

اهمیت تحقیق حاضر با توجه به اینکه جرائم رایانه‌ای از مسائل مهم جامعه امروزی بوده و دستگاه انتظامی و قضایی به نوعی درگیر مسائل اثباتی این نوع جرائم هستند، برکسی پوشیده نیست. این حوزه از جرائم از مسائل جدید در نظام حقوقی بوده و در سال‌های آینده، جامعه با حجم انبوهی از جرائم در فضای مجازی مواجه خواهد شد. بنابراین، ضرورت دارد تحقیقات جامعی در حوزه جمع‌آوری ادله در فضای مجازی انجام و قوانین کشورهای مختلف با هم تطبیق و مورد بررسی قرار گیرند. به لحاظ اینکه ایران به کنوانسیون جرائم سایبری<sup>۱</sup> بوداپست<sup>۲</sup> (۲۰۰۱) ملحق نشده است، لذا مطالعه تطبیقی مقررات کشور ایران و فرانسه و همچنین این کنوانسیون در جمع‌آوری ادله کیفری در

### 1. Convention on Cybercrime

۲- کنوانسیون جرائم سایبری بوداپست، نخستین معاهده بین‌المللی است که به جرائم رایانه‌ای و اینترنتی می‌پردازد. این کنوانسیون توسط شورای اروپا در هشتم نوامبر ۲۰۰۱ به تصویب رسیده و از ۲۳ نوامبر ۲۰۰۱ در شهر بوداپست، در کنفرانس بین‌المللی جرائم سایبر، جهت امضاء مفتوح مانده است. از ابتدای ژوئیه ۲۰۰۴ کنوانسیون به اجرا درآمد و تا سال ۲۰۱۳، ۳۹ کشور از جمله کشورهای عضو اتحادیه اروپا این کنوانسیون را تصویب کردند و ۱۲ کشور نیز آن را امضاء کرده بودند. در حال حاضر، براساس آخرین اطلاعات موجود در وبسایت کنوانسیون، ۶۱ کشور کنوانسیون را تصویب و ۴ کشور آن را امضاء کردند و کشور ما هنوز به این کنوانسیون ملحق نشده است.

فضای مجازی با توجه به نقش و اختیارات پلیس می‌تواند سازنده و راهگشا باشد. بنابراین، هدف اصلی از این تحقیق، مطالعه تطبیقی نقش و اختیارات پلیس در جمع‌آوری ادله در فضای مجازی در نظام حقوق ایران، فرانسه و کنوانسیون جرائم سایبری است و اهداف فرعی این تحقیق شامل تبیین چالش‌های موجود پیش‌روی پلیس و ارائه راهکارهای نظامند و بیان اصول و مقررات حاکم در جمع‌آوری ادله در فضای مجازی است. برای نیل به این اهداف، این پرسش‌ها مطرح می‌شود که جایگاه و اختیارات پلیس در جمع‌آوری ادله الکترونیکی در فضای مجازی در حقوق ایران، فرانسه و کنوانسیون جرائم سایبری چیست؟ و اینکه آیا جمع‌آوری ادله توسط پلیس مستلزم رعایت اصول، مقررات، مهارت‌های فنی و تخصصی است؟ همچنین، راهکارهای مقرر در قوانین ایران در زمینه جمع‌آوری ادله الکترونیک در مقایسه با قوانین کشور فرانسه و کنوانسیون راهگشا و کارآمد است یا خیر؟

در کشورهای غربی به پلیس حوزه فناوری اطلاعات، پلیس سایبر می‌گویند. براساس ماده ۳۵ کنوانسیون جرائم سایبری، «اعضاء موظف‌اند یک مرکز تماس ۲۴ ساعته در دسترس در ۷ روز را تأسیس کنند تا معاضدت فوری جهت تحقیقات یا رسیدگی‌های کیفری مرتبط با داده‌ها و سیستم‌های رایانه‌ای یا جمع‌آوری ادله الکترونیکی جرائم را تضمین کنند» (جلالی فراهانی، ۱۳۹۵، ص ۱۲۶). در ایران نیز با تصویب قانون جرائم رایانه‌ای در سال ۱۳۸۸ و به ویژه آیین‌نامه اجرایی ماده ۵۴ آن (مصوب ۱۳۹۳/۰۵/۱۲) در خصوص جمع‌آوری و استنادپذیری ادله الکترونیکی و مشخص شدن ضوابط، مقررات و اختیارات ذی‌ربط به ویژه پلیس، بسیاری از مشکلات موجود در این حوزه برطرف شده است.

فرانسه از سال ۱۹۸۸ به یک سری مقررات کیفری مخصوص مبارزه با «بزهکاری رایانه‌ای» مجهز شده است. در واقع، تا این تاریخ هیچ نوع جرم‌انگاری خاصی که شامل بزهکاری مربوط به رایانه باشد وجود نداشت. در فرانسه که حفاظت از اطلاعات و داده‌های شخصی افراد از سال ۱۹۷۰ با قانون «فناوری اطلاعات و آزادی» به وجود آمد، در سال ۱۹۷۸ در جهت حفاظت از داده‌های شخصی و حریم خصوصی و آزادی‌های مدنی و عمومی، «کمیسیون ملی فناوری اطلاعات و آزادی»<sup>۱</sup> که یک نهاد مستقل اداری

1.CNIL

است تأسیس شد (حسنی سامره، ۱۳۹۲، ص ۱۶) و دفتری تحت عنوان «دفتر مرکزی مبارزه با جرم و جنایت در فناوری اطلاعات و ارتباطات»<sup>۱</sup> طی فرمان شماره ۲۰۰-۴۰۵ در ۱۵ می ۲۰۰۰ ایجاد شده که اهداف آن مبارزه با جرائم سایبری و جمع‌آوری ادله و رمزگشایی داده‌ها است. همچنین، در فرانسه شرکت‌های خصوصی تحت عنوان «خدمات ادله رایانه‌ای» تأسیس شده‌اند. در قوانین فرانسه صرفاً مقررات عام جمع‌آوری ادله در فضای مجازی پیش‌بینی شده و به مقررات خاص این حوزه اشاره‌ای نشده است و باید در کنوانسیون این موارد را جستجو کرد. کشور فرانسه عضو کنوانسیون بوده و آن را در سال ۲۰۰۱ امضاء و در سال ۲۰۰۶ تصویب کرده است.

تحقیقات متعددی به مباحث جمع‌آوری، توقیف و تفتیش ادله در فضای مجازی پرداخته است. در مطالعات مشابه به طور غیرمستقیم و صرفاً در حوزه خاصی به این موضوع پرداخته شده است که در ادامه به تعدادی از آن‌ها اشاره می‌شود. مؤذن زادگان و شایگان (۱۳۸۸) در مقاله‌ای با عنوان «استنادپذیری و تحصیل ادله الکترونیکی در حقوق کیفری ایران» به بررسی جنبه‌های شکلی جرائم رایانه‌ای و موضوعاتی از قبیل ارزش اثباتی دلایل رایانه‌ای و مستندسازی آن‌ها، رهگیری ارتباطات اینترنتی، شنود داده‌ها، تفتیش و توقیف داده‌ها و سیستم رایانه‌ای پرداخته‌اند. محور اساسی این مقاله، استنادپذیری و تحصیل ادله الکترونیکی بوده و نویسندگان بخش مهم مقاله را به جمع‌آوری ادله اختصاص و مهم‌ترین ابزار و روش تحصیل دلیل را تفتیش و توقیف داده‌های ذخیره یا پردازش شده معرفی می‌کنند. در نهایت، به این نتیجه رسیده‌اند که قانون‌گذار ایران ارزش اثباتی ادله الکترونیکی را پذیرفته ولی با این حال، در زمینه جمع‌آوری و استنادپذیری با چالش‌های جدی از جمله عدم تخصص مقامات تعقیب و خصیصه فرامرزی مواجه است. کریمی (۱۳۹۰) نیز در پایان‌نامه خود با عنوان «جمع‌آوری و استنادپذیری ادله الکترونیکی در حقوق کیفری ایران» به بررسی چگونگی جمع‌آوری و ارائه ادله الکترونیکی به دادگاه و در نهایت میزان ارزش اثباتی ادله الکترونیکی با توجه به مبانی نظام ادله کیفری ایران و قوانین جدید ناظر بر این حوزه پرداخته و در نهایت این‌چنین نتیجه گرفته که در جمع‌آوری ادله جرم باید از مقررات

1. OCLCTIC

خاصی پیروی کرد و جمع‌آوری، نظم خاصی را می‌طلبد و به دلیل ویژگی‌های خاص اینگونه ادله، باید احتیاط و سرعت عمل در دستور کار قرار گیرد.

حسنی سامره (۱۳۹۲) در پایان‌نامه‌ای تحت عنوان «مطالعه تطبیقی تفتیش و توقیف داده‌های رایانه‌ای و سامانه‌های مخابراتی در حقوق ایران و فرانسه»، کشف و تعقیب جرائم سایبری و ضوابط ناظر بر تفتیش و توقیف داده‌های رایانه‌ای را مورد بررسی قرار داده و نتیجه گرفته که جرائم رایانه‌ای و سایبری واجد ویژگی‌های منحصر به فردی است که کشف و پیگیری اینگونه جرائم نیازمند زیرساخت‌های ملی است و اعلام می‌کند که قوانین ایران در زمینه شکلی دارای کاستی است و تأسیس نهادهای غیررسمی برای جمع‌آوری ادله الکترونیک در کشور فرانسه را به‌عنوان الگوی مناسبی برای سایر کشورها معرفی می‌کند. همچنین، شایق و ناجی زواره (۱۳۹۵) در مقاله‌ای با عنوان «مطالعه تطبیقی تحصیل دلیل کیفری در فضای سایبری در حقوق ایران، انگلستان و فرانسه با تأکید بر وظایف و اختیارات پلیس»، ضمن تعریف ادله الکترونیک و بیان ویژگی‌های اینگونه ادله، به نقش پلیس در تحصیل دلیل و چگونگی کشف ادله دیجیتال و مستندسازی ادله و تفتیش و توقیف ادله در کشور ایران، فرانسه و انگلستان پرداخته‌اند. در این مقاله، نویسندگان ضمن توضیح نحوه کشف، تفتیش و توقیف ادله، به استنادپذیری ادله جمع‌آوری شده اشاره و ادله جمع‌آوری شده از طرق غیرقانونی را فاقد اعتبار معرفی می‌کنند.

مرور پژوهش‌های انجام‌شده نشان می‌دهد محققان بدون اشاره به نقش و اختیارات پلیس، صرفاً به تحصیل ادله الکترونیکی پرداخته‌اند و صرفاً یک تحقیق، مشابه تحقیق حاضر توسط شایق و ناجی زواره (۱۳۹۵) به موضوع جمع‌آوری ادله الکترونیک در نظام حقوقی ایران، انگلستان و فرانسه با تأکید بر وظایف و اختیارات پلیس پرداخته است و در خصوص نظام حقوقی فرانسه نیز به جز ترجمه قانون آیین دادرسی کیفری و کنوانسیون جرائم سایبر، منبع دیگری به زبان فارسی در دسترس نبود. لذا پژوهش حاضر از جهت بررسی مقررات کنوانسیون جرائم سایبری واجد جنبه نوآوری است که در نظر دارد علاوه بر بیان مقررات کشور ایران، مقررات کشور فرانسه و کنوانسیون جرائم سایبری را مورد مطالعه قرار دهد.

**ادله الکترونیکی:** ادله جمع دلیل است و در لغت به معنی راهبر، رهنمون و راهنماست. در اصطلاح حقوقی، دلیل در دو مفهوم بکار می‌رود؛ در مفهوم اخص، به هر وسیله‌ای

گفته می‌شود که در قانون پیش‌بینی شده و در مراجع قضایی سبب اقناع دادرسی به واقعیت شود و در مفهوم اعم، دلیل فراهم آوردن وسایلی است که وجدان دادرس را اقناع کند. (شمس، ۱۳۹۶، ص ۲۴). مطابق ماده ۱۹۴ قانون آیین دادرسی مدنی، «دلیل امری است که اصحاب دعوا برای اثبات یا دفاع از ادعا به آن استناد می‌کنند». در حقوق کیفری، تعریفی از دلیل ارائه نشده است و تنها قانون‌گذار در ماده ۱۶۰ قانون مجازات اسلامی به احصای ادله پرداخته است (مؤذن زادگان، سلیمان دهکردی و یوشی، ۱۳۹۴، ص ۷۲). قانون آیین دادرسی کیفری مصوب ۱۳۹۲ نیز در فصل دادرسی الکترونیک تعریفی از ادله الکترونیک ارائه نکرده است، اما نویسندگان تعاریف مختلفی از دلیل الکترونیکی ارائه کرده‌اند. در تعاریف ارائه شده، ادله الکترونیکی با واژه «داده پیام» تعریف شده است که تعریف آن در ماده ۲ قانون تجارت الکترونیک، «هر نمادی از واقعه، اطلاعات یا مفهوم است که با وسایل الکترونیکی، نوری یا فناوری جدید اطلاعات تولید، ارسال، دریافت، ذخیره یا پردازش می‌شود» آمده و در ماده ۱۲ همان قانون، ارزش اثباتی داده پیام را غیرقابل رد اعلام و در موارد ۱۳ و ۱۴ همان قانون بر قابل استناد بودن آن تأکید شده است. دلیل الکترونیکی، اطلاعات ذخیره شده است که در هر نوع دستگاه الکترونیکی می‌توان یافت و از آن به عنوان دلیل در نظام حقوقی بهره گرفت (موسوی مجاب، ۱۳۹۲، ص ۴). در رابطه با ماهیت این نوع دلایل نیز به طور مختصر می‌توان گفت در فضایی غیر از فضای فیزیکی اطراف فرد موجودیت دارند و هرگونه عملیاتی بر روی آن‌ها نیز در آن فضا امکان‌پذیر است؛ چنین فضایی را فضای سایبر می‌گویند و گروهی نیز آن را فضای مجازی می‌نامند.

دلایل الکترونیکی نسبت به سایر دلایل آسیب‌پذیرتر هستند؛ زیرا به آسانی می‌توان آن‌ها را دست‌کاری، جعل یا پنهان کرد. در جمع‌آوری اینگونه ادله نیز چالش‌هایی وجود دارد که شامل حجم زیاد اطلاعات، فراملی بودن جرائم رایانه‌ای (از جمله ویروس‌ها و کرم‌ها) (دلخون اصل، ۱۳۹۲، ص ۳۲) و کمبود نیروی انسانی متخصص است. سازمان ملل در تحقیق جامع خود با بررسی میان ۶۹ کشور به این نتیجه رسیده است که در کشورهای کمتر توسعه‌یافته به طور میانگین به ازای هر صد هزار نفر کاربر فضای سایبر، ۲ درصد نیروی پلیس متخصص مشغول به فعالیت هستند؛ در حالی که این عدد برای کشورهای توسعه‌یافته ۲ تا ۵ برابر بیشتر است. همچنین، تعداد نیروهای پلیس

متخصص سایبری تمام کشورها، کمتر از ۱ درصد نسبت به کل نیروهای پلیس است (فرهادی آلاشتی و جوان جعفری بجنوردی، ۱۳۹۶، ص ۲۵).

**حفاظت و نگهداری داده‌ها:** مطابق ماده ۷۶۰ و ۷۶۱ قانون مجازات اسلامی، ارائه‌دهندگان خدمات دسترسی و خدمات میزبانی موظفاند داده‌های ترافیک و اطلاعات کاربران خود را حداقل ۶ ماه نگهداری کنند. محتوای داده، ترافیک داده و اطلاعات کاربران باید به نحوی نگهداری شوند که صحت و تمامیت محرمانگی، اعتبار و انکارناپذیری آن‌ها محفوظ بماند. حفاظت مستلزم این است که داده‌های ذخیره شده کنونی در برابر هر چیزی که باعث تغییر یا بدتر شدن وضعیت یا کیفیت فعلی آن‌ها می‌شود، محافظت شوند. «حفظ داده‌ها» به منزله ارائه و افشای آن‌ها نبوده، بلکه صرفاً به این دلیل از داده حفاظت می‌شود که در صورت لزوم، مورد بررسی و تجزیه و تحلیل قرار گیرند. مدت زمان حفاظت از داده‌ها حداکثر سه ماه است و در صورت لزوم با دستور مقام قضایی، قابل تمدید است. حفظ داده‌ها به معنای نگهداری داده‌هایی است که کماکان به شکل ذخیره وجود دارند و از آن‌ها در برابر هر چیزی که باعث تغییر یا از بین رفتن کیفیت یا وضعیت فعلی آن‌ها می‌شود، حفاظت می‌شود. اما «نگهداری داده‌ها»، به معنای نگهداری داده‌های است که هم اکنون ایجاد می‌شوند و در آینده در تصرف شخص قرار می‌گیرند. نگهداری داده‌ها بیانگر انباشته کردن داده‌ها در زمان کنونی و نگهداری یا تصرف آن‌ها در آینده است. این تعبیر فرآیند ذخیره داده‌هاست. از سوی دیگر، حفظ داده‌ها اقدامی است که داده‌های ذخیره شده را سالم و ایمن نگه می‌دارد (جلالی فراهانی، ۱۳۹۵، ص ۶۱).

**تفتیش و توقیف داده‌ها:** مهم‌ترین قدم در جمع‌آوری ادله، تفتیش<sup>۳</sup> و توقیف<sup>۴</sup> داده‌های ذخیره یا پردازش شده در سیستم‌های رایانه‌ای است. از گذشته، در قوانین آیین دادرسی کیفری کشورها قواعد خاصی برای تفتیش اماکن و اموال افراد در راستای کشف و تعقیب جرائم پیش‌بینی شده است. هدف اصلی از وضع چنین مقرراتی، حفاظت از حریم خصوصی افراد در مقابل تعرض غیرقانونی و بی‌مورد مقامات تعقیب است (دلخون

1.Data Preservation  
2.Data Retention  
3.Search  
4.Seize

اصل، ۱۳۹۳، ص ۳۵). جمع‌آوری داده‌های ذخیره شده در سیستم‌های رایانه‌ای مستلزم ورود و بازرسی محل نصب رایانه و توقیف داده‌هاست. در قانون مجازات اسلامی، مقررات ویژه‌ای در مورد تفتیش و توقیف داده‌ها و سیستم‌های رایانه‌ای در مواد ۷۶۴، ۷۶۵، ۷۶۶ و ۷۶۷ در نظر گرفته شده است و در ماده ۷۶۹، این اجازه را داده که در مواردی، مقامات بتوانند سامانه‌های رایانه‌ای را توقیف کنند. در توقیف داده‌ها و سامانه‌های رایانه‌ای در صورت ضرورت در برخورد با سیستم‌های رایانه‌ای که در قرار تفتیش و بازرسی ذکر نشده است، بازرسان می‌توانند حیطة تحقیق خود را گسترش دهند؛ مشروط به اینکه به دستور مقام قضایی باشد (موذن زادگان و شایگان، ۱۳۸۸، ص ۹۳).

**شنود داده‌ها:** نظارت یک امر ضروری جهت پیشگیری از وقوع جرم است. کنترل ارتباطات مخابراتی افراد ممنوع بوده و قانون‌گذار در ماده ۱۵۰ آیین دادرسی کیفری در موارد خاص این اجازه را داده که مأموران بتوانند با مجوز قانونی و با رعایت اصول حاکم، نسبت به کنترل و شنود مکالمات تلفنی اشخاص اقدام کنند. براساس توصیه شورای اروپا، اختیاراتی که شنود الکترونیکی را مجاز می‌دانند باید صریحاً به وسیله قانون تعریف شوند. از آنجا که شنود الکترونیکی مستقیماً بر مسائل محرمانگی فردی ضربه می‌زند باید حمایت‌های مناسبی وجود داشته باشند که تعادل متناسبی را بین حقوق فرد و منافع عدالت حفظ کنند (زندى، ۱۳۹۳، ص ۱۵۷). مقنن در ماده ۷۷۶ از قانون مجازات اسلامی، شنود محتوای در حال انتقال ارتباطات غیرعمومی در سامانه‌های رایانه‌ای یا مخابراتی را پذیرفته و رعایت مقررات راجع به شنود مکالمات تلفنی را بر آن ضروری دانسته و در تبصره، دسترسی به محتوای اطلاعات غیرعمومی ذخیره شده نظیر پست الکترونیکی یا پیامک را در حکم شنود اعلام کرده است.

با توجه به مطالعات انجام شده و نقش پلیس در جمع‌آوری ادله الکترونیکی، نمودار ۱ مدل مفهومی تحقیق را نشان می‌دهد.





نمودار ۱ - مدل مفهومی تحقیق

### روش‌شناسی تحقیق

تحقیق حاضر از نظر هدف، کاربردی و از نظر روش، توصیفی-تحلیلی است که بر پایه منابع کتابخانه‌ای، با استفاده از منابع موجود به بررسی و توصیف و تحلیل ابعاد و زوایای گوناگون موضوع پژوهش پرداخته شده است. تجزیه و تحلیل اطلاعات جمع‌آوری‌شده به صورت کیفی و مبتنی بر استنتاج محقق از منابع و متون بوده است. در این تحقیق کلیه مقررات داخلی در خصوص جمع‌آوری ادله الکترونیک و مقررات قانونی کشور فرانسه و همچنین مفاد کنوانسیون جرائم سایبری بوداپست مورد توجه قرار گرفته است. تجزیه و تحلیل داده‌ها هم عمدتاً متکی بر مقررات قانونی و ادراک و تحلیل عقلانی بوده است. بنابراین، اطلاعات لازم با توجه به موضوع تحقیق به وسیله ابزارهای سنجش کتابخانه‌ای و اسنادی گردآوری شده است. برای بررسی تطبیقی پژوهش، قوانین کشور فرانسه و همچنین مفاد کنوانسیون جرائم سایبری که به زبان فارسی ترجمه شده‌اند و همچنین مقالات و کتب موجود به زبان انگلیسی و فرانسه، مطالعه و اطلاعات گردآوری شده است.

### یافته‌های تحقیق

با توجه به افزایش جرائم رایانه‌ای که حسب اظهار مدیران پلیس فتا، افزایش ۶۰ درصدی در سال‌های اخیر داشته است، رسیدن به اهداف و کشف جرائم و مجازات مرتکبان، مستلزم جمع‌آوری ادله در فضای مجازی است. کلیه اقدامات کشف جرائم، تحقیقات مقدماتی، دستگیری متهمان، جمع‌آوری، حفظ و تفتیش ادله از وظایف و

اختیارات پلیس است و اهمیت این موضوع برکسی پوشیده نیست. انجام تحقیقات و جمع‌آوری ادله در جرائم رایانه‌ای از عهده دستگاه قضایی خارج است؛ چراکه برخلاف جرائم سنتی که دستگاه قضایی می‌تواند بدون دخالت پلیس تحقیقات را انجام دهد، تحقیقات در اینگونه جرائم، مستلزم تجهیزات فنی و سامانه‌های ارتباطی و رصد شبانه روزی فضای مجازی است که این تجهیزات صرفاً در اختیار پلیس سایبری و سازمان‌های امنیتی است. پلیس به غیر از موارد امنیتی و جرائم سازمان‌یافته، نباید برای جمع‌آوری ادله از ترفند دام‌گستری استفاده کند (تدین، ۱۳۹۳، ص ۲). کشف و جمع‌آوری ادله در فضای مجازی به درایت، هوشیاری و تخصص پلیس بستگی دارد و آموزش دستگاه‌های پلیسی و امنیتی برای رسیدن به این امر مهم، اهمیت بسزایی دارد. با بررسی و مطالعه قوانین کشور ایران و فرانسه می‌توان گفت که پلیس در هر دو کشور نقش اساسی و کلیدی در جمع‌آوری ادله الکترونیک در فضای مجازی دارد و مسئولیت جمع‌آوری و بررسی ادله جرم در جرائم رایانه‌ای بر عهده پلیس سایبری است.

با توجه به ویژگی فرامرزی بودن برخی جرائم رایانه‌ای، قانون ایران و کنوانسیون جرائم سایبری راهکاری در خصوص جمع‌آوری ادله موجود در خارج از مرزهای کشور ارائه نکرده‌اند و این امر به عنوان مهم‌ترین چالش در پلیس سایبری کشورها مطرح شده و راهکاری در این خصوص ارائه نشده است. هرچند در قانون کشورها مواردی به عنوان استثناء از جمله صلاحیت واقعی و صلاحیت جهانی و تابعیتی گنجانده شده است (جلالی فراهانی، ۱۳۹۴، ص ۴۷)، ولی با این حال، کنوانسیون به عنوان سند بین‌المللی باید با ارائه راهکار، کشورهای عضو را ارشاد و راهنمایی می‌کرد. در خصوص جمع‌آوری ادله در خارج از مرزهای کشور، در کشور فرانسه راه حل نیابت قضایی (کیومنر<sup>۱</sup>، ۲۰۰۹، ص ۲۴۷) و استرداد مجرمان ارائه شده است.

**اختیارات پلیس در جمع‌آوری ادله:** بررسی‌های انجام شده در این تحقیق نشان می‌دهد در قوانین کشور ایران، فرانسه و کنوانسیون جرائم سایبری، جمع‌آوری ادله الکترونیکی شامل حفاظت، تفتیش، توقیف و شنود داده‌ها است. پلیس براساس قوانین کشور ایران، در تفتیش و توقیف داده‌ها نقش اساسی دارد و کلیه مراحل توسط پلیس انجام می‌شود. پلیس سایبری با توجه به اینکه به تجهیزات فنی و افراد متخصص در

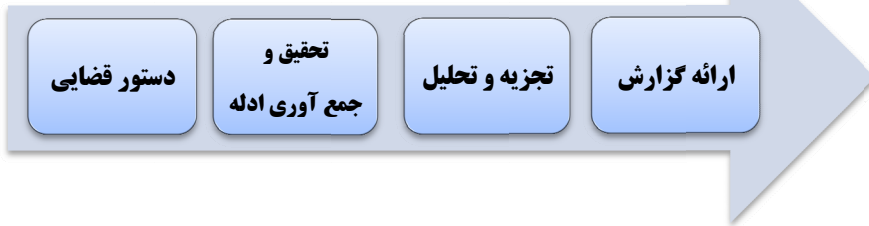
1. Quemener

حوزه رایانه مجهز است، از داده‌ها حفاظت می‌کند تا در موارد دستور قضایی، بررسی شده و در صورت کشف جرم و درخواست ادله، مراتب به مقام قضایی ارائه شود. شنود داده‌ها به دلیل اینکه مستلزم داشتن تجهیزات فنی بوده، توسط پلیس انجام می‌شود. پلیس در نگهداری داده‌ها نقشی ندارد و نگهداری داده‌ها به عهده ارائه‌دهندگان خدمات دسترسی و میزبانی بوده تا در مواقع نیاز و دستور ارائه داده‌ها توسط مقام قضایی، داده‌ها را تحویل گرفته و به بررسی آن‌ها بپردازد. بنابراین، براساس قوانین دو کشور و کنوانسیون قسمت اعظم جمع‌آوری ادله توسط پلیس انجام می‌شود.

در فرانسه، طبق حکم ۲۶ اکتبر ۲۰۰۷، شرکت‌های دولتی و خصوصی ملزم شده‌اند تا اطلاعات مشتریان خود را در دسترس پلیس قرار دهند (فرال شوول<sup>۱</sup>، ۲۰۱۰، ص ۹۶). در قانون آیین دادرسی کیفری فرانسه در مرحله تحقیقات ابتدایی، افسران پلیس قضایی می‌توانند اقدام به توقیف اسناد، مدارک یا داده‌های رایانه کنند و افسر پلیس قضایی اشیاء اسناد، مدارک و اطلاعات رایانه‌ای که در کشف حقیقت مؤثر باشد را نگهداری می‌کند (کیسی، ۱۳۸۷، ص ۸۵). کنوانسیون جرائم سایبری در بند ۱، ۲ و ۳ ماده ۱۹، به تفتیش و توقیف داده‌های رایانه‌ای ذخیره‌شده اشاره و مقرراتی را پیشنهاد داده است. در خصوص شنود، قانون‌گذار فرانسه در سال ۱۹۹۱ در خصوص مسئله کنترل و شنود مکالماتی افراد، قوانین و شرایط ویژه‌ای وضع کرد (تدین، ۱۳۹۴، ص ۸۶). همچنین، کنوانسیون جرائم سایبری در ماده ۲۱ شنود داده محتوا را در جهت جمع‌آوری ادله تجویز و به اعضاء اجازه شنود و وضع قوانین در این خصوص داده است.

ماهیت خاص دلایل الکترونیکی به گونه‌ای است که پذیرش آن‌ها را در مراجع قضایی با چالش‌های جدی مواجه کرده است. در دلایل الکترونیک، کلیه مراحل از لحظه جمع‌آوری تا ارائه آن به مقام قضایی توسط پلیس سایبری تجزیه و تحلیل و ارزیابی می‌شود. با توجه به قوانین دو کشور و کنوانسیون، به‌طور کلی می‌توان گفت که در جرائم مشهود، پلیس بدو می‌تواند به جمع‌آوری ادله و حتی توقیف آن‌ها تا ۲۴ ساعت اقدام کند. براساس قوانین، جمع‌آوری دلایل الکترونیکی در جرائم غیرمشهود، مرکب از چهار مرحله است که در نمودار ۲، این چهار مرحله مشخص شده است.

1. Feral Schuhl



### نمودار ۲ - مراحل جمع‌آوری ادله الکترونیک توسط پلیس سایبری

- موارد افتراق قوانین ایران و فرانسه: بررسی‌های انجام شده نشان داد، روش جمع‌آوری ادله الکترونیک در ایران، فرانسه و کنوانسیون جرائم سایبری یکسان بوده و شباهت‌های زیاد بین مقررات قانونی ایران با فرانسه و همچنین کنوانسیون وجود دارد و سه روش به‌طور مستقیم توسط پلیس انجام می‌شود. قانون‌گذار ایران نیز در تصویب مقررات، مفاد کنوانسیون را در نظر گرفته است. با وجود شباهت‌های فراوان، تفاوت‌های بسیاری در حوزه جمع‌آوری ادله در مقررات بین دو کشور و حتی کنوانسیون وجود دارد. این تفاوت‌ها در جدول ۱ مشخص شده است.

### جدول ۱ - موارد افتراق قوانین ایران و فرانسه در جمع‌آوری ادله

فرانسه	ایران
- تشکیل پلیس سایبری؛ - تشکیل دفتر مرکزی مبارزه با جرائم فناوری اطلاعات با هدف مبارزه و جمع‌آوری ادله و رمزگشایی؛ - قوانین فرانسه مالک یا نماینده قانونی را بکار برده است؛ - مدت توقیف ۴ ماه است که قابل تمدید است؛ - تفتیش آنلاین (برخط) توسط پلیس سایبری مجاز شناخته شده است؛ - تفتیش از ساعت ۶ الی ۲۱ مجاز است، مگر در موارد تروریسم؛ - نصب دستگاه و ضبط اطلاعات بدون اجازه مالک در مواردی که منافع عمومی و امنیت جامعه در میان باشد پذیرفته شده، مگر در خصوص وکلا، مطبوعات، پزشکان، نمایندگان مجلس و سناتورها که با شرایطی مجاز است؛ - در موارد نیاز، دادستان می‌تواند از افراد متخصص عادی جهت رمزگشایی اطلاعات استفاده کند؛ - جزئیات و ضوابط جمع‌آوری ادله در قانون آیین دادرسی کیفری نیامده و با الحاق و تصویب کنوانسیون، قانون خاصی در این حوزه به تصویب نرسیده است؛ - در قانون و کنوانسیون، ارائه‌کنندگان خدمات دسترسی و میزبانی از هم تفکیک نشده است؛ - دستور حفاظت، مستلزم دستور قضایی است؛ - موارد ممنوعیت توقیف داده‌ها و سامانه‌های ارتباطی و مخبراتی در قانون و کنوانسیون مشخص نشده است؛ - جمع‌آوری زنده داده‌ها در کنوانسیون پذیرفته شده است؛ - شش مورد جرائم جنایی مطلقاً و جرائم جنبه مشروط بر اینکه مجازات قانونی دو سال یا بیشتر باشد، تجویز شده است؛	- فقدان تأکید قوانین بر تشکیل پلیس سایبری؛ - عدم تشکیل دفتر مبارزه با جرائم فناوری اطلاعات در قوه قضاییه و سازمان‌های امنیتی؛ - قوانین ایران واژه «ذی نفع» و «متصرف» را بکار برده است؛ - مدت توقیف مشخص نشده است؛ - اشاره‌ای به تفتیش آنلاین (برخط) نشده ولی می‌تواند از مصادیق جرائم مشهود باشد؛ - ساعت مجاز تفتیش مشخص نشده است؛ - نصب دستگاه در قوانین نیامده و صرفاً شش مورد مجاز است؛ - مقام قضایی مجاز است از کارشناسان رسمی دادگستری یا متخصصان پلیس فتا جهت رمزگشایی استفاده کند؛ - جزئیات و ضوابط جمع‌آوری ادله در آیین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیکی آمده است؛ - در قانون، ارائه‌کنندگان خدمات دسترسی و میزبانی از هم تفکیک شده است؛ - دستور حفاظت از داده‌ها مستلزم دستور قضایی است، مگر در موارد فوری (خطر آسیب دیدن یا تغییر یا از بین رفتن) که ضابطان می‌توانند رأساً دستور حفاظت را صادر کنند؛ - موارد ممنوعیت توقیف داده‌ها و سامانه‌ها در قانون مشخص شده است؛ - جمع‌آوری زنده داده‌ها در قانون پذیرفته نشده، البته می‌تواند از مصادیق جرم مشهود تلقی و جمع‌آوری ادله توسط پلیس انجام شود؛ - شش مورد امنیت داخلی و خارجی و جرائم بند الف، ب، پ و ت ماده ۳۰۲ با شرایطی تجویز شده است؛

موارد تشابه قوانین ایران و فرانسه: همان‌طوری که عنوان شد، بین مقررات قوانین کشور ایران، فرانسه و کنوانسیون جرائم سایبری در خصوص جمع‌آوری ادله و اقدامات پلیس، شباهت‌های فراوانی وجود دارد و نویسندگان قانون جرائم رایانه‌ای و آیین‌نامه از کنوانسیون جرائم سایبری الهام گرفته‌اند. موارد تشابه مقررات قوانین ایران، فرانسه و کنوانسیون در جمع‌آوری ادله و اقدامات پلیس عبارت‌اند از:

- نقش کلیدی پلیس در فرآیند جمع‌آوری ادله؛
- مراحل و روش جمع‌آوری ادله در قوانین هردو کشور و کنوانسیون یکسان است؛
- کلیه اقدامات توقیف و تفتیش توسط پلیس سایبری انجام می‌شود؛
- شهود جهت جمع‌آوری ادله الکترونیک در هردو کشور و کنوانسیون پذیرفته شده است؛
- در قوانین و کنوانسیون، به بازرسی و توقیف فرامرزی توجه نشده است؛
- به همکاری‌های بین‌المللی و دوجانبه در جمع‌آوری ادله توسط پلیس توجه نشده است؛
- مراحل برخورد با ادله الکترونیک در یک صحنه جرم تا حدودی در قوانین یکسان است؛
- تأکید قوانین و کنوانسیون در به‌کارگیری متخصصان رایانه به‌عنوان پلیس و قضات؛
- تفتیش، توقیف و حفاظت از ادله باید با صدور دستور قضایی انجام شود؛
- در قوانین و کنوانسیون، مدت زمان حفاظت داده‌ها حداکثر ۳ ماه تعیین شده است.

## بحث و نتیجه‌گیری

همان‌طوری که بیان شد، بزهکاری در فضای مجازی در حال گسترش است و جامعه هر روز با نوع جدیدی از اینگونه جرائم مواجه است. با قطع و یقین می‌توان گفت که بیشتر جرائم مربوط به آینده در فضای مجازی اتفاق خواهد افتاد. جرائم رایانه‌ای به دلیل اینکه از خصوصیات و ویژگی‌های خاصی برخوردار هستند، پلیس به‌عنوان نهاد برقرارکننده نظم و امنیت اجتماعی و مسئول پیشگیری از وقوع جرم، نقش مؤثری در انجام تحقیقات مقدماتی اینگونه جرائم ایفا می‌کند. پلیس‌های آینده مجبور هستند قانون را به وسیله مغزشان به اجرا بگذارند. فرآیند تحقیق، کشف و جمع‌آوری ادله در فضای مجازی بر عهده پلیس بوده و انجام این مراحل نیازمند دانش، ابزار و نیروهای متخصص در زمینه فناوری اطلاعات است. هدف اساسی از جمع‌آوری ادله در فضای مجازی، تحصیل ادله است که بتوان براساس آن، بزه را به مرتکب منتسب کرد. برای اینکه ادله در دادگاه

پذیرفته شود، باید براساس مقررات قانونی توقیف، کشف و جمع‌آوری شده باشد. کوچک‌ترین سهل‌انگاری در این مراحل باعث می‌شود ادله توسط دادگاه رد شده یا از بین رفته و در یک‌صدم ثانیه محو و حذف شوند. به همین جهت، در فضای مجازی همه نگاه‌ها و امیدها به سمت پلیس است. اگر ادله موجود در فضای مجازی براساس اصول، ضوابط و مقررات قانونی، جمع‌آوری و مستندسازی شود، برخلاف ادله سنتی، غیرقابل انکار خواهد بود. در حقوق ایران، تعقیب جرم جز در موارد جرائم مشهود باید با اجازه مقام قضایی باشد، بنابراین اگر ضابطان قضایی بدون اجازه مقام قضایی دست به تعقیب بزنند، نه تنها دلایل جمع‌آوری شده فاقد اعتبار است، بلکه تخلف از آن مستوجب تعقیب کیفری است.

براساس بررسی انجام شده، در هر دو کشور ایران و فرانسه، پلیس نقش اساسی در جمع‌آوری ادله ایفا می‌کند. به همین دلیل است که قانون‌گذار در قانون جرائم رایانه‌ای ۵ بار و در آیین‌نامه ۸ بار واژه ضابطان را بکار برده و این امر نشانگر اهمیت نقش پلیس در جمع‌آوری ادله الکترونیک است. پلیس در جمع‌آوری ادله باید اصول و ضوابط فنی و حقوقی را رعایت کند، در صورت عدم رعایت این ضوابط و اصول نه تنها به دلیل سرعت بالای تغییر و تحریف داده‌ها، نمی‌توان ادله‌ای را جمع‌آوری کرد، بلکه ادله جمع‌آوری شده نیز در دادگاه رد می‌شود. جرائم سنتی به محیط فیزیکی و صحنه جرم متمرکز بوده، ولی در جرائم رایانه‌ای، پراکندگی جغرافیایی صحنه جرم وسیع بوده و حتی ممکن است صحنه جرم و ادله در دورترین نقطه کره زمین قرار گرفته باشد. ادله موجود در فضای مجازی با سرعت قابل ملاحظه‌ای تغییر و محو می‌شود. بنابراین، سرعت عمل و دقت در بررسی صحنه جرم و جمع‌آوری ادله بسیار ضروری است و داشتن دانش بالای فنی و مهندسی موجب افزایش سرعت در رصد و پایش سایت‌های اینترنتی و شبکه‌های اجتماعی و سرعت تشخیص جرم و در نهایت افزایش دقت در جمع‌آوری ادله می‌شود. راهکارها و مقررات ارائه شده در قانون جرائم رایانه‌ای و آیین‌نامه ایران، راهگشای مجریان بوده و جوابگوی نیازهای حقوقی و فنی حوزه جمع‌آوری ادله است.

نتایج تحقیق نشان داد هرچند کشور ما به کنوانسیون ملحق نشده، ولی می‌توان گفت که در تنظیم آیین دادرسی جرائم رایانه‌ای و همچنین آیین‌نامه، از مفاد کنوانسیون به‌عنوان الگو بهره گرفته شده است و بسیاری از مقررات کنوانسیون در قانون ایران آمده است و شباهت فراوانی بین قانون ما و کنوانسیون وجود دارد. در ایران و فرانسه، پلیس

نقش اساسی و محوری در جمع‌آوری ادله دارد و وظایف پلیس به طور کامل در قوانین دو کشور و حتی کنوانسیون تشریح شده است. هر چند قوانین موضوعه ایران به پلیس سایبری اشاره‌ای نکرده، ولی نیروی انتظامی با احساس نیاز در این حوزه، پلیس فتا را به عنوان ضابط قانونی تأسیس کرده است. قانون جرائم رایانه‌ای و مخصوصاً آیین‌نامه هر چند از کنوانسیون اقتباس شده، ولی با این حال در مواردی از جمله مبحث تفتیش و توقیف و حفاظت از ادله، نسبت به کنوانسیون، کامل و جزئیات بیشتری را تشریح کرده است، ولی از جهت اینکه دادسرا و دادگاه تخصصی تشکیل نشده و صرفاً تعدادی از شعبات به جرائم رایانه‌ای اختصاص یافته، دارای ایراداتی است. ضمن اینکه در قوه قضاییه و سازمان‌های امنیتی، نهادی وجود ندارد که بتواند با جرائم رایانه‌ای در حجم گسترده و بین‌المللی و تروریستی مبارزه کند. راهکار نیابت قضایی قوانین فرانسه در جمع‌آوری ادله در خارج از مرزهای کشور نارآمد است؛ چراکه در جمع‌آوری ادله، سرعت عمل نقش اساسی دارد و مجرم می‌تواند در زمان مناسب، داده‌ها را حذف یا تغییر دهد، بنابراین نیابت قضایی نمی‌تواند راهکار مناسبی باشد. همچنین، راهکار استرداد مجرم تنها در صورتی امکان‌پذیر است که عمل در هر دو کشور جرم و قابل مجازات باشد و اینکه ادله در محل وقوع جرم ضبط یا حفظ شده باشد. بهترین راه حل برای رفع این چالش، همکاری دوجانبه و توافقنامه بین‌المللی است.

نتایج حاصل از تحقیق حاضر با یافته‌های تحقیق شایق و ناجی زواره (۱۳۹۵) در تأکید بر نقش پلیس در تحصیل دلیل و چگونگی کشف ادله دیجیتال و مستندسازی ادله و تفتیش و توقیف ادله، مشابهت و همخوانی دارد. حسنی سامره (۱۳۹۲) نیز در مطالعه خود، قوانین ایران در زمینه شکلی را دارای کاستی دانسته و تأسیس نهادهای غیررسمی برای جمع‌آوری ادله الکترونیک در کشور فرانسه را به عنوان الگوی مناسبی برای سایر کشورها معرفی کرده است که در تحقیق حاضر، با توجه به تصویب آیین‌نامه مربوطه، به رفع این کاستی تا حدودی اشاره شده است. به‌طور کلی، می‌توان مباحث نظری این تحقیق را در تدوین مقررات و قوانین در آینده و همچنین آموزش مقررات قانونی به مجریان قانون از جمله پلیس مورد استفاده قرار داد. با توجه به مطالب عنوان شده و نتایج پژوهش، پیشنهادهایی ارائه می‌شود:

- ضرورت همکاری بین‌المللی دوجانبه و چندجانبه کشورها و پلیس از طریق پلیس اینترپل در خصوص جمع‌آوری ادله؛

- لزوم توجه و تأکید بر مدیریت فناوری اطلاعات با توجه به نقش مؤثری که در جمع‌آوری ادله دارد؛
- لزوم به‌کارگیری ابزار و روش‌های نوین و همچنین نرم‌افزارهای مفید توسط پلیس در کشف جرم و جمع‌آوری ادله؛
- تأسیس مرکز فوریت و تیم واکنش سریع در سطح ملی در قوه قضاییه متشکل از قضات ویژه و متخصصان متبحر فنی و پلیس (آنچه در ماده ۳۵ کنوانسیون به اعضا پیشنهاد شده است)؛
- تأمین نیازمندی‌های نرم‌افزاری و سخت‌افزاری پلیس فتا در راستای تجهیز مراکز تخصصی و فنی و به‌کارگیری نیروهای متخصص و زبده؛
- حضور یک نفر مشاور متخصص امور رایانه‌ای با معرفی پلیس سایبری در شعبات تخصصی دادسرا و دادگاه ویژه رسیدگی به جرائم رایانه‌ای به منظور کمک فنی به قضات در جهت ارزیابی ادله و ارائه مشاوره.

## تشکر و قدردانی

از همه عزیزانی که در مراحل تدوین و تکمیل این پژوهش، به عنوان راهنما و مشاوره نقش داشته‌اند، قدردانی می‌شود؛ از راهنمای‌های ارزنده جناب دکتر ایرج گلدوزیان و جناب دکتر کیومرث کلانتری که با بزرگواری تمام در تهیه این پژوهش تلاش و کوشش کردند و همچنین از کلیه مسئولان، اعضای هیئت تحریریه، هیئت داوران، عوامل اجرایی و ویراستاری «فصلنامه پژوهش‌های اطلاعاتی و جنایی» که در پذیرش، داوری و چاپ این اثر، دلسوزانه همکاری داشتند، صمیمانه تشکر و قدردانی به عمل می‌آید.

## منابع

### منابع فارسی

- تدین، عباسی (اسفند ۱۳۹۳). پنهان‌کاری در تحصیل ادله در فرآیند دادرسی کیفری در ایران و فرانسه. نشریه پیام آموزشی. (۳۴)، صص ۵۹-۷۱. بازیابی از: <http://von.ir/uRZoZ>
- تدین، عباس (۱۳۹۴). آیین دادرسی کیفری فرانسه. تهران: انتشارات خرسندی. چاپ اول.



- جلالی فراهانی، امیرحسین (۱۳۹۴). *درآمدی بر آیین دادرسی کیفری جرائم سایبری*. تهران: انتشارات خرسندی. چاپ اول.
- جلالی فراهانی، امیرحسین (۱۳۹۵). *کنوانسیون جرائم سایبر و پروتکل الحاقی آن*. تهران: انتشارات خرسندی. چاپ اول.
- حسنی سامره، سیده الهام (۱۳۹۲). *مطالعه تطبیقی تفتیش و توقیف داده‌های رایانه‌ای و سامانه‌های مخابراتی در حقوق ایران و فرانسه*. پایان‌نامه کارشناسی ارشد دانشکده حقوق. دانشگاه شیراز.
- دلخون اصل، رامین (۱۳۹۲). *بررسی جرائم رایانه‌ای و اینترنتی*. تهران: انتشارات آرنا. چاپ اول.
- دلخون اصل، رامین (۱۳۹۳). *نحوه تعقیب و کشف جرائم رایانه‌ای*. تهران: انتشارات آرنا. چاپ اول.
- زندی، محمدرضا (۱۳۹۳). *تحقیقات مقدماتی در جرائم سایبری*. تهران: انتشارات جنگل. چاپ اول.
- شایق، علیرضا و ناجی زواره، مرتضی (۱۳۹۵). *مطالعه تطبیقی تحصیل دلیل کیفری در فضای سایبری در حقوق ایران، انگلستان، فرانسه با تأکید بر وظایف و اختیارات پلیس*. فصلنامه مطالعات حقوقی-انتظامی. ۱(۲)، صص ۱۱۶-۹۳. بازیابی از: <https://b2n.ir/18153>
- شمس، عبدالله (۱۳۹۶). *آیین دادرسی مدنی (جلد اول)*. تهران: انتشارات دراک. چاپ سی و سوم.
- فرهادی آلاستی، زهرا و جوان جعفری بجنوردی، عبدالرضا (بهار ۱۳۹۶). *چالش‌های رویاروی پیشگیری موقعیت مدار از جرائم سایبری فرامرزی*. فصلنامه پژوهش‌های اطلاعاتی و جنایی. ۱۲(۴۵)، صص ۳۲-۹. بازیابی از: [http://icra.jrl.police.ir/article\\_18198.html](http://icra.jrl.police.ir/article_18198.html)
- کریمی، محسن (۱۳۹۰). *جمع‌آوری و استنادپذیری ادله الکترونیکی در حقوق کیفری ایران*. پایان‌نامه کارشناسی ارشد رشته حقوق جزا و جرم‌شناسی دانشکده حقوق. دانشگاه علامه طباطبائی.

- کیسی، اوئن (۱۳۸۷). دلایل دیجیتالی و جرم رایانه‌ای؛ علم قانونی، رایانه‌ها و اینترنت (امیرحسین جلالی فراهانی و علی شایان، مترجمان)، تهران: انتشارات سلسبیل. چاپ اول.

- موسوی مجاب، سید درید (۱۳۹۲). شناسایی ادله الکترونیک و شیوه‌های کشف ادله پنهان، وبسایت مرکز امور وکلا و مشاوران قوه قضاییه استان قم. بازیابی از:

<https://b2n.ir/10505>

- مؤذن زادگان، حسنعلی؛ سلیمان دهکردی، الهام و یوشی، مهشید (۱۳۹۴). حفظ صحت و استنادپذیری ادله الکترونیکی با استفاده از بیومتریک و رمزنگاری. فصلنامه پژوهش حقوق کیفری. ۴(۱۲)، صص ۶۹-۹۷ بازیابی از: <https://b2n.ir/46515>

- مؤذن زادگان، حسنعلی و شایگان، محمد رسول (۱۳۸۸). استنادپذیری و تحصیل ادله الکترونیکی در حقوق کیفری ایران. فصلنامه دیدگاه‌های حقوقی. ۱۴(۴۸)، صص ۷۷-۱۰۲ بازیابی از: <https://b2n.ir/83220>

#### منابع انگلیسی

- Convention on Cybercrime (2001). Retrieved from: <https://b2n.ir/56166>
- Feral Schuhl, Christiane (2010). Cyberdroit Le droit à l'épreuve de l'Internet (Cyberright The right to the test of the Internet), Paris, Dalloz Publications, 6 edition.
- Quemener, Myriam (2009). Cybercriminalité défi mondial (Cybercrime global challenge), Paris, Economyica Publications, 2 edition. Retrieved from: [https://en.wikipedia.org/wiki/Convention\\_on\\_Cybercrime](https://en.wikipedia.org/wiki/Convention_on_Cybercrime)