Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

جرایم فضای مجازی و چالش های اثبات در دادگاه

مرتضی متقی — کارشناسی ارشد حقوق جزا و جرم شناسی دانشگاه آزاد اسلامی واحد تهران شمال

دکتر محمدرضا دهقانی سانیج — دکتری حقوق جزا و جرم شناسی دانشگاه آزاد اسلامی واحد تهران شمال

فصلنامه علمی فقه و حقوق نوین

Print ISSN: 2717- 1469
Online ISSN: 2717 – 1477

ISC.SID.NOORMAGZ.MAGIRAN
GOOGLESCHOLAR.ENSANI
www.jaml .ir

سال ۱۴۰۴، سال ششم، شماره ۲۳،
صفحات ۱۴-۱

چکیده

با گسترش روزافزون فناوری اطلاعات و ارتباطات، جرایم سایبری به یکی از چالش‌های بزرگ جوامع مدرن تبدیل شده‌اند. این مقاله به بررسی ابعاد مختلف جرایم سایبری و راهکارهای مقابله با آن‌ها می‌پردازد. در ابتدا، به تعریف مفاهیم پایه‌ای مانند هک، فیشینگ و کلاهبرداری اینترنتی پرداخته می‌شود. سپس، به مشکلاتی نظیر ردپای دیجیتال، پیچیدگی‌های حوزه قضائی بین‌المللی و نیاز به تخصص فنی در تحلیل داده‌های دیجیتال اشاره می‌شود. در ادامه، اهمیت بازنگری و به‌روزرسانی قوانین، تقویت همکاری‌های بین‌المللی، آموزش و توانمندسازی نیروهای قضائی و استفاده از فناوری در فرآیند دادرسی مورد بررسی قرار می‌گیرد. نتایج نشان می‌دهد که ترکیبی از این اقدامات می‌تواند به بهبود مبارزه با جرایم سایبری و ارتقاء امنیت فضای دیجیتال منجر شود.

واژگان کلیدی: جرایم سایبری، هک، فیشینگ، کلاهبرداری اینترنتی، ردپای دیجیتال، حقوق بین‌الملل، تخصص فنی، قوانین سایبری، همکاری بین‌المللی، آموزش قضائی، فناوری دادرسی.

طبقه‌بندی JEL: فقه – حقوق – جزا و جرم شناسی – حقوق بین الملل – حقوق خصوصی

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

Cybercrimes and the challenges of proof in court

Scientific Journal of Modern Jurisprudence and Law

Print ISSN: 2717- 1469
Online ISSN: 2717 - 1477

Profile in ISC,SID, Noormags, Magiran, Ensani, GoogleScholar
www.jaml .ir

Year 2025و Sixth year ,Issue 23

Pages 1-14

Morteza Mottaqi — Master of Criminal Law and Criminology, Islamic Azad University, North Tehran Branch

Dr. Mohammadreza Dehghani Sanij — PhD in Criminal Law and Criminology, Islamic Azad University, North Tehran Branch

Abstract

With the increasing development of information and communication technology, cybercrime has become one of the major challenges of modern societies. This article examines the different dimensions of cybercrime and the solutions to combat them. First, it defines basic concepts such as hacking, phishing, and cyber fraud. Then, it refers to problems such as digital footprints, the complexities of international jurisdiction, and the need for technical expertise in analyzing digital data. It then examines the importance of reviewing and updating laws, strengthening international cooperation, training and empowering the judiciary, and using technology in the judicial process. The results show that a combination of these measures can improve the fight against cybercrime and enhance the security of the digital space.

Keywords: Cybercrime, hacking, phishing, internet fraud, digital footprint, international law, technical expertise, cyber law, international cooperation, judicial education, litigation technology.

JEL Classification: Jurisprudence - Law - Criminal and Criminology - International Law - Private Law

مقدمه

۱ با توسعه فناوری اطلاعات و گسترش استفاده از فضای مجازی، جرایم سایبری به یکی از چالش‌های اساسی نظام‌های حقوقی و قضائی تبدیل شده‌اند. این جرایم، به‌دلیل ویژگی‌هایی نظیر ناشناس بودن مرتکبان، فرامرزی بودن و پیچیدگی‌های فنی، مشکلات متعددی را در فرآیند شناسایی، اثبات و پیگرد قانونی ایجاد کرده‌اند. بنابراین، بررسی چالش‌های حقوقی مرتبط با این جرایم و ارائه راهکارهای مؤثر برای مقابله با آن‌ها امری ضروری به نظر می‌رسد.

ضرورت تحقیق

در سطح بین‌المللی، با گسترش فناوری اطلاعات و ارتباطات، جرایم فضای مجازی به یکی از چالش‌های اساسی نظام‌های حقوقی تبدیل شده است. این جرایم، به‌دلیل ماهیت فرامرزی و ناشناس بودن مرتکبان، مسائل پیچیده‌ای را در زمینه اثبات و دادرسی ایجاد کرده‌اند.

یکی از مباحث کلیدی در این حوزه، صلاحیت قضائی است. با توجه به اینکه جرایم سایبری می‌توانند در یک کشور رخ داده و تأثیرات آن در کشوری دیگر نمایان شود، تعیین دادگاه صالح برای رسیدگی به این جرایم پیچیدگی‌هایی را به همراه دارد. برخی پژوهش‌ها به تحلیل چالش‌های حقوقی در مقابله با جرایم ارتکابی در فضای تاریک وب و مشکلات ناشی از ناشناس بودن مجرمان و مسائل مربوط به صلاحیت دادگاه‌ها پرداخته‌اند .(حیدری و میلانی، ۱۴۰۱)

ادله الکترونیکی نیز به عنوان یکی از چالش‌های مهم در دادرسی جرایم سایبری مطرح است. با توجه به ماهیت دیجیتال این ادله، مسائل مربوط به جمع‌آوری، نگهداری و ارائه آن‌ها در دادگاه‌ها پیچیدگی‌های خاص خود را دارد. تحقیقات تطبیقی نشان داده است که نظام‌های حقوقی مختلف، از جمله ایران و چین، در ارزیابی و پذیرش ادله الکترونیکی تفاوت‌هایی دارند که می‌تواند بر روند دادرسی تأثیرگذار باشد .(پورقهرمانی و قادری، ۲۰۲۲)

همچنین، همکاری بین‌المللی در مبارزه با جرایم سایبری از اهمیت ویژه‌ای برخوردار است. با توجه به فرامرزی بودن این جرایم، نیاز به همکاری و هماهنگی میان کشورهای مختلف برای مقابله مؤثر با آن‌ها احساس می‌شود. برخی مطالعات به تحلیل الزامات اثربخشی قوانین و احکام کیفری خارجی در قلمرو ملی و چالش‌های مرتبط با آن پرداخته‌اند .(فامیل مدبران و همکاران، ۲۰۲۴)

در مجموع، پیشرفت فناوری و گسترش فضای مجازی، نظام‌های حقوقی را با چالش‌های جدیدی مواجه کرده است. ضرورت بازنگری در قوانین، تقویت همکاری‌های بین‌المللی و توسعه روش‌های نوین جمع‌آوری و ارائه ادله الکترونیکی، از جمله اقداماتی هستند که می‌توانند به بهبود روند دادرسی جرایم سایبری کمک کنند.

اهداف تحقیق

- تحلیل چالش‌های حقوقی مرتبط با جرایم فضای مجازی و فرآیندهای اثبات آن‌ها در دادگاه‌ها.
- ارائه راهکارهای حقوقی برای بهبود فرآیند اثبات و پیگرد قانونی جرایم فضای مجازی.

سؤالات تحقیق

- چه چالش‌های حقوقی در فرآیند اثبات جرایم فضای مجازی در دادگاه‌ها وجود دارد؟
- چه راهکارهای حقوقی می‌توانند به بهبود فرآیند اثبات و پیگرد قانونی جرایم فضای مجازی کمک کنند؟

پیشینه تحقیق در زمینه جرایم فضای مجازی و چالش‌های اثبات در دادگاه‌ها

الف) پیشینه داخلی

با توجه به گسترش استفاده از فضای مجازی در ایران، توجه به جرایم مرتبط با این حوزه افزایش یافته است. پژوهش‌های متعددی به تحلیل و بررسی این جرایم و چالش‌های حقوقی مرتبط پرداخته‌اند. برای مثال، در مقاله‌ای تحت عنوان "مسئولیت کیفری در فضای سایبر در حقوق ایران" نوشته بهزاد رضویفرد و سید نعمتاله موسوی، به بررسی مسئولیت کیفری در محیط سایبر و چالش‌های حقوقی مرتبط پرداخته شده است .(رضوی فرد و موسوی، ۱۳۹۵)

همچنین، مقاله‌ای با عنوان "مطالعه کیفی عوامل ارتکاب جرائم در فضای مجازی (تحلیل محتوای کیفی پرونده‌های جرائم سایبری)" نوشته زهرا جاه بین، افسانه مظفری نوروز، هاشم زهی و سید محمد دادگران، به تحلیل علل ارتکاب جرایم سایبری و چالش‌های نظام کیفری در برخورد با این جرایم می‌پردازد .(جاه‌بین و همکاران، ۲۰۱۹)

این تحقیقات نشان‌دهنده اهمیت روزافزون توجه به جرایم سایبری و لزوم به‌روزرسانی قوانین و مقررات مرتبط در نظام حقوقی ایران است.

ب) پیشینه خارجی

در سطح بین‌المللی، توجه به جرایم فضای مجازی و مشکلات مرتبط با اثبات آن‌ها در دادگاه‌ها افزایش یافته است. یکی از منابع برجسته در این حوزه، کتاب "اصول جرایم سایبری " نوشته جاناتان کلاف (Clough, 2015) است که به تحلیل اصول حقوقی مرتبط با جرایم سایبری و چالش‌های اثبات آن‌ها در سیستم‌های حقوقی مختلف می‌پردازد.

همچنین، "جرایم سایبری: مسائل کلیدی و مباحث "نوشته آنتونی گیلسپی (Gillespie, 2016) به بررسی مسائل کلیدی و مباحث مرتبط با جرایم سایبری، از جمله چالش‌های حقوقی و فرآیندهای اثبات در دادگاه‌ها می‌پردازد.

کتاب "حقوق جرایم رایانه‌ای "نوشته اورین اس. کر (Kerr, 2005)نیز قوانین مرتبط با جرایم رایانه‌ای و مشکلات ناشی از اثبات این جرایم در دادگاه‌ها را مورد تحلیل قرار می‌دهد.

علاوه بر این، مقاله "حقوق حمله سایبری "نوشته مایکل ن. اشنیت (Schmitt, 2013) به بررسی حقوق بین‌الملل در زمینه حملات سایبری و چالش‌های اثبات آن‌ها در دادگاه‌های بین‌المللی می‌پردازد.

انواع جرایم فضای مجازی

۱. هک **(Hacking):** : به معنای دسترسی غیرمجاز به سیستم‌ها و شبکه‌های کامپیوتری است که با هدف سرقت اطلاعات حساس، ایجاد اختلال در عملکرد سیستم‌ها یا دستیابی به منابع محدود انجام می‌شود. این عمل می‌تواند توسط افراد یا گروه‌های مخرب صورت گیرد و عواقب جدی امنیتی به همراه داشته باشد . (بهدادی و همکاران، ۱۴۰۱)

انواع هک

هک را می‌توان بر اساس اهداف و روش‌های مورد استفاده به دسته‌های مختلف تقسیم کرد :(بهدادی و همکاران، ۱۴۰۱)

- هک کلاه سفید **:(White Hat Hacking)** این نوع هک توسط متخصصان امنیتی انجام می‌شود که با اجازه سازمان‌ها به شناسایی و رفع آسیب‌پذیری‌های سیستم‌ها می‌پردازند تا از نفوذهای غیرمجاز جلوگیری شود.
- هک کلاه سیاه **:(Black Hat Hacking)** هکرهای کلاه سیاه به صورت غیرمجاز و با اهداف مخرب مانند سرقت اطلاعات، ایجاد اختلال یا آسیب رساندن به سیستم‌ها اقدام می‌کنند.
- هک کلاه خاکستری **:(Gray Hat Hacking)** این نوع هک ترکیبی از هک کلاه سفید و سیاه است؛ هکرهای کلاه خاکستری بدون اجازه به سیستم‌ها نفوذ می‌کنند، اما اهداف مخربی ندارند و ممکن است آسیب‌پذیری‌ها را به اطلاع مالکان سیستم برسانند.

روش‌های متداول هک

هکرها از روش‌های متنوعی برای نفوذ به سیستم‌ها استفاده می‌کنند، از جمله:

- مهندسی اجتماعی **:(Social Engineering)** تکنیکی که در آن هکر با فریب و دستکاری افراد، اطلاعات حساس را از آن‌ها استخراج می‌کند.
- استفاده از بدافزارها **:(Malware)** نرم‌افزارهای مخربی که برای آسیب رساندن به سیستم‌ها یا سرقت اطلاعات طراحی شده‌اند، مانند ویروس‌ها، تروجان‌ها و کرم‌ها.
- حملات فیشینگ **:(Phishing)** ارسال پیام‌های تقلبی برای فریب کاربران و دریافت اطلاعات حساس مانند نام کاربری و رمز عبور.
- حملات **DDoS (Distributed Denial of Service):** اشباع کردن منابع سیستم یا شبکه با ترافیک زیاد به منظور ایجاد اختلال در عملکرد آن‌ها.

پیامدهای هک

- نفوذ به سیستم‌ها و سرقت اطلاعات می‌تواند عواقب جدی به همراه داشته باشد، از جمله:
- سرقت هویت **:**استفاده غیرمجاز از اطلاعات شخصی برای انجام فعالیت‌های غیرقانونی.
- خسارات مالی **:**هزینه‌های ناشی از بازیابی اطلاعات، تقویت امنیت و جبران خسارات وارده.
- آسیب به شهرت **:**از دست دادن اعتماد مشتریان و شرکای تجاری به دلیل نقض امنیت اطلاعات.
- اختلال در خدمات **:**موقوف شدن یا کند شدن عملکرد سیستم‌ها و شبکه‌ها به دلیل حملات.

راهکارهای مقابله با هک

- برای جلوگیری از هک و کاهش آسیب‌های ناشی از آن، اقدامات زیر توصیه می‌شود:
- تقویت امنیت رمز عبور **:**استفاده از رمزهای عبور قوی و تغییر منظم آن‌ها.

- به‌روزرسانی منظم نرم‌افزارها :نصب بروزرسانی‌ها و پچ‌های امنیتی برای رفع آسیب‌پذیری‌ها.
- آموزش کاربران :آگاه‌سازی کاربران درباره روش‌های حملات و نحوه مقابله با آن‌ها.
- استفاده از نرم‌افزارهای امنیتی :نصب و به‌روزرسانی آنتی‌ویروس‌ها و فایروال‌ها.
- پشتیبان‌گیری منظم :تهیه نسخه‌های پشتیبان از داده‌ها برای بازیابی در صورت حمله.

با اتخاذ این تدابیر، می‌توان تا حد زیادی از نفوذهای غیرمجاز جلوگیری کرده و امنیت سیستم‌ها و اطلاعات را حفظ نمود.

۲. فیشینگ **:(Phishing)** : یکی از رایج‌ترین روش‌های کلاهبرداری در فضای مجازی است که با هدف سرقت اطلاعات شخصی و مالی کاربران انجام می‌شود. در این روش، کلاهبرداری‌ها از طریق ارسال ایمیل‌ها یا پیام‌های جعلی صورت می‌گیرد که ظاهراً از منابع معتبر و شناخته‌شده به نظر می‌رسند. (قدرت و نیرومند حسینی، ۱۳۹۵)

انواع حملات فیشینگ

حملات فیشینگ می‌توانند به صورت‌های مختلفی صورت گیرند: (قدرت و نیرومند حسینی، ۱۳۹۵)

- ایمیل‌های فیشینگ عمومی :در این حملات، ایمیل‌هایی به تعداد زیاد ارسال می‌شوند که در آن‌ها از گیرندگان خواسته می‌شود اطلاعات شخصی یا مالی خود را به‌روز کنند یا جزئیات حساب کاربری خود را تأیید نمایند .
- فیشینگ نیزه‌ای **:(Spear Phishing)** در این نوع حملات، کلاهبرداری‌ها با هدف قرار دادن افراد یا سازمان‌های خاص صورت می‌گیرند. مهاجم با جمع‌آوری اطلاعات شخصی از قربانی، ایمیلی سفارشی‌شده ارسال می‌کند که ظاهراً از یک منبع معتبر است .
- فیشینگ از طریق پیامک **(Smishing)** و تماس تلفنی **:(Vishing)**در این روش‌ها، کلاهبرداری‌ها از طریق پیامک‌های متنی یا تماس‌های تلفنی انجام می‌شوند که در آن‌ها از قربانی خواسته می‌شود اطلاعات حساس خود را ارائه دهد .

روش‌های شناسایی ایمیل‌های فیشینگ

برای جلوگیری از افتادن در دام حملات فیشینگ، توجه به نشانه‌های زیر مفید است:

- بررسی آدرس فرستنده :آدرس ایمیل فرستنده را با دقت بررسی کنید تا از معتبر بودن آن اطمینان حاصل نمایید.
- محتوای ایمیل :ایمیل‌های فیشینگ معمولاً دارای غلط‌های املایی و نگارشی هستند و لحن غیررسمی دارند.
- درخواست اطلاعات حساس :سازمان‌های معتبر هیچ‌گاه از طریق ایمیل اطلاعات حساس را درخواست نمی‌کنند.
- لینک‌های موجود در ایمیل :بر روی لینک‌های موجود در ایمیل کلیک نکنید و قبل از وارد کردن اطلاعات، آدرس وب‌سایت را بررسی کنید.

اقدامات پیشگیرانه

برای کاهش خطر ابتلا به حملات فیشینگ، می‌توانید اقدامات زیر را انجام دهید:

- استفاده از نرم‌افزارهای امنیتی :نصب و به‌روزرسانی منظم آنتی‌ویروس‌ها و فایروال‌ها.
- آموزش و آگاهی‌بخشی :افزایش آگاهی کاربران درباره روش‌های شناسایی حملات فیشینگ و رفتارهای امن در فضای مجازی.
- احراز هویت دو مرحله‌ای :استفاده از روش‌های احراز هویت اضافی برای افزایش امنیت حساب‌های کاربری.
- پشتیبان‌گیری منظم :تهیه نسخه‌های پشتیبان از اطلاعات مهم برای جلوگیری از از دست دادن داده‌ها در صورت حملات موفق.

با رعایت این نکات، می‌توانید تا حد زیادی از حملات فیشینگ جلوگیری کرده و امنیت اطلاعات شخصی و مالی خود را حفظ نمایید.

۳. کلاهبرداری اینترنتی :کلاهبرداری اینترنتی به استفاده از فضای مجازی برای فریب کاربران و دریافت غیرقانونی وجه یا اطلاعات شخصی اطلاق می‌شود. با گسترش فناوری اطلاعات و ارتباطات، کلاهبرداری‌های اینترنتی نیز افزایش یافته و به یکی از جرایم رایانه‌ای تبدیل شده است که در قوانین مختلف جرم‌انگاری شده است. (زاهره، ۱۴۰۳)

انواع کلاهبرداری اینترنتی

کلاهبرداری‌های اینترنتی به روش‌های گوناگونی انجام می‌شوند، از جمله:

- کلاهبرداری از طریق درگاه‌های جعلی :طراحی و ایجاد وب‌سایت‌ها و درگاه‌های پرداخت تقلبی با ظاهری مشابه سایت‌های معتبر، به‌منظور سرقت اطلاعات کارت بانکی و وجوه کاربران.
- کلاهبرداری از طریق تبلیغات جعلی :نمایش تبلیغات یا بنرهای تقلبی که کاربران را به صفحات فریبنده هدایت کرده و اطلاعات شخصی یا مالی آن‌ها را جمع‌آوری می‌کنند.

مجازات کلاهبرداری اینترنتی

در قوانین جمهوری اسلامی ایران، کلاهبرداری اینترنتی تحت عنوان "جرایم رایانه‌ای" شناخته می‌شود. بر اساس ماده ۷۴۱ قانون مجازات اسلامی، مجازات کلاهبرداری اینترنتی می‌تواند شامل حبس، جزای نقدی و یا هر دو باشد. میزان مجازات بسته به شدت جرم، مبلغ کلاهبرداری و شرایط خاص پرونده متغیر است. (زاهره، ۱۴۰۳)

اقدامات پیشگیرانه

برای جلوگیری از کلاهبرداری‌های اینترنتی، کاربران می‌توانند اقدامات زیر را انجام دهند:

- آگاهی و آموزش :افزایش دانش درباره روش‌های کلاهبرداری و هشدارهای امنیتی.
- بررسی صحت منابع :تأیید اصالت ایمیل‌ها، پیام‌ها و وب‌سایت‌ها قبل از ارائه اطلاعات شخصی یا مالی.
- استفاده از نرم‌افزارهای امنیتی :نصب و به‌روزرسانی منظم آنتی‌ویروس‌ها و فایروال‌ها.

- حفظ محرمانگی اطلاعات :عدم به اشتراک‌گذاری اطلاعات حساس با منابع ناشناس یا غیرمعتبر.

با رعایت این توصیه‌ها، می‌توان تا حد زیادی از خطر کلاهبرداری‌های اینترنتی جلوگیری کرده و امنیت اطلاعات شخصی و مالی را حفظ نمود.

چالش‌های اثبات جرایم سایبری در دادگاه

اثبات جرایم سایبری به دلیل ماهیت پیچیده و ناشناس فضای مجازی با چالش‌های متعددی مواجه است:

۱. ردپای دیجیتال :ردپای دیجیتال به مجموعه‌ای از داده‌ها و نشانه‌هایی اطلاق می‌شود که در فضای مجازی از فعالیت‌های کاربران باقی می‌ماند و می‌تواند به شناسایی و ردیابی آن‌ها منجر شود. مجرمان سایبری با استفاده از تکنیک‌های مختلف، سعی در مخفی کردن این ردپاها دارند که این امر جمع‌آوری شواهد را برای مراجع قضائی دشوار می‌سازد. (والائی، ۱۳۹۸)

تکنیک‌های مخفی‌سازی ردپای دیجیتال

مجرمان سایبری از روش‌های گوناگونی برای پنهان کردن ردپای خود استفاده می‌کنند، از جمله:

- استفاده از شبکه‌های ناشناس :ابزارهایی مانند Tor به مجرمان امکان می‌دهند تا هویت و مکان خود را مخفی کنند، که شناسایی و ردیابی آن‌ها را برای مقامات قانونی دشوار می‌سازد .
- حذف یا تغییر داده‌ها :مجرمان ممکن است فایل‌ها و لاگ‌های مرتبط با فعالیت‌های خود را حذف کنند یا تغییر دهند تا از شناسایی جلوگیری کنند.
- استفاده از رمزنگاری :رمزگذاری ارتباطات و داده‌ها می‌تواند مانع از دسترسی مقامات به محتوای اطلاعات شود و جمع‌آوری شواهد را پیچیده‌تر کند.

چالش‌ها در جمع‌آوری شواهد دیجیتال

مخفی‌سازی ردپای دیجیتال می‌تواند مشکلات متعددی را در فرآیند جمع‌آوری شواهد ایجاد کند:

- پیچیدگی‌های فنی :نیاز به تخصص و دانش فنی برای کشف و تحلیل داده‌های مخفی‌شده وجود دارد که ممکن است برای مراجع قضائی چالش‌برانگیز باشد.
- حجم بالای داده‌ها :با توجه به حجم عظیم اطلاعات دیجیتال، شناسایی داده‌های مرتبط و مهم می‌تواند زمان‌بر و دشوار باشد.
- محدودیت‌های قانونی :در برخی موارد، قوانین و مقررات ممکن است اجازه دسترسی به داده‌های خاص را ندهند، که می‌تواند فرآیند جمع‌آوری شواهد را محدود کند.

۲. حوزه قضائی بین‌المللی: با توجه به جهانی بودن اینترنت، وقوع جرم در یک کشور و آسیب به شهروندان کشوری دیگر، مسائل حقوقی پیچیده‌ای را ایجاد می‌کند که نیازمند توجه ویژه در حوزه قضائی بین‌المللی است.

ماهیت فرامرزی جرایم سایبری

جرایم سایبری به دلیل ماهیت فرامرزی خود، چالش‌های متعددی را در نظام قضائی بین‌المللی ایجاد می‌کنند. این جرایم می‌توانند از مرزهای ملی عبور کرده و آسیب‌های جدی به شهروندان کشورهای مختلف وارد کنند، که این امر مسائل حقوقی پیچیده‌ای را به همراه دارد.

چالش‌های حقوقی در تعقیب و استرداد مجرمان سایبری

تعقیب و استرداد مجرمان سایبری با مشکلات متعددی مواجه است. این مشکلات شامل تفاوت‌های حقوقی بین کشورها، کمبود همکاری‌های بین‌المللی و مسائل فنی مرتبط با فناوری اطلاعات می‌شوند. بررسی تطبیقی قوانین و مقررات در این حوزه می‌تواند به درک بهتر و حل این چالش‌ها کمک کند. (زررخ و همکاران، ۱۳۹۹)

۳. تخصص فنی :تخصص فنی در تحلیل داده‌های دیجیتال و درک تکنیک‌های مورد استفاده مجرمان سایبری، برای مقابله مؤثر با جرایم فضای مجازی و جمع‌آوری شواهد دیجیتال ضروری است.

مهارت‌های فنی مورد نیاز برای تحلیل داده‌های دیجیتال

تحلیلگران امنیت سایبری باید با مفاهیم و ابزارهای متنوعی آشنا باشند تا بتوانند داده‌های دیجیتال را به‌طور مؤثر تحلیل کنند:

- آشنایی با فرمت‌های مختلف لاگ‌ها :درک فرمت‌های رایج لاگ‌ها مانند سیستم لاگ(Syslog) ، آپاچی (Apache)و لاگ‌های رویداد ویندوز (Windows Event Logs)به تحلیلگران کمک می‌کند تا داده‌های لاگ را به‌درستی تفسیر کنند .
- تسلط بر تکنیک‌های تحلیل لاگ :مهارت‌هایی مانند شناسایی ناهنجاری‌ها(Anomaly Detection) ، تحلیل همبستگی (Correlation Analysis) و شکار تهدید (Threat Hunting) به تحلیلگران امکان می‌دهد تهدیدات را شناسایی و واکنش مناسبی نشان دهند .
- استفاده از ابزارهای تجسمی :ابزارهایی که نمودارها، جداول و داشبوردهای تحلیلی ایجاد می‌کنند، به تحلیلگران کمک می‌کنند تا روندها و ناهنجاری‌ها را سریع‌تر شناسایی کنند .

اهمیت درک تکنیک‌های مورد استفاده مجرمان سایبری

مجرمان سایبری به‌طور مداوم در حال توسعه و استفاده از تکنیک‌های پیچیده برای پنهان کردن ردپای خود هستند. برای مثال، آن‌ها ممکن است از ابزارهای رمزنگاری برای مخفی کردن داده‌ها یا از روش‌های پیچیده برای پنهان کردن فعالیت‌های خود استفاده کنند. بنابراین، تحلیلگران امنیتی باید با این تکنیک‌ها آشنا باشند تا بتوانند آن‌ها را شناسایی و خنثی کنند.

راهکارهای حقوقی برای مقابله و اثبات جرایم سایبری

- بازنگری و به‌روزرسانی قوانین :با توجه به سرعت پیشرفت فناوری و ظهور تکنیک‌های نوین در جرایم سایبری، ضروری است که قوانین مرتبط با این حوزه به‌صورت منظم بازنگری و به‌روز شوند تا با تحولات جدید هم‌راستا باشند.

تأثیر پیشرفت فناوری بر تکامل جرایم سایبری

فناوری اطلاعات و ارتباطات با سرعتی بی‌سابقه در حال تحول است و این تحولات به‌طور مستقیم بر شکل و ماهیت جرایم سایبری تأثیر می‌گذارد. مجرمان سایبری با بهره‌گیری از فناوری‌های پیشرفته، روش‌های پیچیده‌تری را برای ارتکاب

جرم به‌کار می‌گیرند که شناسایی و مقابله با آن‌ها را دشوارتر می‌سازد. به‌عنوان مثال، استفاده از تکنیک‌های رمزنگاری، حملات توزیع‌شده و روش‌های پنهان‌سازی داده‌ها، چالش‌های جدیدی را برای مقامات قضائی و انتظامی ایجاد کرده است.

ضرورت بازنگری و به‌روزرسانی قوانین

با توجه به تحولات سریع فناوری و پیچیدگی‌های روزافزون جرایم سایبری، بازنگری و به‌روزرسانی قوانین مرتبط با این حوزه امری ضروری است. سردار وحید مجید، رئیس پلیس فتا فراجا، با اشاره به افزایش تنوع و پیچیدگی جرایم سایبری، بر لزوم به‌روزرسانی قوانین و مقررات موجود تأکید کرده و اظهار داشت که برای مقابله با این جرایم نوظهور، نیازمند قوانینی به‌روز و کارآمد هستیم .

چالش‌های موجود در نظام قضائی و لزوم هماهنگی بین‌المللی

یکی از مشکلات اساسی در رسیدگی به جرایم سایبری، عدم تناسب مجازات‌ها با شدت و پیچیدگی جرایم ارتکابی است. این عدم تناسب می‌تواند تأثیر بازدارندگی لازم را نداشته و مجرمان را به ادامه فعالیت‌های غیرقانونی تشویق کند. همچنین، با توجه به ماهیت فرامرزی اینترنت، وقوع جرم در یک کشور و آسیب به شهروندان کشوری دیگر، مسائل حقوقی پیچیده‌ای را ایجاد می‌کند که نیازمند هماهنگی و همکاری بین‌المللی است.(دفتر مقابله با مواد مخدر و جرم سازمان ملل متحد، ۱۳۹۲)

- تقویت همکاری‌های بین‌المللی :با توجه به جهانی بودن اینترنت و وقوع جرایم سایبری در مرزهای ملی مختلف، تقویت همکاری‌های بین‌المللی برای رسیدگی به این جرایم و تبادل اطلاعات میان کشورهای مختلف امری ضروری است.

چالش‌های ناشی از جرایم سایبری فراملی

جرایم سایبری فراملی، به‌دلیل ماهیت پیچیده و فرامرزی خود، چالش‌های متعددی را در پی دارند. مجرمان سایبری با استفاده از فناوری‌های پیشرفته، مرزهای ملی را درنوردیده و سیستم‌های اطلاعاتی کشورهای مختلف را هدف قرار می‌دهند. این امر نیازمند پاسخگویی هماهنگ و مشترک از سوی جامعه بین‌المللی است.

اهمیت همکاری‌های بین‌المللی در مبارزه با جرایم سایبری

همکاری‌های بین‌المللی در مبارزه با جرایم سایبری می‌تواند به‌صورت‌های زیر تأثیرگذار باشد:

- تبادل اطلاعات و داده‌ها :به‌اشتراک‌گذاری اطلاعات میان کشورهای مختلف می‌تواند به شناسایی و پیگیری مجرمان سایبری کمک کند.
- هماهنگی در تحقیقات و عملیات :همکاری در تحقیقات و عملیات مشترک می‌تواند به افزایش کارایی و اثربخشی مبارزه با جرایم سایبری منجر شود.
- توسعه ظرفیت‌ها و آموزش :برگزاری دوره‌های آموزشی و کارگاه‌های تخصصی می‌تواند به تقویت مهارت‌ها و دانش فنی نیروهای امنیتی و قضائی کمک کند.

اقدامات صورت‌گرفته در راستای تقویت همکاری‌های بین‌المللی

در سال‌های اخیر، اقدامات متعددی برای تقویت همکاری‌های بین‌المللی در مبارزه با جرایم سایبری انجام شده است. به‌عنوان مثال، دفتر مقابله با مواد مخدر و جرم سازمان ملل متحد (UNODC) کارگاه‌هایی را برگزار کرده است که در آن‌ها چالش‌های عملی و مشکلات اجرائی در زمینه همکاری‌های قضائی بین‌المللی مورد بحث و تبادل نظر قرار گرفته است . (ادیبان و افروغ، ۱۴۰۰)

با توجه به ماهیت فرامرزی جرایم سایبری و پیچیدگی‌های مرتبط با آن‌ها، تقویت همکاری‌های بین‌المللی و تبادل اطلاعات میان کشورهای مختلف امری اجتناب‌ناپذیر است. این همکاری‌ها می‌تواند به بهبود پاسخگویی جهانی به تهدیدات سایبری و تأمین امنیت فضای مجازی کمک کند.

- آموزش و توانمندسازی نیروهای قضائی :با توجه به پیچیدگی و سرعت تغییرات در حوزه فناوری اطلاعات و ارتباطات، آموزش و توانمندسازی نیروهای قضائی، به‌ویژه قضات و وکلا، در زمینه تکنیک‌های نوین جرم‌شناسی سایبری امری حیاتی است. برگزاری دوره‌های تخصصی می‌تواند به بهبود فرآیند دادرسی و ارتقاء کیفیت رسیدگی به جرایم سایبری کمک کند.

اهمیت آموزش تخصصی در جرم‌شناسی سایبری

جرایم سایبری با استفاده از فناوری‌های پیشرفته، پیچیدگی‌های خاص خود را دارند که نیازمند دانش تخصصی برای شناسایی، تحلیل و رسیدگی به آن‌ها است. بنابراین، قضات و وکلا باید با تکنیک‌ها و روش‌های نوین جرم‌شناسی سایبری آشنا باشند تا بتوانند به‌صورت مؤثر و کارآمد به این نوع جرایم رسیدگی کنند.

اقدامات انجام‌شده در راستای آموزش نیروهای قضائی

در سال‌های اخیر، نهادهای قضائی و آموزشی اقداماتی را در جهت آموزش نیروهای قضائی در حوزه فناوری‌های نوین انجام داده‌اند:

- برگزاری دوره‌های تخصصی :مؤسسات حقوقی و دانشگاه‌ها دوره‌های آموزشی متعددی را برای قضات و وکلا برگزار کرده‌اند. به‌عنوان مثال، مرکز آموزش علمی-کاربردی کانون وکلای دادگستری مرکز دوره‌های تخصصی در حوزه دعاوی سایبری ارائه داده است .
- توسعه آموزش‌های مجازی :با توجه به محدودیت‌های زمانی و مکانی، برخی مراکز آموزشی دوره‌های مجازی را برای تسهیل دسترسی به آموزش‌های تخصصی برگزار کرده‌اند. مرکز وکلا، کارشناسان رسمی و مشاوران خانواده قوه قضائیه نیز با ارائه دوره‌های آموزش مجازی، گامی در جهت توانمندسازی نیروهای قضائی برداشته است .
- برگزاری کارگاه‌ها و همایش‌ها :برگزاری کارگاه‌ها و همایش‌های تخصصی می‌تواند به تبادل تجربیات و به‌روز رسانی اطلاعات قضات و وکلا در زمینه تکنیک‌های نوین جرم‌شناسی سایبری کمک کند.

با توجه به رشد روزافزون جرایم سایبری و پیچیدگی‌های مرتبط با آن‌ها، آموزش و توانمندسازی نیروهای قضائی در زمینه تکنیک‌های نوین جرم‌شناسی سایبری ضروری است. برگزاری دوره‌های تخصصی، توسعه آموزش‌های مجازی و برگزاری کارگاه‌ها و همایش‌های مرتبط می‌تواند به بهبود

فرآیند دادرسی و ارتقاء کیفیت رسیدگی به جرایم سایبری منجر شود.

- استفاده از فناوری در فرآیند دادرسی :استفاده از فناوری‌های نوین، به‌ویژه هوش مصنوعی، در فرآیند دادرسی می‌تواند تحولاتی اساسی در سیستم قضائی ایجاد کند. به‌کارگیری ابزارهای دیجیتال برای جمع‌آوری و تحلیل شواهد، می‌تواند کارایی رسیدگی‌ها را به‌طور چشمگیری افزایش دهد.

نقش هوش مصنوعی در بهبود فرآیند دادرسی

هوش مصنوعی با توانایی پردازش حجم بالای داده‌ها و شناسایی الگوهای پیچیده، می‌تواند در بخش‌های مختلف سیستم قضائی به کار گرفته شود:(حاجیلو، ۱۴۰۳)

- تحلیل و پردازش داده‌ها :سیستم‌های هوش مصنوعی قادرند حجم عظیمی از داده‌های مربوط به پرونده‌ها را تحلیل کرده و الگوها و روابط پنهان را شناسایی کنند، که این امر به تسریع در فرآیند دادرسی کمک می‌کند.

- پیش‌بینی نتایج پرونده‌ها :با استفاده از الگوریتم‌های یادگیری ماشین، می‌توان نتایج احتمالی پرونده‌ها را پیش‌بینی کرده و به قضات در اتخاذ تصمیمات آگاهانه‌تر یاری رساند.

- اتوماسیون وظایف اداری :هوش مصنوعی می‌تواند وظایف روزمره و تکراری اداری را خودکار کرده و زمان و منابع انسانی را برای رسیدگی به مسائل پیچیده‌تر آزاد کند.

چالش‌ها و ملاحظات حقوقی

با وجود مزایای بالقوه، به‌کارگیری فناوری در دادرسی با چالش‌هایی نیز همراه است:

- حریم خصوصی و امنیت داده‌ها :جمع‌آوری و تحلیل داده‌های شخصی با استفاده از هوش مصنوعی ممکن است به نقض حریم خصوصی منجر شود، که نیازمند تدابیر امنیتی و حقوقی مناسب است.

- شفافیت الگوریتم‌ها :الگوریتم‌های هوش مصنوعی باید شفاف و قابل فهم باشند تا از تبعیض و ناعدالتی جلوگیری شود.

- پذیرش توسط جامعه :استفاده از فناوری در دادرسی ممکن است با مقاومت‌هایی از سوی قضات، وکلا و عموم مردم مواجه شود، که نیازمند آموزش و فرهنگ‌سازی است.

به‌کارگیری فناوری‌های نوین، به‌ویژه هوش مصنوعی، در فرآیند دادرسی پتانسیل بالایی برای افزایش کارایی و دقت سیستم قضائی دارد. با این حال، توجه به ملاحظات حقوقی و اخلاقی مرتبط با استفاده از این فناوری‌ها ضروری است تا از حقوق فردی و عدالت در فرآیند دادرسی محافظت شود.

نتیجه‌گیری

با توجه به گسترش روزافزون فناوری اطلاعات و ارتباطات، جرایم سایبری به یکی از چالش‌های بزرگ جوامع مدرن تبدیل شده‌اند. این جرایم نه‌تنها تهدیدی برای امنیت فردی و ملی محسوب می‌شوند، بلکه می‌توانند به اعتماد عمومی نسبت به فضای دیجیتال آسیب برسانند.

یکی از گام‌های اساسی در مقابله با جرایم سایبری، آموزش و توانمندسازی نیروهای قضائی است. برگزاری دوره‌های تخصصی در زمینه تکنیک‌های نوین جرم‌شناسی سایبری می‌تواند به بهبود فرآیند دادرسی و افزایش کارایی رسیدگی‌ها کمک کند. تحقیقات نشان داده است که آموزش‌های تخصصی می‌تواند به بهبود فرآیند دادرسی و کاهش زمان رسیدگی به پرونده‌ها منجر شود.

با توجه به سرعت پیشرفت فناوری، ضروری است قوانین مرتبط با جرایم سایبری به‌صورت منظم بازنگری و به‌روز شوند تا با تحولات جدید هم‌راستا باشند. عدم تطابق قوانین با فناوری‌های نوین می‌تواند منجر به خلأهای قانونی و کاهش اثربخشی سیستم قضائی در مقابله با جرایم سایبری شود.

از آنجا که جرایم سایبری مرزهای جغرافیایی را درنوردیده و به صورت فراملی رخ می‌دهند، تقویت همکاری‌های بین‌المللی امری ضروری است. تبادل اطلاعات، هماهنگی در تحقیقات و اقدامات مشترک می‌تواند به بهبود مبارزه با جرایم سایبری کمک کند. مطالعات نشان داده است که همکاری‌های بین‌المللی می‌تواند به کاهش نرخ جرایم سایبری و افزایش اثربخشی اقدامات پیشگیرانه منجر شود.

به‌کارگیری ابزارهای دیجیتال و فناوری‌های نوین در فرآیند دادرسی می‌تواند کارایی رسیدگی‌ها را افزایش دهد. استفاده از فناوری اطلاعات برای جمع‌آوری و تحلیل شواهد، مدیریت پرونده‌ها و ارتباطات بین مقامات قضائی می‌تواند به تسریع در فرآیند دادرسی و کاهش هزینه‌ها منجر شود.

مجموعه اقداماتی نظیر آموزش تخصصی نیروهای قضائی، بازنگری و به‌روزرسانی قوانین، تقویت همکاری‌های بین‌المللی و استفاده از فناوری در فرآیند دادرسی می‌تواند به بهبود مبارزه با جرایم سایبری و ارتقاء امنیت فضای دیجیتال منجر شود. توجه به این مسائل برای جوامع امروزی که به شدت به فناوری اطلاعات وابسته هستند، حیاتی است.

سپاسگزاری

از معاونت محترم پژوهشی به خاطر حمایت حمایت معنوی در اجرای پژوهش حاضر سپاسگزاری می‌شود.
از آقای دکتر عبدالله علیزاده به خاطر بازبینی متن مقاله و ارائه نظرهای ساختاری تشکر و قدردانی می‌شود.
از داوران محترم به خاطر ارائه نظرهای ساختاری و علمی سپاسگزاری می‌شود.
نگارندگان بر خود لازم می‌دانند از آقای دکتر محمد رسول آهنگران به خاطر مطالعه متن مقاله حاضر و ارائه نظرهای ارزشمند سپاسگزاری نمایند.

منابع

- بهدادی، ا., زندی، م & .,ناجی زواره، م. (۱۴۰۱). ماهیتِ تصمیم کارگروه تعیین مصادیق محتوای مجرمانه سایبری و پیامدهای آن .مطالعات حقوقی فضای مجازی.
- قریشی محمدی, فاطمه السادات . (۱۴۰۱). جرایم بانکی در فضای مجازی در حقوق ایران و اسناد بین‌المللی. فقه جزای تطبیقی, ۲(۳), ۴۵-۵۴ .
- جلالی, محمود و توسلی اردکانی, سعیده . (۱۳۹۸). ضرورت ایجاد نظام هماهنگ حقوقی بین‌المللی در مقابله با جرائم در فضای مجازی. فصلنامه مطالعات حقوق عمومی دانشگاه تهران, ۴۹(۴), ۱۳۵۱-۱۳۷۲ .
- رضوی فرد, بهزاد و موسوی, سید نعمت اله . (۱۳۹۵). مسئولیت کیفری در فضای سایبر در حقوق ایران. فصلنامه پژوهش حقوق کیفری, ۵(۱۶), ۲۹-۴۵ .
- قدرت، م.، و نیرومند حسینی، ف. س. (۱۳۹۵). بررسی روش‌های هوشمند شناسایی، پیشگیری و مقابله با حملات فیشینگ. سومین کنفرانس سراسری نوآوری‌های اخیر در مهندسی برق و کامپیوتر، تهران.

- جاه‌بین، ز.، مظفری، ا.، هاشم‌زهی، ن.، و دادگران، س. م. (۲۰۱۹). مطالعه کیفی عوامل ارتکاب جرائم در فضای مجازی (تحلیل محتوای کیفی پرونده‌های جرائم سایبری). تغییرات اجتماعی–فرهنگی، ۴(۱۵)، ۴۸–۷۱.
- دشتی, بیتا , & افشاری, مریم . (۱۳۹۸). مطالعه تطبیقی جرایم سایبری در ایران و حقوق بین الملل. پژوهشنامه حقوق تطبیقی, ۳(۱), ۸۳–۱۱۰ .
- حیدری, حسن و میلانی, دکتر علیرضا . (۱۴۰۱). بررسی تطبیقی جایگاه صلاحیت سرزمینی در رسیدگی به جرائم سایبری با تکیه بر نظام کیفری ایران. مجله علمی حقوق و مطالعات نوین, ۳(۴), ۱–۲۲.
- میرسلامی، سید کامیار، واحدیاریجان، یونس، و جمال زاده، عبدالرضا. (۱۴۰۱). بررسی فقهی و حقوقی جرم در فضای مجازی. مطالعات راهبردی ناجا، ۷(۲۳)، ۱۰۵–۱۳۱.
- پور قهرمانی، بابک، و قادری، رضا. (۲۰۲۲). مطالعه تطبیقی ارزیابی ادله الکترونیکی در نظام عدالت کیفری ایران و چین. مطالعات حقوقی فضای مجازی، ۱(۱)، ۵۹–۷۴.
- فامیل مدبران، اشکان، گیوکی، آذر، و علیزاده سرشت، نادر. (۲۰۲۴). الزامات اثربخشی به قوانین و احکام کیفری خارجی در قلمرو ملی: تحولات، موانع و راهکارها در حوزه جرایم سایبری. مطالعات حقوقی فضای مجازی، ۱(۳)، ۴۵–۵۸.
- زاهره، ع. ا. (۱۴۰۳). جرم کلاهبرداری اینترنتی چیست و چه مجازاتی دارد؟
- والائی، ح. (۱۳۹۸). ادله الکترونیکی (دیجیتال) به عنوان ادله اثبات جرم و دعوی. در دومین کنفرانس ملی پدافند سایبری، مراغه .
- زررخ، ا.، کاظمی، ق.، و جعفری، م. (۱۳۹۹). سیاست جنایی بین‌المللی در مقابله با جرایم سازمان‌یافته سایبری: رویکردها و راهبردها. ماهنامه جامعه‌شناسی سیاسی ایران، ۳(۴)، ۲۸۷۶–۲۸۹۴ .
- حاجیلو، ا. (۱۴۰۳). نقش هوش مصنوعی در فرآیند دادرسی: مقایسه استفاده از سیستم‌های حقوقی هوشمند در ایران و کشورهای پیشرفته. حقوق و علوم سیاسی، ۱(۲)، ۱۰۸–۱۱۴.
- ادیبان، ف.، و افروغ، ع. (۱۴۰۰). بررسی و تحلیل جرایم سازمان‌یافته فراملی از منظر اسناد و حقوق بین‌الملل.
- دفتر مقابله با مواد مخدر و جرم سازمان ملل متحد. (۱۳۹۲). توسعه همکاری‌های قضایی بین‌المللی با هدف مبارزه با جرائم سازمان‌یافته فرامرزی.
- **Clough, J. (2015).** Principles of Cybercrime. Cambridge University Press.
- **Gillespie, A. (2016).** Cybercrime: Key Issues and Debates. Routledge.
- **Kerr, O. S. (2005).** Computer Crime Law. Aspen Publishers.
- **Schmitt, M. N. (2013).** The Law of Cyber-Attack. California Law Review, 101(6), 1591-1662.