Legal Studies in Cyberspace

مطالعات حقوقی فضای مجازی

Received: 2023/10/10
Accepted: 2024/09/28
Publish: 2025/09/09
Pages: 1-16

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

Volume 4, Issue 14, Summer 2025
Article Type: **Research**
DOI: 10.71488/cyberlaw.2025.1217493

A Comparative Analysis of the Role of the United Nations and the European Union in Combating International Cybercrime

Mohammad Nasiri Nojadeh Sadat
Department of Public International Law, Mar.C., Islamic Azad University, Maragheh, Iran
Mehdi Niknafs
Department of International Law, Bu.C., Islamic Azad University, Bushehr, Iran
(Corresponding Author) nicknafs@iaut.ir
Babak Pourghahramani
Department of Criminal Law and Criminology, Mar.C., Islamic Azad University, Maragheh, Iran

Abstract
Cybercrimes are inherently harmful and multifaceted, and therefore affect virtually all governments. The development and evolution of cyberspace have given rise to diverse forms of cybercrime, prompting states over recent decades to pursue international treaties aimed at combating such offenses. There is no doubt as to the harmful nature of cybercrime and the necessity of harmonizing laws to facilitate international cooperation in addressing it. Structural changes brought about by the adoption of modern information and communication technologies have posed new challenges for human societies while simultaneously opening new horizons. International relations cannot remain indifferent to cybercrime, as inaction would only fuel the ambitions of cyber attackers and result in severe criminal consequences. One of the key international instruments in this field is the Council of Europe Convention on Cybercrime (the Budapest Convention), drafted in 2001 as the first treaty dedicated to cybercrime. According to the report of the UN Governmental Experts Group (since 2015), the United Nations and its member states have pursued the concept of "cyber empowerment" with multiple objectives, including establishing cyber deterrence to effectively counter malicious activities violating international law by state or non-state actors, creating an effective network to combat transnational organized crime, and promoting human rights standards aimed at enhancing transparency.

Keywords: Cybercrime, Computer Crime, The European Union, The United Nations

❋Citation (APA): Nasiri Nojadeh Sadat, M.; Niknafs, M.; Pourghahramani, B. (2025). A comparative study of the performance of the United Nations and the European Union against cybercrime international. *Cyberspace legal studies*, 4(14), 1-26.

مطالعات حقوقی فضای مجازی
Legal Studies in Cyberspace
ISSN: 2821-126X
ویگاه مجله: https://sanad.iau.ir/journal/cyberlaw
تاریخ دریافت: ۱۴۰۲/۰۷/۱۸
تاریخ پذیرش: ۱۴۰۳/۰۷/۰۷
تاریخ انتشار: ۱۴۰۴/۰۶/۱۸
صفحه: ۱ الی ۱۶
دوره ۴ / شماره ۱۴ / تابستان ۱۴۰۴
نوع مقاله: پژوهشی
DOI: 10.71488/cyberlaw.2025.1217493

مطالعه تطبیقی عملکرد سازمان ملل متحد و اتحادیه اروپا در قبال جرائم سایبری بین‌المللی

محمد نصیری نوجه ده سادات
گروه حقوق بین الملل عمومی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران
مهدی نیک نفس
گروه حقوق بین الملل، واحد بوشهر، دانشگاه آزاد اسلامی، بوشهر، ایران
(نویسنده مسئول) پست الکترونیک: mehdiinicknafs@gmail.com
بابک پور قهرمانی
گروه حقوق کیفری وجرم شناسی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران

چکیده
جرایم سایبری به طور بالقوه مضر و چند وجهی هستند. بنابراین، جرایم سایبری تقریباً همه دولت‌ها را تحت تأثیر قرار می‌دهد. توسعه و تکامل فضای سایبری منجر به پیدایش انواع جرایم سایبری شده است و از این رو در دهه‌های اخیر کشورها در راستای تدوین معاهدات بین المللی برای مبارزه با جرایم سایبری گام برداشته‌اند. در مورد لزوم مضر بودن و سازگاری با قوانینی که شامل همکاری بین‌المللی برای مبارزه با جرایم سایبری می‌شود، تردیدی وجود ندارد. تغییرات ساختاری ناشی از بکارگیری فناوری‌های نوین اطلاعاتی و ارتباطی، جوامع بشری را با چالش‌های جدیدی مواجه کرده و زمینه‌ها و افق‌های جدیدی را برای بشریت گشوده است. روابط بین‌الملل نمی‌تواند نسبت به جرایم فضای مجازی بی‌تفاوت باشد که محرکی برای طمع مهاجمان فضای مجازی و نتیجه رفتارهای مجرمانه جدی خواهد بود. یکی از این معاهدات بین‌المللی، معاهده جرایم سایبری شورای اروپا (کنوانسیون بوداپست) در سال ۲۰۰۱ به عنوان اولین معاهده در زمینه جرایم سایبری نوشته شد. بر اساس گزارش کارگروه کارشناسان دولتی از سال ۲۰۱۵، سازمان ملل متحد و تمامی دولت‌ها در طراحی مفهوم توانمندسازی سایبری به طور همزمان چندین هدف را در نظر گرفته‌اند که از جمله آنها می‌توان به موارد زیر اشاره کرد: ایجاد مانع سایبری برای مبارزه موثر با فعالیت‌های مخرب و ناقض حقوق بین‌المللی نهادهای دولتی یا غیردولتی، ایجاد شبکه‌ای موثر برای مبارزه با جرایم سازمان یافته بین المللی و ارتقای استانداردهای حقوق بشر با هدف ایجاد شفافیت.

واژگان کلیدی: جرائم سایبری، جرائم رایانه‌ای، اتحادیه اروپا، سازمان‌ملل

مقدمه

به موازات گسترش فعالیت‌ها و ارتباطات در فضای مجازی، برخی مجرمان نیز فعالیت‌های مجرمانه خود را به فضای مجازی منتقل می‌کنند یا از طریق چنین فضایی مرتکب جرم می‌شوند. تعریف جرایم در محیط‌های مجازی با تعاریف کلاسیک مطابقت ندارد و در بسیاری از موارد متفاوت است. فضای مجازی نیز مانند فضای واقعی محل ارتکاب جنایت را برای مجرمان فراهم کرده و از دیگر بازیگران حاضر در این فضا سوء استفاده می‌کنند. حفاظت از قربانیان سایبری مهم است زیرا انسان‌ها دارای کرامت و حقوق هستند و این حقوق صرف نظر از نژاد، قومیت، مذهب، ملیت و غیره رعایت می‌شود. و جلوگیری از نقض حقوق انسانی یا حقوقی افراد در هر فضایی اعم از حقیقی و مجازی جزء وظایف اساسی دولت‌ها است و در صورت تضییع این حقوق به هر دلیلی باید با سازوکارهای قضایی و اداری مناسب احیا شود. در این تحقیق از روش توصیفی- تحلیلی و کتابخانه‌ای ـ میدانی استفاده شده است و به این ترتیب که پس از طرح سوالات تحقیق با مراجعه به منابع حقوقی داخلی و خارجی و بررسی دیدگاه‌های حقوق دانان در منابع حقوق داخلی و بین‌المللی، با تجزیه و تحلیل اطلاعات گردآوری شده و سازمان دهی آنها به بررسی موضوع و اثبات فرضیات پرداخته‌ایم.

۱- مفهوم فضای مجازی

برخی حقوقدانان و کارشناسان معتقدند مفهوم سایبر در سطح بین‌المللی گسترش یافته و یک واژه بین‌المللی تبدیل شده است. آن‌ها بر این باورند که ترجمه این کلمه یا یافتن معادلی برای آن ممکن است دامنه و معنای آن را محدود کند، بنابراین توصیه می‌کنند که از آن به‌عنوان کلمه «مجازی» استفاده شود که در سطح بین‌المللی به همین معنی است و در تمام نقاط جهان با همین مفهوم استفاده می‌شود. و کلمه سایبر را باید با یک کلمه عام بین‌المللی نیز به کار برد با این تعریف در فارسی کلمه سایبر معادل کلمه مجازی و کلمه فضا معادل کلمه فضا می‌باشد. (باستانی، ۱۳۹۰: ۵۴).

۲- تهدید سایبری

تهدید[1] عبارت است از هر آنچه که امنیت را مورد خدشه قرار دهد. حال تهدید سایبری[2] عبارت است از هر اقدامی که بتواند امنیت شبکه و سیستم را به منظور هدفی خاص مورد خدشه قرار دهد. اهداف تهدید سایبری به سه سطح تقسیم میشوند: در سطح اول، معمولاً افراد مورد هدف قرار می گیرند و اقداماتی از قبیل سرقت هویت یا دسترسی غیرمجاز به اطلاعات شخصی به منظور باج خواستن از فرد قربانی را که بیشتر رنگ و بوی مالی دارند، شامل می‌شود. سطح دوم دولت‌ها هستند که هدف، آسیب رساندن به زیرساختهای حیاتی یا جاسوسی از آنها با انگیزه های سیاسی است. در سطح سوم شرکت های بزرگ غیردولتی قرار دارند که هدف از آن ترکیبی از سطح اول و سطح دوم است. تهدیداتی که در سطح فردی صورت می گیرند، در بیشتر مواقع در دسته جرائم سایبری[3] قرار می گیرند. اما تهدیداتی که در سطح دوم و سوم قرار می‌گیرند، جنبهٔ حمله سایبری[4] دارند. این تهدیدات در قالب حوادث[5] که صورت فنی دارند، از حالت بالقوه به حالت بالفعل در می‌آیند. در ادامه ابتدا حوادث معمول سایبری را معرفی کرده و سپس تهدیدات رایج همانند جرائم سایبری و حمله سایبری در سطح اتحادیه اروپا را مورد بررسی قرار می دهیم. (جلالی فراهانی، ۱۳۹۱، ۳۳)

[1] Threat
[2] Cyberthreat
[3] Cybercrime
[4] Cyberattack
[5] Incidents

۱-۲ حوادث سایبری

همان طورکه در بخش قبل گفته شد، تهدیدات در قالب حوادث از حالت بالقوه به حالت بالفعل در میآیند. آژانس امنیت سایبری اتحادیه اروپا پانزده حادثهٔ مربوط به حوزهٔ امنیت سایبری را در سال ۲۰۲۰ بررسی کرده است که عبارت اند از: بدافزار، حملات بر پایه وب، فیشینگ، حملات برنامه های وب، هرزنامه، حملات محروم سازی از سرویس توزیع شده، سرقت هویت، نقض داده، تهدید داخلی، بات نت ها، دستکاری فیزیکی، آسیب، سرقت، ضرر، نشت اطلاعات، باج افزار، جاسوسی سایبری و سرقت رمز ارز. (اکبری فومنی، ۱۳۸۷، ۱۰۵)

۳- جرائم سایبری

عموما جرائم سایبری به طیف گستردهای از فعالیت‌های جنایی مختلف اشاره دارد که در آن رایانه ها یا سیستم های اطلاعاتی به عنوان ابزار اصلی یا هدف اصلی درگیرند.[۱] مرکز جرائم سایبری اروپایی[۲] جرائم سایبری را به سه دسته جرائم وابسته به سایبر،[۳] بهره برداری جنسی از کودکان به صورت برخط[۴] و کلاهبرداری برخط تقسیم می کند. (آریا، ناصر، ۱۳۷۲، ۶۷)

۳-۱ حمله سایبری

حمله سایبری یک حمله فناوری اطلاعات[۵] به یک یا چند سیستم فناوری اطلاعات دیگر به منظور آسیب رساندن به آن در فضای سایبر است. طیف حملات سایبری از اقداماتی همچون هک کردن سایت های دولتی و بانک‌ها تا زیرساخت‌های حیاتی همچون نیروگاه‌های اتمی را شامل می‌شود. در سال ۲۰۰۷ مجموعه‌ای از حملات سایبری در استونی رخ داد. هکرها رشته ای از حملات انکار سرویس را آغاز کردند که با درخواست های پی درپی سرورهای آنها به طور موقت از کار افتادند و سیستم های اطلاعاتی بانک ها، خبرگزاری ها و سازمان های دولتی تحت فشار قرار گرفتند. درسال ۲۰۱۷، باج افزاری به عنوان برنامه بروزرسانی نرم افزار ام. ای. داک[۶] پخش شد. که اکثر مشاغل در اوکراین مجبور بودند از آن برای استفاده در پرونده های مالیاتی استفاده کنند، در این حمله نه تنها رایانه های مشاغل اوکراین آلوده شده بودند، بلکه تعداد قابل توجهی از رایانه های شرکت های دارای شعبه یا دفاتر در اوکراین نیز آلوده شدند. حدود ۲۰٪ از رایانه های آلوده اوکراینی‌ها نبودند؛ به عنوان مثال، حدود ۹٪ از کل رایانه های آلوده در آلمان بودند که پس از اوکراین با این حمله شدیدترین آسیب را دید. نوتپتی۷ دو هزار کاربر در سرتاسر جهان را تحت تأثیر قرار داد و تخمین زده می شود که نزدیک به ۲/۱ میلیارد دلار به شرکتها ضرر رسانده است. باج افزار واناکرای ۸در طی حملهٔ گسترده به چندین کشور در سال ۲۰۱۷ مشاهده شد. براساس چندین گزارش از متخصصان امنیت شبکه، در مجموع ۳۰۰۰۰۰ سیستم در بیش از ۱۵۰ کشور به شدت آسیب دیدند. این حمله دامنهٔ گسترده ای از بخش ها از جمله بهداشت، دولت، ارتباطات از راه دور و انرژی را شامل شد. در انگلستان ۸۰ سرویس بهداشت ملی۹ به طور موقت قطع شدند و وقت های ملاقات برخط پزشکی نیز به مدت یک هفته به تعویق افتادند. پرونده های پزشکی آلوده و از دسترس خارج شدند. اگرچه واناکرای به طور خاص سیستم های کنترل صنعتی را هدف قرار نداده بود، تعدادی از سیستم های کنترل صنعتی تحت تأثیر قرار گرفتند. شرکت های مختلف در صنایع مختلف کنترل فرایندهای صنعتی خود را از دست دادند که شرکت فرانسوی رنو نمونه‌ای از آن است. این سه مورد از مهمترین حملات سایبری بوده که در سالهای اخیر در سطح اتحادیه اروپا رخ دادهاند؛ درحالی که تعداد حملات سایبری در اروپا سال به سال در حال افزایش است؛ به عنوان مثال در سال ۲۰۲۰، ۷۵۶ مورد حمله سایبری اتفاق افتاده است؛ درحالی که این رقم در سال ۲۰۱۹، ۴۳۲ مورد بوده است. (درگاهی، ۱۳۸۶، ۵۵)

---

[1] Cyber-dependent crime
[2] European Cybercrime Centre
[3] Cyber-dependent crime
[4] Online child sexual exploitation
[5] IT
[6] M.E.Doc
[7] NotPety
[8] WannaCry
[9] National Health Service (NHS)

۴- کنوانسیون بین المللی جرایم رایانه‌ای (بوداپست)

کنوانسیون جرایم رایانه‌ای (بوداپست) یک سند بین المللی است که در یک کنفرانس بین المللی در ۲۳ سپتامبر ۲۰۰۱ با حضور ۲۴ کشور عضو شورای اروپا و چهار کشور آمریکا، ژاپن، کانادا و آفریقای جنوبی در شهر بوداپست مجارستان با موضوع جرایم رایانه‌ای به تصویب رسید است. در این کنوانسیون نیز جرم رایانه‌ای به طور مشخص و مستقل وجود ندارد، ولی مصادیق زیادی تحت عنوان جرم تبادل اطلاعات ذکر شده و از اعضای کنوانسیون خواسته شده است که به جرم انگاری آنها از طریق قوانین کیفری داخلی خود اقدام کنند. مقدمات این کنوانسیون به این شرح است که: (خالقی،۱۳۹۰: ۲۳) کمیته اروپایی مشکلات جنایی، در اجرای مصوبه شماره CDPC/۱۰۳/۲۱۲۲۹۶ نوامبر ۱۹۹۶ تصمیم گرفت کمیته ای متشکل از کارشناسان برای برخورد با جرایم رایانهای تشکیل دهد. که استدلال‌های ذیل را در برداشت: (Akbanov,2019, 114)

پیشرفت‌های سریع حوزه فناوری اطلاعات، ارتباط مستقیمی با تمامی بخش های جامعه مدرن دارد. انسجام سیستم های اطلاعات و ارتباطات راه دور که صرف نظر از فواصل جغرافیایی، ذخیره و انتقال تمامی انواع اطلاعات را مقدور ساخته، طیف وسیعی از احتمالات جدید را به وجود آورده است. جرایم رایانه‌ای ممکن است علیه ثبات، موجودیت و قابلیت اطمینان به سیستم‌های رایانه‌ای در شبکه های ارتباط راه دور رخ دهند یا این که از خدمات ارائه شده برای ارتکاب جرایم سنتی استفاده شود. ماهیت فرامرزی چنین جرایمی مثلا در صورتی که از طریق اینترنت ارتکاب یابند، با صلاحیت سرزمینی نیروهای پلیس در تضاد است. (خرم آبادی، ۱۳۹۱،۱۹)

به دنبال خاتمه مدت مهلت اعطایی به کمیته، متخصصان و کارشناسان تحت حمایت کمیته CDPC سه جلسه اضافه را برای تکمیل پیش نویس کنوانسیون و یادداشت توجیهی تشکیل دادند و پیش نویس کنوانسیون را با کمک و نظر انجمن پارلمانی بررسی کردند کمیته آرا در اکتبر ۲۰۰۰ از انجمن یادشده درخواست کرد که نظراتش را پیرامون پیش نویس کنوانسیون ارائه دهد که انجمن هم در دومین بخش جلسه عمومی خود در آوریل ۲۰۰۱ آن را تصویب کرد.(پاکزاد، ۱۳۸۵، ۹۲)

۵- سازمان ملل متحد و تعهد آن به امنیت سایبری

هدف سازمان ملل متحد در ماده ۱ و اصول مندرج در ماده ۲ منشور مکمل ایده هایی است که انگیزه کشورهای شرکت کننده در ایجاد سازمان ملل متحد را برانگیخت. اهداف و اصول ذکر شده در بالا را می توان به عنوان توصیه هایی برای سازمان ملل متحد در نظر گرفت. (اسلامی، ۱۳۷۲، ۶۱)

ماده ۱ منشور نحوه حل تعارضاتی را که ممکن است بین اهداف مختلف ایجاد شود را نشان می دهد. این تنها از طریق ایجاد توافقات عملی و در عین حال اولویت دادن به حفظ بلندمدت صلح و امنیت بین المللی از طریق اقدام جمعی امکان پذیر است. دیوان بین الملل دادگستری درنظریه مشورتی خود درباره برخی هزینه ها اظهار داشت که «اولویت صلح و امنیت بین المللی طبیعی است، زیرا تحقق اهداف دیگر منوط به دستیابی به این شرط اساسی است. (امامی، ۱۳۷۷، ۱۵)

مقدمه و مواد ۱ (۱)، (۲) و (۳) منشور نشان می دهد که صلح چیزی بیشتر از نبود جنگ است. این مواد به تحول در وضعیت روابط بین‌الملل اشاره دارد که می تواند منجر به کاهش مواردی شود که احتمالاً به بروز جنگ منجر می‌شوند .نمونه هایی از این تفسیر را می توان در برخی قطعنامه‌های سازمان ملل مشاهده نمود. درنتیجه، مجمع عمومی سازمان ملل مکرراً بر ارتباط نزدیک بین تقویت صلح و امنیت بین المللی از یکسو و خلع سلاح، استعمار و توسعه از سوی دیگر تأکید کرده است. این رویکرد مبنایی برای اعلام سال جهانی صلح بود. در این اعلامیه آمده است که ارتقای صلح و امنیت بین المللی مستلزم اقدام مستمر و مثبت همه دولت ها و مردم در رابطه با یکسری اهداف ازجمله : ممانعت از توسل به زور، رفع تهدیدهای مختلف صلح (از جمله تهدید هسته ای)، احترام به اصل عدم استفاده از زور، توسعه اقدامات اعتمادساز و... می باشد . مرجع گزارش در کشور با

عنوان «دنیایی امن تر- مسئولیت مشترک ما» به تهدیدات بزرگی که صلح و امنیت جهان را تهدید می کند و از جمله به تروریسم و جرایم سازمان یافته بین المللی اشاره دارد .(داودی گرمارودی، ۱۳۸۴، ۸۶)

با ظهور اینترنت، بخش مهمی از معضل امنیت بین المللی مورد توجه قرار گرفته است. فضای مجازی با سیستم فنی پیچیده خود چالش بزرگی را پیش روی دولت‌ها قرار داده است که شرکت های فناوری را به سمت بازیگری فعال سوق داده است. یکی از بزرگ ترین خطراتی که فضای مجازی برای همه کشورها اعم از کشورهای پیشرفته و توسعه نیافته ایجاد می کند، این است که ضعف فناوری یک کشور می تواند بستری برای تهدید جدی برای همه کشورها فراهم کند. دلیل این امر این است که سوء استفاده از زیرساخت های اینترنتی در کشورهایی که توانایی نظارت و جلوگیری جدی از انجام فعالیت‌های مخرب و حتی جنگ سایبری با سایر کشورها را ندارند، امری عادی شده است. (دزیانی، ۱۳۸۴، ۹۸)

۵-۱ اقدام سازمان ملل متحد در زمینه اینت سایبری

توجه بین المللی به امنیت سایبری طی سال های اخیر به طور چشمگیری افزایش یافته است زیرا فضای مجازی به زیر ساخت مرکزی جهان تبدیل شده است. این امر امکان توسعه و رشد را ایجاد اما در عین حال فرصت های گسترده ای را برای منازعات و ارتکاب جرایم فراهم نموده است. کشورها اهمیت فضای سایبر را درک کرده اند و همراه با آن، نیاز به همکاری جهانی برای ایجاد ثبات و امنیت بیشتر دارند. (Kriangsak,2017,206)

سازمان ملل متحد نقشی اساسی در این میان ایفا می کند، زیرا اغلب دولت ها مسئول اقدامات مخرب و بی ثبات کننده هستند. این را می توان با شمارش ساده حوادث مهم تعیین کرد. این امر به سازمان ملل نقش اساسی در رسیدگی به مسئله اعتماد و امنیت می بخشد و اهمیت چارچوب سازمان ملل برای رفتار مسئولانه دولت ها در فضای سایبر که در سال ۲۰۱۵ ایجادشده را برجسته می کند. (رحمدل، ۱۳۸۳، ۵۲)

هسته اصلی این چارچوب مورد توافق هنجارهای توصیف شده در گزارش ۲۰۱۵ گروه کارشناسان دولتی سازمان ملل متحد است. هنجارها تفاهم دولت ها بر سر رویه هایی است که رفتار مناسب را شناسایی و هدایت می کنند. هنجارها تعهدات بین المللی را که کشورها پذیرفته اند را تعریف می کنند. این چارچوب توسط گروه کارشناسی دولتی ایجادشده است که توسط کمیته اول سازمان ملل متحد تأسیس شده تا تحولات حوزه اطلاعات و مخابرات در زمینه امنیت بین المللی را بررسی کند. آخرین مورد از این مجموعه تلاش ها تصویب دو قطعنامه درسال ۲۰۱۸ است و یک کارگروه کارشناسی جدید و بدون محدودیت زمانی ایجاد شد. (حسن بیگی، ۱۳۸۴، ۲۲)

گروه کارشناسان دولتی در توسعه اطلاعات و ارتباطات از راه دور در بستر امنیت بین المللی[1] تحت نظر کمیته نخست شورای امنیت (کمیته خلع سلاح و امنیت بین المللی) تشکیل گردید.این گروه گزارش نخست خود را به تاریخ ۲۴ ژوئن ۲۰۱۳ منتشر نمود. گزارش بر این امر تاکید دارد که امنیت سایبری می بایست دوشادوش احترام به حقوق بشر و آزادی های بنیادین مندرج در اعلامیه جهانی حقوق بشر و سایر اسناد بین المللی توسعه یابد. گزارش مذکور اشعار می دارد که دولت ها می بایست بر میزان همکاری ها علیه جرایم سایبری و تروریستی در بستر فناوری اطلاعات بیفزایند. (دی انجلیز، ۱۳۸۳، ۴۱)

در طی سال‌های ۲۰۱۴-۲۰۱۵، گروهی از کارشناسان دولتی بر استفاده از فناوری اطلاعات در درگیری‌ها و نحوه اعمال قوانین بین‌المللی برای استفاده از این فناوری توسط دولت‌ها تمرکز کردند. گزارش دوم این گروه در جولای ۲۰۱۵ منتشر شد. این بحث ها در سازمان ملل درک مشترکی از نحوه رفتار دولت ها در فضای سایبری و نحوه همسویی آن با تعهدات بین المللی موجود یک کشور ایجاد کرد. این هنجارها چارچوبی برای رفتار مسئولانه دولت ایجاد می کند. در این گزارش آمده است که دولت ها باید در پیشگیری از اقدامات خرابکارانه همکاری کنند و آگاهانه اجازه ندهند که قلمرو خود برای جنایات بین المللی با استفاده

[1] GGE

از فناوری اطلاعات مورد استفاده قرار گیرد. به اشتراک گذاری اطلاعات و کمک در تعقیب تروریست ها و استفاده مجرمانه از فناوری اطلاعات بین دولت ها باید گسترش یابد، در حالی که احترام کامل به حقوق بشر، از جمله حق حریم خصوصی و آزادی بیان، باید تضمین شود. در حالی که دولت‌ها باید اقدامات مناسبی را برای محافظت از زیرساخت‌های حیاتی خود در برابر تهدیدات فناوری اطلاعات انجام دهند، اما نباید درگیر فناوری‌های شوند که عمداً باعث آسیب یا سایر اشکال آسیب در استفاده و کاربرد زیرساخت‌ها می‌شود. توسط سایر منابع حیاتی کشورها حمایت می شود.گروهی از کارشناسان دولتی توسل به اقدامات اعتمادساز را برای گسترش همکاری های بین المللی و کاهش خطر درگیری پیشنهاد کرده اند. بخش خصوصی، دانشگاه و جامعه می توانند نقش مهمی در حمایت از مسئولیت اصلی دولت ها برای حفظ امنیت فناوری اطلاعات ایفا کنند. نویسندگان گزارش بر این باورند که توانمندسازی، زیربنای همکاری های بین المللی است و منجر به افزایش ظرفیت دولت ها برای همکاری و اقدام مشترک می شود. (خسروی فارسانی، ۱۳۸۹، ۷۳)

۲-۵ تصویب قوانین مقررات در سازمان ملل متحد و اتحادیه اروپا

به این قطعنامه ۷۹ کشور رای مثبت، ۶۰ عضو این مجمع به آن رای منفی و ۳۳ کشور نیز به قطعنامه رای ممتنع دادند. مجمع عمومی سازمان ملل متحد با ایجاد یک کمیته تخصصی بین دولتی به نمایندگی از همه مناطق موافقت کرد تا یک کنوانسیون بین المللی جامع برای مبارزه با استفاده از فناوری اطلاعات و ارتباطات برای مقاصد غیرقانونی ایجاد کند. (امامی، ۱۳۷۷، ۲۳)
این کمیته در تهیه پیش نویس کنوانسیون مذکور، اقدامات ملی و بین المللی برای مبارزه با استفاده از فناوری اطلاعات و ارتباطات برای مقاصد غیرقانونی را بررسی می کند. لایحه پیشنهادی روسیه پس از تصویب در کمیته سوم مجمع عمومی سازمان ملل به این مجمع داده شد. (پوربافرانی، ۱۳۸۲، ۴۲)

آندری کرتسکیک، نماینده رئیس جمهور روسیه برای همکاری های بین المللی در زمینه امنیت اطلاعات، بیان نمود: هدف از ارائه این تصمیم مقابله با این شر بزرگ است که خسارات زیادی را به اقتصاد جهانی وارد می کند. (حبیب زاده، ۱۳۸۷، ۱۷)

کنوانسیون جرم سایبری شورای اروپا موسوم به کنوانسیون بوداپست، تنها ابزار بین المللی الزام آور در مورد این مساله است.(دبلفون، ۱۳۸۸، ۱۰۴)

این کنوانسیون به عنوان دستورالعملی برای کشورهایی که قانون ملی جامعی علیه جرایم سایبری تدوین می کنند، مورد استفاده قرار می گیرد. این کنوانسیون همچنین به عنوان چارچوبی برای همکاری بین المللی بین کشورهای امضاکننده این پیمان عمل می کند. (حسنوی، ۱۳۷۹، ۳۹)

سازمان های بین المللی و منطقه ای از جمله اتحادیه اروپا از طریق تنظیم قواعد و مقررات مرتبط در قالب تدابیر قانونی و حقوقی بعنوان یکی از مهمترین ارکان مورد توجه در روند قانون مند سازی در حوزه جرائیم سایبری نقش برجسته ای ایفا می نمایند. اتحادیه اروپا از کشورهای فعال در حکمرانی فضای مجازی در دنیا محسوب می شود. این اتحادیه در چارچوب دیپلماسی سایبری می کوشد به مهره ای کلیدی در سیاستگذاری خارجی و حکمرانی فضای سایبر با نگاهی ویژه به امنیت سایبری در دنیا تبدیل شود. (حاجیلی، ۱۳۸۸، ۴۸)

در واقع اتحادیه اروپا با لحاظ رویکردی جدی از سال ۲۰۰۹ و با تصویب اسنادی الزام آور و متعدد که بطور مداوم و با توجه به پیشرفت فناوری ارتباطات و اطلاعات درحال اصلاح و بروز رسانی هستند (برعکس رویکرد شورای اروپا با در نظر گرفتن کنوانسیون جرایم رایانه‌ای) به اقدامات جدی در حوزه جرایم رایانه‌ایی و اصول و قانونمند سازی این دنیای وسیع در بستر تدابیر حقوقی و قانونی پرداخته است. قوانین فعلی اتحادیه اروپا در رابطه با حملات سایبری بازتابی از قوانین وضع و ثبت شده موجود در گزارش سازمان ملل است که طی آن قوانین عمومی بین المللی را ملاک عملیات فرض می کند. به عبارت دیگر از منظر اتحادیه اروپا قوانین فعلی بین المللی معیار و ملاک رفتار هنجارمند در عرصه سایبری می باشد. با این حال این اتحادیه بر

بروز رسانی قوانین موجود حاکم یا قانون گذاری بروز به منظور مشخص کردن مباحث و ویژگی های خاص فضای سایبری تاکید دارد. اتحادیه اروپا بهبود الگوی حکمرانی چند وجهی را برای اینترنت دنبال می کند؛ الگویی که بر اساس تعامل و هماهنگی میان تمامی ذی نفعان بنا شده است که متشکل از: دولت های کشورهای عضو (نهادهای انتظامی و قضایی، نهادهای پاسخگوی حوادث سایبری، نهادهای اطلاعاتی)، شرکت های خصوصی فعال در زمینه فناوری اطلاعات و صنایع دفاعی، سازمان های بین المللی و میان دولتی، سازمان های مردم نهاد، اجتماعات مردمی، دانشگاه ها، متخصصان فنی و همچنین اتاق فکر و غیره می باشد .بر اساس قوانین جدید اتحادیه اروپا که در پارلمان این منطقه به تصویب رسیده است، از این پس هر گونه اقدام علیه امنیت سایبری جرایم سنگین‌تری را شامل می‌شود که از جمله این اقدامات می‌توان به حملات ساده مبتنی بر بوت‌نت‌ها هم اشاره کرد. در سطح اتحادیه اروپا سازمان ها و نهادهایی برای مدیریت حوادث با ساختاری متفاوت، مانند حوادث سایبری تشکیل یافته اند. از جمله آژانس امنیت اطلاعات و شبکه اروپایی که در سال ۲۰۰۴ رسما آغاز به کار کرد. اتحادیه اروپا سعی دارد با بکارگیری و تغییر چیدمان قوانین و نهادها و سازوکارهای موجود واکنشی متناسب با تهدیدهای سایبری ارائه دهد؛ در این راستا می توان به ایجاد نهادی به نام مرکز جرایم سایبری اروپا درون سازمان پلیس بین الملل اروپا یا ایجاد ستاد مشورتی بررسی مسائل سایبری اشاره کرد. (تراب زاده، ۱۳۸۸، ۶)

۶- جرم انگاری تروریسم در اسناد اتحادیه اروپا

با توجه به ناکارآمدی مقابله نظامی با تروریسم بلافاصله پس از حوادث تروریستی 11 سپتامبر که توقع و مطالبه عمومی حاکمیت قانون را بسیار کاهش داد، اتحادیه اروپا با تصویب اسناد حقوقی متعدد و با بازگشت به رویکرد اجرای قانون در مقابلهٔ با تروریسم، معیارهای جهانی را در دست یابی به توازن بین آزادی های مدنی و امنیت ملی وضع نموده و با توجه به اصل حاکمیت قانون ازرهگذرمقابله حقوقی با تروریسم سعی نمود خطرات جدی که از ناحیه شیوه جنگ علیه تروریسم متوجته حاکمیت قانون و اعتبار استانداردهای حقتوق بشر و حقتوق بشردوستانه بین المللی است را برطرف نماید. (بسته نگار، ۱۳۸۹، ۶۸)

اتحادیه اروپا در حوزه حقوق کیفری به موجب معاهده اتحادیه اروپایی سعی نمود مقابله با تروریسم را قاعده مند نماید. در دهه اخیر اسناد راهبردی متعددی را در خصوص مبارزه با تروریسم به تصویب رسانده که همگی حکایت از اهمیت اصل حاکمیت قانون، توجه به آزادی، امنیت و عدالت از طریق پیشگیری و مقابله با جرم دارد. مهم ترین خط مشی سیاست گذاری اتحادیه اروپا درمورد فضای مجازی، راهبرد مقابله با تروریسم شورای اتحادیه اروپاست که راهبرد و واکنش این اتحادیه تمرکز بر اصول حقوق کیفری و مبادی اجرای قانون در چهار رکن پیشگیری، حمایت، تعقیب و واکنش، سازمان دهی نموده است و به نام حمایت از حقوق شهروندان و پیشگیری از رادیکال سازی تأکید بسیار دارد. (آشوری، ۱۳۸۲، ۱۱)

اتحادیه اروپا درحوزه های متنوعی از امنیت فضای سایبر فعالیت کرده است. اتحادیه کشورهای اروپایی، سیاست های متعددی را در خصوص حملات علیه شبکه های رایانه‌ای، انتشار ویروس ها، کرم های رایانه‌ای، روجان ها، هرزنامه های اینترنتی، حملات فیشینگ و سرقت هویت صادر کرده است. باتوجه به اینکه موارد فوق، به طور غالب در تروریسم سایبری به کار می رود، می تتوان نتیجه گرفت که اتحادیه اروپا یکی از مهم ترین سازمان هایی است که به منظور پیشگیری از تروریستم سایبری گام برداشته است. این اتحادیه در سال ۲۰۰۴ به منظور اطمینان از امنیت «آژانس اطلاعات و شبکه در جامعه اروپا» را تأسیس کرد. هدف از تأسیس این آژانس، کمک به تقویت و توسعه فرهنگ امنیت اطلاعات و شبکه برای حفات از منافع شهروندان، مشتریان،سرمایه گتذاران و سازمان های عهده دار امور اجرایی کشور در اتحادیه اروپاست (ذوالفقاری، ۱۳۹۸، ۲۵)

همچنین کنوانسیون جرایم سایبر در سال ۲۰۲۰ در کنفرانس بین المللی که با شرکت کشورهای عضو شورای اروپا و چهار کشور دیگر (امریکا، ژاپن، آفریقای جنوبی و کانادا) تشکیل شد، به تصویب رسید و به کامل ترین سند بین المللی در مورد جرایم رایانه‌ای تبدیل شد. کنوانسیون مذکور، سه تعهد ضروری را بر دولت های عضو تحمیل می کند که عبارتند از: الف) جرم انگاری

برخی رفتارهای مرتبط با سامانه های رایانه‌ای؛ ب) وضع آیین دادرسی برای تحقیق و تضمین دسترسی پذیری آنها برای مجریان قانون داخلی برای تحقیق درباره جرایم سایبری؛ پ) ایجاد نظام همکاری بین المللی گسترده. براین اساس جرم انگاری تروریسم یک مسأله فراملی و برای پیشگیری از آن به راهبردهای همکاری فراملی نیاز هست. (خرم آبادی، ۱۳۸۴، ۳۷)

۶-۱ راهبردهای اتحادیه اروپا در کشف جرائم تروریستی

پس از یک سری حملات تروریستی از سال ۲۰۱۵، اتحادیه اروپا اقدامات مختلفی را برای متوقف کردن تروریسم اتخاذ کرده است. اگرچه مسئولیت مبارزه با تروریسم و حفظ امنیت در درجه اول بر عهده کشورهای عضو است، اما حملات تروریستی سال های اخیر نشان داده استت که این نیز یک مسئولیت مشترک است که آنها با ید با هم به دوش بکشند. راهبردهای اتحادیه اروپا درکشف جرائم تروریستی شامل راهبردهای تقنینی در مقابله با جرایم، اقدامات یوروپل در کشف جرائم تروریستی، اقدامات فرانکس و اقدامات ناتو می باشد. (آلبوعلی، ۱۳۹۲، ۷۸)

۶-۲ راهبردهای تقنینی در مقابله با جرائم

اقدامات تقنینی همان گونه که از نام آن پیداست، ار بر تصمیم گیری ها و اتخاذ قوانینی در مبارزها تروریسم در حوزه اتحاد یه اروپا میباشتد. این متوارد شامل کنوانستیون راجتع به سرکوبی تروریسم، اتخاذ سیاست مشترک در مبارزه با تروریسم، چارچوب تصمیم گیری شورا در مبتارزه باتروریسم و تدوین استراتژی مبارزه با تروریسم با رعایت حقوق بشر می باشد که در ذیل به بررستی هر یک خواهیم پرداخت. لازم به ذکر است که از آنجا که برای برخی از این متوارد منابع خاصی شامل کتب و مقالات وجود نداشته یا بسیار محدود می باشند، برای بررسی ماه یتی آنها بیشتر ازترجمه انگلیسی اسناد ذکر شده استفاده شده است. (توکل، ۱۳۸۴، ۲۰)

۶-۳ تصویب کنوانسیون اروپایی راجع به سرکوبی تروریسم (۱۹۷۷)

این کنوانسیون در سال ۱۹۷۷ توسط اعضای شورای اروپا بتا هدف رسیدن به اتحاد بیشتتر میان اعضاء در مبارزه با تروریسم و اطمینان از تعقیب و مجازات عاملان سوء قصدهای تروریستی به تصویب رسید. این کنوانسیون لزوم استرداد مجرمان و همکاری کشورها در این زمینه را عمل مهمی در مبارزه با تروریسم دانسته است. کنوانسیون لیستی از جرائمی که عنوان اعمال ترور یستی دارد را بیان نموده که بر استاس آن اقتداماتی مانندهواپیماربایی، سوء قصد علیه دیپلمات‌های کشوها،آدم ربایی، گرفتن گروگان، استفاده از بمب، نارنجک، موشک، اسلحه گرم به صورتخودکار، نامه و یا بمب بسته ای و امثال آن از مصادیق اعمال تروریستی عنوان گردیده است (ماده۱ کنوانسیون).

همان گونه که بیت ان گردید، برخی از مفتاد این کنوانسیون ناار به مستئله استرداد مجرمان می باشد. از آنجا که مبارزه با تروریسم نیازمند همکاری و مشارکت کشتورها مت یباشتد، لذا برای پرهیز از نزاع به دلیل اختلافات احتمالی نظام داوری برای حل وفصل مسالمت آمیز اختلافات دراین کنوانسیون پیش بینی شده است اگرچه پیشتر به دلیل ازدیاد جرائم سازمان‌یافته و فراملی در سطح اروپا، کنوانستیون های اروپایی استرداد به تصویب رسیده بود و مبنای کشورها برای استرداد مجرمان و مجازات آنها بود و کنوانسیون اروپایی سرکوب تروریسم مصوب ۱۹۷۷ نیز در ادامه همان سیاست ها به اصلاح برخی شرایط آنها اقدام نمود، اما همچنان تکیه بر موضوع استرداد مجرمان در این کنوانسیون برای مبارزه با تروریسم کافی نبود و نیاز به اندیشیدن راهکارهای بهتری در امر مبارزه با تروریسم بود (جمشیدی، ۱۳۹۰، ۹۸)

۶-۴ اتخاذ سیاست موضع مشترک در مبارزه با تروریسم (۲۰۰۱)

این سیاست ها با تصویب سندی با عنوان موضع مشترک شورا در استتفاده از اقتدامات خاص برای مبارزه با تروریسم در ۲۷ دسامبر سال ۲۰۰۱ توسط اتحادیه اروپا اتخاذ گردید. این سند در واقع ماحصل نشستی بود که شورای اروپا در ۲۱ دسامبر سال۲۰۰۱ برگزار کرد و در آن تروریستم را چالش واقعی جهان و مبارزه با آن را هدف اصلی اتحادیه اروپا عنوان نمود. در واقع

هدف ازتصویب این سند، ایجاد هماهنگی و داشتن موضع مشترک میان کشورهای اروپایی برای مبارزه باتروریسم خصوصاً تأمین منابع مالی و اجرای اقدامات بیشتر به منظور اجرای قطعنامه۱۳۷۳ (۲۰۰۱) شورای امنیت سازمان ملل متحد میباشد. همچنین عامل دیگری که در این سند به آن پرداخته شده است، همکاری کشورهای عضو به منظور تبادل اطلاعات با یکدیگر در مبارزه با تروریسم است. بر این اساس همکاری با دولت ایالات متحده آمریکا نیز در دستور کار اتحادیه اروپا قرارگرفته است. (باقرزاده، ۱۳۸۸، ۱۰)

به علاوه این سند برای تبیین بهتر اقدام به تعریف «افراد » و «گروه های تروریستی» و «اعمال تروریستی» نموده است. بر مبنای این سند افراد تروریست به کسانی اطلاق میشود که مرتکب و یا تلاش برای ارتکاب اعمال تروریستی می‌کنند و یا کسانی که در ارتکاب اعمال تروریستی مشارکت یا معاونت دارند. همچنین گروه های تروریستی شامل سازمان‌هایی است که به طور مستقیم یا به طور غیرمستقیم توسط این افراد کنترل می‌شوند. (جوکز، ۱۳۸۹، ۶۹)

این سند در تعریف اقدامات تروریستی، به احصاء یت ک سری اعمال مبادرت نموده است که چنانچه این اعمال به صورت عمدی صورت پذیرد در عمل، اقدام تروریستی محقق گردیده است. این موارد عبارتند از:

الف) انجام اعمال به منظور بی ثبات کردن یا از بین بردن ساختارهای اساسی، قانون اساسی، اقتصادی و اجتماعی یک کشور یا یک سازمان بین المللی؛ ب) انجام اقداماتی که باعث آسیب گسترده به دولت و یا تخریب تسهیلات عمومی، سیستم حمل ونقل، تأسیسات زیربنایی و... گردد؛ ج) تصرف هواپیما، کشتی یا دیگر وسایل حمل و نقل عمومی؛ چ) تولید، نگهداری، خرید، حمل ونقل، عرضه و یا استفاده از سلاح، مواد منفجره یا سلاح های هسته ای، بیولوژیکی یا شیمیایی و همچنین تحقیقات در و توسعه، سلاح های بیولوژیکی و شیمیایی؛ ح) انتشار مواد خطرناک که باعث آتش سوزی، انفجار و غیره گردد؛ خ) اخلال در تأمین آب، برق و یا هر منبع طبیعی اساسی دیگر که اثر آن منجر به خطر افتادن زندگی انسان‌ها گردد؛ د) شرکت در فعالیت های یک گروه تروریستی، از جمله با فراهم کردن اطلاعات یا منابع مادی یا مالی، با آگاهی از این واقعیت که این اعمال مشارکت در فعالی تهای جنایی یک گروه تروریستی می باشد. (Swire, 2005, 192)

این ماده در ادامه در تعریف «گروه تروریستی» عنوان نموده که گروه‌های تروریستی، به گروه های سازمان یافته‌ای گفته می‌شود که بیش از دو نفر بوده و در طی یک دوره از زمان تأسیس و با اعمالی هماهنگ اقدام به عملیات تروریستی می‌نمایند. درواقع آنچه به عنوان نشانه‌های این گروه‌ها بیان شده جدای از تعداد نفرات سازمان یافته بودن آن است. به بیانی دیگر اقدامات این گروه ها با مدیریت و هماهنگی توسط یک ارگان سازمان یافته انجام می‌شود. این سند به لحاظ احصاء جرائم تروریستی و همچنین تعاریف ذکر شده از اهمیت بسیار بالایی برخوردار است. به علاوه آنکه این سند توانست هماهنگی و انسجام لازم برای مبارزه با تروریسم را در سطح اتحاد یه اروپا به صورت جدی ایجاد نماید که این خود گام بسیار ارزشمندی در مبارزه با تروریسم در سطح بین الملل و اتحادیه اروپا محسوب می شود. (رضوی، ۱۳۸۶، ۴۲

۷- معاهده لیسبون

معاهده لیسبون مستلزم لغو ساختار سه ستونی است. چارچوب نهادی جدید برای سیاست های اقتصادی اعمال می شود و نقش بسیاری از نهادهای اروپایی تقویت شده است. کمیسیون دارای قدرت ابتکار است که با یک چهارم کشورهای عضو مشترک است و اسناد حقوقی (مقررات و دستورالعمل‌ها) توسط شورا (با اکثریت مشروح) و پارلمان اروپا تصویب می‌شوند. همچنین نقش دیوان دادگستری اروپا گسترش یافته است. به ویژه، کمیسیون این حق را دارد که متخلفان را به دلیل نقض تعهدات معاهدات به دادگاه معرفی کند. (walden, 2004, 273)

این نوآوری ها ممکن است فرصت های جدیدی را برای پیش نویس اقدامات قانونی خاص تر و نوآورانه تر در زمینه جرایم سایبری فراهم کند. به طور خاص، کمیسیون ممکن است رویه‌های نقض را علیه کشورهایی که کنوانسیون‌ها را اجرا نمی‌کنند باز کند و اتحادیه اروپا می‌تواند دستورالعمل جدیدی را اتخاذ کند که تعاریف دقیق‌تری را در مورد برخی از نکات نامشخص، همانطور که توسط ادبیات درخواست می‌شود، اتخاذ کند. با این حال، یک اقدام انتقالی به طور قابل توجهی این احتمالات را برای اقدامات اتخاذ شده، کاهش می دهد. همچنین در مورد مقررات انتقالی، اختیارات جدید کمیسیون و دیوان را در مورد رویه نقض به مدت پنج سال پس از لازم‌الاجرا شدن معاهده لیسبون (مگر اینکه اسناد قانونی اصلاح شوند) را مسدود می‌کند. اقدام انتقالی، تأثیر چارچوب نهادی جدید را کاهش می دهد، اما ممکن است همچنان به کمیسیون اجازه دهد تا پیشنهاد جدیدی در زمینه جرایم سایبری ارائه کند. برآورد بیش از حد قابل اجرا بودن تعهدات ممکن است مخاطره آمیز باشد. با این حال، این عنصر ممکن است در تشویق اجرای موثر کشورهای اتحادیه اروپا مفید باشد. در واقع، رویه نقض ممکن است واکنش های سیاسی و افکار عمومی را به همراه داشته باشد و در نهایت تعادل را به نفع اجرای اقدامات بین المللی در مورد جرایم سایبری تغییر دهد. (Stolz,1983,117)

برنامه استکهلم جانشین برنامه لاهه است و دستورالعمل ها و سیاست های توسعه را ارائه می کند. برنامه استکهلم به جرایم سایبری می پردازد و بر اهمیت اجرای کامل کنوانسیون‌ها و ترویج همکاری و تفاهم بهتر در زمینه جرایم سایبری تاکید می کند. به نظر نمی رسد که باعث ایجاد تغییرات اساسی در وضعیت کنونی شود. برنامه استکهلم اهمیت «اجرای مؤثر، اجرا و ارزیابی ابزارهای موجود» را برجسته می کند. بر این اساس، برنامه اجرای سازوکارهای «عینی و بی‌طرفانه» ارزیابی را فراهم می‌کند. بنابراین کمیسیون باید یک یا چند پیشنهاد برای ارزیابی سیاست های اتحادیه اروپا ارائه کند. از این منظر، همکاری قضایی در امور کیفری که باید اولین بخشی باشد که مورد ارزیابی قرار می گیرد. علاوه بر این، ارزیابی جدید باید شامل «سیستم پیگیری کارآمد» باشد.(Sharma,2005, 212)

بهبود روش‌های ارزیابی ممکن است یک فرصت مهم باشد. اگرچه اغلب در قوانین نادیده گرفته می شود، اما ممکن است پیشرفت های مهمی در کیفیت کلی اقدامات و سیاست های قانونی اتحادیه اروپا ایجاد کند. در واقع، ارزیابی فعلی توسط کمیسیون ناقص است و رویه های موثری برای حل مسائل مشکل زا ارائه نمی دهد. امکان ایجاد ارزیابی مؤثر و مستقل از اجرای اسناد قانونی اتحادیه اروپا ممکن است اثر معکوس ایجاد کند. البته کمیسیون هم ممکن است دلایل بهتری برای حمایت از نقض خود داشته باشد(Wired, 2002, 167)

سطح فعلی اجرای چارچوب قانونی اروپا در مورد جرایم سایبری چندین تناقض را نشان می دهد. این موارد بیشتر به عوامل امنیتی، سیاسی، اقتصادی و اعتباری در اجرای اقدامات بین‌المللی مربوط می‌شوند تا قابلیت اجرای قانونی آنها. در حال حاضر، اقدام اتحادیه اروپا موفقیت‌های قابل توجهی را نشان نمی دهد و مشکلات اجرای کنوانسیون‌های مربوطه این وضعیت را تأیید می کند. معاهده لیسبون و برنامه استکهلم تغییراتی را در این وضعیت ایجاد خواهند کرد، اما احتمالاً در کوتاه مدت تغییرات اساسی را در پی نخواهد داشت. با این وجود، این امکان وجود دارد که آنها در دراز مدت اجرای بهتر چارچوب قانونی در مورد جرایم سایبری را تحریک کنند. با توجه به ماهیت سریع در حال تغییر جرایم سایبری، جای تعجب است که آیا چارچوب حقوقی کنونی اروپا پس از اعمال این تغییرات در نهایت، همچنان اهمیت خواهد داشت یا خیر. (Schell,2004,103)

جرایم سایبری چالش های مهمی را برای سیستم های عدالت کیفری اروپا ایجاد می کند. رویکرد سه مسیری که در بالا توضیح داده شد، تلاش قابل توجهی برای بهبود کنوانسیون سرکوب اروپایی (و بین المللی) جرایم سایبری است و ابزارهای جدیدی را برای رسیدگی به این جرایم معرفی می کند. ثانیاً، تعاریف ملی چندین جرم مرتبط با رایانه را هماهنگ می کند. ثالثاً، حداقل چارچوبی را برای همکاری بین المللی در مورد مسائل جنایی فراهم می کند. چارچوب قانونی ارائه شده توسط کنوانسیون‌ها به طور کلی گامی مهم به جلو در واکنش بین المللی به جرایم سایبری در نظر گرفته شده است. برخی از این انتقادات ممکن است به دلیل درک نادرست از عملکرد کلی همکاری های بین المللی در امور کیفری یا توجه به حقوق و آزادی های بشر باشد. با این حال، اثربخشی و اجرای واقعی این اسناد بین‌المللی همچنان حیاتی‌ترین مسائل است. در واقع، اجرای قانونی آنها مشکلاتی را

نشان می دهد و به نظر می رسد اجرای غیرمستقیم این موارد موفقیت آمیزتر باشد. این امر از این ایده حمایت می کند که موضوعات غیر قانونی مانند امنیت ملی، سیاست، اقتصاد و افکار عمومی عوامل مهم تری نسبت به قابلیت اجرایی قانونی در اجرای این اسناد بین المللی هستند. تا کنون، ارزش افزوده اقدام اتحادیه اروپا در این بخش نسبتاً کم به نظر می رسد. معاهده لیسبون و برنامه استکهلم ممکن است این وضعیت را بهبود بخشد، اما نباید انتظار داشت که این اتفاق در مدت کوتاهی رخ دهد.(Yam,2001,135)

نتیجه گیری

بررسی روش های پیشگیری از جرایم سایبری فناوری اطلاعات مبتنی بر روش‌های فناوری اطلاعات شامل ردیابی هویت مجازی مهاجمان، گشت‌زنی در فضای مجازی و کنترل و پایش فضای مجازی، جمع‌آوری مدارک الکترونیکی جرایم و مستندسازی صحنه جرم در پیشگیری از جرایم سایبری مؤثر است. پیشگیری از جرایم سایبری با محوریت جرم یابی از جرایم سایبری تنها با پیشگیری وضعی و یافته های جرم یابی راه به جایی نمی برد. اگرچه از این طریق، پیشـــگیری تســـهیل می گردد؛ لیکن ناکافی به نظرمی رسد. فلذا بایستی با کمک شناسایی انواع راه های پیشـــگیری که از علوم مختلف حاصل می گردد؛ به صورت همه جانبه و در سطح ملی و بین المللی به مقابله با جرایم سایبری به عنوان یکی از جلوه های بزهکاری نوین پرداخت. پیشگیری از جرایم سایبری و محدودیت های حاکم بر آن از با توجه به افزایش آمار جرایم و استفاده از روش های جدید ارتکاب جرایم سایبری و ناکارآمدی واکنش های مجرمانه، لزوم استفاده از اقدامات پیشگیرانه در قالب اقدامات فنی با هدف پیشگیری از افرادی که با تغییر شرایط محیطی مصمم به ارتکاب جرم هستند. در دهه های اخیر در بسیاری از کشورهای جهان مورد توجه قرار گرفته است.

بی شک به موازات گسترش فعالیت ها و ارتباطات در فضای مجازی، برخی مجرمان نیز فعالیت مجرمانه خود را به فضای مجازی منتقل کرده و یا از طریق چنین فضایی مرتکب جرم می شوند. تحقیقات در ابعاد مختلف جرایم سایبری نشان می‌دهد که رایانه ها و شبکه های ارتباطی دارای ویژگی هایی هستند که فرصت بسیار خوبی را برای مجرمان ایجاد می کند. اصولاً زیاده روی منجر به مشکلات خواهد شد. مثل تکنولوژی کامپیوتر و ارتباطات، سهولت ارتباط بین مردم و نیازهای فراوان انسانها در هر زمینه ای اجابت کرده است و موفقیت و آسایش را به ارمغان آورده اند، از سوی دیگر در طول مسیرراه را برای جنایتکاران و مجرمان فراهم می کند. سازمان ملل و اتحادیه اروپا قوانین بیشتر و جرایم سخت تری را در مورد جرایم سایبری در نظر گرفته اند. سازمان‌های بین‌المللی و منطقه‌ای از جمله اتحادیه اروپا با تنظیم قوانین و مقررات مرتبط در قالب تدابیر قانونی به عنوان یکی از مهم‌ترین عناصری که در فرآیند تدوین قوانین در این زمینه باید مورد توجه قرار گیرد، نقش مهمی را ایفا می‌کنند. اتحادیه اروپا با توجه به ساختار خود، با تصویب اسناد و الزامات مختلف، از جمله معاهدات، قطعنامه های چارچوب و دستورالعمل های متعدد، سعی در ایجاد و توسعه چارچوب های قانونی دارد. اتحادیه اروپا با تصویب اسناد حقوقی متعدد و با بازگشت به رویکرد اجرای قانون در مقابله‌ی با تروریسم، معیارهای جهانی را در دست یابی به توازن بین آزادی های مدنی و امنیت ملی وضع نموده و با توجه دوباره به محوریت اصل حاکمیت قانون از رهگذر مقابله حقوقی با تروریسم ,سعی نمود خطرات جدی که از ناحیه شیوه جنگ علیه تروریسم متوجه حاکمیت قانون و اعتبار استانداردهای حقوق بشر و حقوق بشردوستانه بین المللی است را برطرف نماید؛

برای پیشگیری همه جانبه از جرایم رایانه‌ای و بین المللی بودن، باید بر اساس رویکردها، اصول و مبانی یک سند پذیرفته شده بین المللی در زمینه پیشگیری از جرم عمل کرد. بر این اساس سند پیشگیری از جرم سازمان ملل متحد مصوب ۲۰۰۲ می تواند به عنوان سند راهبردی پیشگیرانه جرایم رایانه‌ای در دستور کار کارشناسان حقوقی و مسئولان مرتبط قرار گیرد. اتحادیه اروپا در حوزه حقوق کیفری به موجب معاهده اتحادیه اروپایی, سعی نمود مقابله با تروریسم را قاعده مند نماید. در دهه اخیر اسناد راهبردی متعددی را در خصوص مبارزه با تروریسم به تصویب رسانده که همگی حکایت از اهمیت اصل حاکمیت قانون, توجه

به آزادی ,امنیت و عدالت از طریق پیشگیری و مقابله با جرم دارد. مهم ترین سند سیاست گذاری اتحادیه اروپا در مورد تروریسم ,راهبرد مقابله با تروریسم شورای اتحادیه اروپاست, که این راهبرد واکنش به تروریسم را با تمرکز بر اصول حقوق کیفری و مبادی اجرای قانون در چهار رکن پیشگیری, حمایت, تعقیب و واکنش سازمان دهی نموده است و بر تامین یا حمایت از حقوق شهروندان و پیشگیری از رادیکال سازی تاکید بسیار دارد.

این مقاله چارچوب قانونی اروپا در مورد جرایم سایبری را تجزیه و تحلیل می کند. در ابتدا، چالش‌های جرایم سایبری برای سیستم‌های عدالت کیفری سنتی را مورد بحث قرار می‌دهد. متعاقباً، بر چارچوب حقوق کیفری در مورد جرایم سایبری با دیدگاه عمدتاً اروپایی تمرکز می کند. چارچوب حقوقی اروپا یک راه حل سه راه ارائه می دهد: کاهش اصطکاک بین قوانین ملی، معرفی پتانسیل‌های تحقیقاتی جدید و تسهیل همکاری بین المللی. علاوه بر این، به نظر می رسد اجرای مؤثر اسناد قانونی اصلی به قابلیت اجرایی قانونی این اقدامات بین المللی بستگی ندارد. در مقابل، عوامل غیر قانونی دیگری مانند امنیت ملی، سیاست، اقتصاد و افکار عمومی به نظر می‌رسد که اجرای دقیق چارچوب قانونی اروپا را میسر می‌کنند. در این زمینه، ابتکارهای اتحادیه اروپا بسیار کم است، اگرچه معاهده لیسبون و برنامه استکهلم ممکن است این وضعیت را در دراز مدت بهبود بخشد.

جرایم سایبری چالش های متعددی را برای قوانین کیفری سنتی و سیستم عدالت کیفری به طور کلی ایجاد می کند. اولین چالش به تعریف آن مربوط می شود. باید در تحلیل چارچوب قانونی اروپا در مورد جرایم سایبری بین جرایم سایبری که در آن سیستم های اطلاعاتی هدف یا ابزار جرم هستند تمایز قائل شویم. اولین گروه از جرایم سایبری شامل جرایم علیه محرمانه بودن، یکپارچگی و در دسترس بودن داده ها و سیستم های اطلاعاتی است. یک نمونه از این جرایم، دسترسی غیرقانونی به رایانه شخصی به منظور جمع آوری یا حذف داده ها است. گروه دوم، جرایم رایانه ای هستند که رایانه اگرچه ابزار مجرمانه است، ولی برای ارتکاب این جرم ضروری نیست. مثلا کلاهبرداری با کارت اعتباری و از طریق یک سایت اینترنتی طراحی شده برای این کار. گروه سوم شامل جرایم مرتبط با محتوا، مانند پورنوگرافی کودکان و اعمال نژادپرستانه و بیگانه هراسانه است. این رفتارها زمانی که با استفاده از یک سیستم کامپیوتری ارتکاب یابد در رده جرایم سایبری قرار می گیرند. گروه چهارم مربوط به نقض حقوق مالکیت فکری است، مانند کپی برداری و فروش غیرمجاز نرم افزارهای کامپیوتری.

منابع

۱. زندی، محمدرضا، تحقیقات مقدماتی در جرائم سایبری، نشر جنگل، چ سوم، ۱۳۹۲،
۲. زندی، محمدرضا، تحقیقات مقدماتی در جرایم سایبری، چاپ دوم، تهران، انتشارات جنگل، ۱۳۹۳.
۳. رضوی، محمد(۱۳۸۶). «جرائم سایبری و نقش پلیس در پیشگیری از این جرائم و کشف آنها»، فصلنامه دانش انتظامی، سال نهم، ش ۱.
۴. دی انجلیز، جینا، جرائم سایبر، ترجمه‌ی سعید حافظی و عبد الصمد خرم آبادی، ۱۳۸۳،چاپ اول، تهران: دبیر خانه‌ی شورای عالی اطلاع رسانی.
۵. دزیانی، محمد حسن، مبانی صلاحیت کیفری در فضای سایبر، کار پژوهشی شورای عالی انفورماتیک، ۱۳۸۴،
۶. دزیانی، محمد حسن (۱۳۸۹). جرایم سایبری، تهران: روزنامهٔ رسمی جمهوریاسلامی ایران.
۷. دبلفون، زویه لینان، حقوق تجارت الکترونیک، ترجمه ستار زرکلام، نشر شهر دانش، چ اول، ۱۳۸۸.
۸. خرم آبادی، احمد، مسئولیت کیفری ارائه دهندگان خدمات اینترنتی، چاپ اول، تهران، انتشارات دادیار،۱۳۹۱.
۹. خالقی، علی، جستارهایی از حقوق جزای بین الملل، چاپ دوم، تهران، انتشارات شهر دانش، ۱۳۹۰.
۱۰. حسنوی، رضا و فرسایی، داریوش(۱۳۷۹). فرهنگ تشریحی کامپیوترماکروسافت ۲۰۰۰، تهران: انتشارات دانشیار.
۱۱. حسن بیگی، ابراهیم، حقوق و امنیت در فضای سایبر، چاپ اول، تهران : موسسه فرهنگی تحقیقات ابرار معاصر تهران، ۱۳۸۴.
۱۲. حسن بیگی، ابراهیم(۱۳۸۴). حقوق و امنیت در فضای سایبر، تهران، مؤسسه مطالعات و تحقیقات بین المللی ابرار معاصر.
۱۳. حبیب زاده، محمدجعفر و امیرحمزه زینالی(۱۳۸۴). «درآمدی بر برخی محدودیت های عملی جرم انگاری»،نامه حقوقی، جلد اول، ش ۱.
۱۴. حاجیلی، محمود) ۱۳۸۸(. وضعیت فناوری ارتباطات در حوزه جوانان، دبیرخانه شورای عالی اطلاع رسانی.
۱۵. حاجی دهآبادی، احمد (۱۳۸۹). «مقررات کیفری لایحه حمایت از خانواده در بوته نقد»، مطالعات راهبردی زنان (کتاب زنان سابق)، ش ۴۸.
۱۶. حاجی ده آبادی، احمد، جبران خسارت بزهدیده، ناشر سازمان انتشارات پژوهشگاه فرهنگ و اندیشه اسلامی، ۱۳۸۸.
۱۷. جیمز اسلوین، اینترنت و جامعه. ترجمه: عباس گیلوری و علی رادباوه، ۱۳۸۰، چاپ اول، تهران: انتشارات کتابدار.
۱۸. جوکز، یونی و همکاران، جرم و اینترنت، برگردان: رسول نجار، تهران، انتشارات دانشگاه علوم انتظامی، ۱۳۸۹.
۱۹. جوکز، یونی و همکاران(۱۳۸۹). جرم و اینترنت، ترجمه: رسول نجار، تهران:
۲۰. جوانمرد، بهروز، آیین دادرسی کیفری اختصاصی در جرایم سازمان یافته فراملی، چاپ اول، تهران، انتشارات جنگل، ۱۳۶۳.
۲۱. جوان جعفری، عبدالرضا و مهدی سیدزاده ثانی(۱۳۹۱). رهنمودهای عملی پیشگیری از جرم، معاونت پیشگیری از وقوع جرم قوه قضائیه، چاپ اول، تهران، انتشارات میزان.
۲۲. جمشیدی، علیرضا، سیاست جنایی مشارکتی، چاپ اول، تهران، انتشارات میزان، ۱۳۹۰.
۲۳. جمشیدی، علیرضا(۱۳۹۰). سیاست جنایی مشارکتی، چاپ اول، تهران، انتشارات میزان.
۲۴. جلالی فراهانی، امیر حسین، ترجمه کنوانسیون جرایم محیط سایبر ۲۰۰۱، چاپ اول، تهران، مرکز مطبوعات و انتشارات قوه قضائیه، ۱۳۸۳.
۲۵. جلالی فراهانی، امیر حسین، منفرد، محبوبه، زیر نظر علی حسین نجفی ابرند آبادی، تهران، میزان، چاپ نخست، ۱۳۹۱.
۲۶. جلالی فراهانی، ا.(۱۳۹۴)، درآمدی بر آئین دادرسی کیفری جرایم سایبری، تهران: انتشارات خرسندی، چاپ دوم.
۲۷. جلالی فراهانی، ا. (۱۳۹۵)، کنوانسیون جرایم سایبر و پروتکل الحاقی آن، تهران، انتشارات خرسندی،چاپ دوم.
۲۸. جلالی فر اهانی، امیرحسین، درآمدی بر آیین دادرسی کیفری جرائم سایبری، انتشارات خرسندی، ۱۳۸۹.
۲۹. جاویدنیا، جواد، جرائم تجارت الکترونیکی، نشر خرسندی، ۱۳۸۷
۳۰. توکل، محمد و ابراهیم کاظم پور(۱۳۸۴). دگرگونی های اجتماعی در یک جامعه اطلاعاتی، تهران،انتشارات کمیسیون ملی یونسکو.
۳۱. تراب زاده، حسین، بررسی صحنه های جرم الکترونیکی، فصلنامه کارآگاه، شماره ۶، ۱۳۸۸.
۳۲. پیکا، ژرژ (۱۳۹۰). جرم شناسی، ترجمه علی حسین نجفی ابرندآبادی، چاپ دوم، تهران، انتشارات میزان.
۳۳. پاکزاد، بتول، جرائم کامپیوتری، پایان نامه کارشناسی ارشد حقوق جزا و جرم شناسی، دانشکده حقوق دانشگاه شهید بهشتی،۱۳۸۵.
۳۴. بکاریا، سزار (۱۳۸۰). رساله جرائم و مجازاتها، ترجمه محمدعلی اردبیلی، چاپ دوم، تهران، انتشارات میزان.
۳۵. بسته نگار، محمد، حقوق بشر از منظر اندیشمندان، شرکت سهامی انتشار 1389
۳۶. باقرزاده، فاطمه، امضای دیجیتال و هویت مجازی، مجموعه مقالات دومین کنفرانس شهر الکترونیکی، نشر جهاد دانشگاهی، تهران، ۱۳۸۸.
۳۷. باستانی، برومند، جرائم کامپیوتری و اینترنتی جلوه ای نوین از بزهکاری، چاپ سوم، تهران،بهنامی، ۱۳۹۰
۳۸. انصاری، محمد باقر، حریم خصوصی، انتشارات سمت، چ دوم، ۱۳۸۶.
۳۹. انصاری، باقر، حقوق رسانه، چاپ اول، تهران، انتشارات سمت، ۱۳۹۰.
۴۰. امیدی، جلیل، حقوق بشر در دعاوی کیفری بر اساس اسناد بین المللی و منطقه ای، مجله دانشکده حقوق و علوم سیاسی دانشگاه تهران، ش ۴۹، ۱۳۷۹، ص۳۹ و نیز همو، دادرسی کیفری و حقوق بشر، مجله پژوهش و مجلس، س۱۰، ش ۳۸، تابستان ۱۳۸۲.
۴۱. آلبوعلی، امیر، صلاحیت محاکم در جرائم سایبری، تهران، انتشارات جنگل، ۱۳۹۲.

۴۲. اکبری فومنی، فرناز، اصل برائت در گذار تاریخ، مجله حقوقی دادگستری، دوره جدید، ش ۶۲ و ۶۳، بهار و تابستان ۱۳۸۷.
۴۳. آقایی جنت مکان، حسین، تضمین حقوق متهم در قانون تشکیل دادگاه های عمومی و انقلاب مصوب ۱۳۷۳، پایان نامه کارشناسی ارشد حقوق جزا و جرم شناسی، دانشگاه تربیت مدرس، دانشکده علوم انسانی، ۱۳۷۵.
۴۴. اصلانی، حمیدرضا، حقوق فناوری اطلاعات، نشر جنگل، چ سوم، ۱۳۹۱.
۴۵. آشوری، محمد، عدالت کیفری، انتشارات گنج دانش، چ اول، ۱۳۷۶، ص ۶۷ و نیز همو، نگاهی به حقوق متهم در حقوق اساسی و قانون آئین دادرسی دادگاه های عمومی و انقلاب در امور کیفری، مجله مجتمع آموزشی عالی قم، سال اول، شماره سوم، ۱۳۸۸،
۴۶. آشوری، محمد، حقوق بشر و مفاهیم مساوات، انصاف و عدالت، ج اول، انتشارات گرایش، چ سوم، ۱۳۸۳،
۴۷. آشوری، محمد، آیین دادرسی کیفری، جلد دوم، تهران، انتشارات سمت، چاپ سوم، ۱۳۸۲.
۴۸. اسلامی، ابراهیم، جایگاه حمایت از بزه دیدگان جرائم سایبری در مقررات کیفری حقوق داخلی و حقوق بین الملل، پژوهش نامه حقوق اسلامی، سال هفدهم، شماره ۱.
۴۹. آریا، ناصر، فرهنگ اصطلاحات کامپیوتر و شبکه های کامپیوتری، مرکز تحقیقات تخصصی حسابداری و حسابرسی، ۱۳۷۲.
۵۰. امامی، محمد، مصلحت گرایی در دادرسی های جزایی، مجله حقوقی دادگستری، ش۲۳، تابستان ۱۳۷۷
۵۱. پوربافرانی، حسین، اصل صلاحیت واقعی در حقوق جزای بین الملل و ایران، مجله حقوقی دادگستری، ۱۳۸۲، شماره ۴۲،
۵۲. پی جوی صحنه جرم الکترونیک، بخش اول، ترجمه و تلخیص محمدحسن دزیانی، خبرنامه انفورماتیک، سال ۱۹، ش۹۴، بهمن ۱۳۸۳.
۵۳. جلالی فراهانی، ا. (1387)، جنبه های حقوقی اقدامات کیفری بین المللی مجریان قانون در قبال جرایم سایبری، فصلنامه مطالعات پیشگیری از جرم، سال 3، شماره 8، صص 81-35.
۵۴. جلالی فراهانی، امیر حسین، صلاحیت کیفری در فضای سایبر، نشریه فقه و حقوق، سال سوم، شماره ۱۱، ۱۳۸۵.
۵۵. جلالی فراهانی، امیر حسین، منفرد، محبوبه، حمایت قانونی از آسیب دیدگان سایبری، فصلنامه مجلس و راهبرد، سال بیستم، شماره ۳، بهار ۱۳۹۲.
۵۶. جلالی فراهانی، امیرحسین (۱۳۸۳). «پیشگیری از جرائم رایانه ای»، مجله حقوقی دادگستری، ش ۴۷.
۵۷. جلالی فراهانی، امیرحسین، «پول شویی الکترونیکی»، فصلنامه فقه و حقوق 1389
۵۸. جلالی فراهانی، امیرحسین، «پیشگیری از جرائم رایانه ای»، مجله حقوقی دادگستری 1392
۵۹. جلالی فراهانی، امیرحسین، استنادپذیری ادله الکترونیکی در امور کیفری، مجله فقه و حقوق، س ۴، ش ۱۵، ۱۳۸۶.
۶۰. جلالی، علی اکبر(1391).رفتار شناسی مجرمان در فضای سایبر، فصلنامهٔ کارآگاه، دورهٔ دوم، سال ششم، شمارهٔ 21.
۶۱. جوان جعفری، عبدالرضا (۱۳۸۵). «جرائم سایبر و چالش های نوین سیاست کیفری»،مجموعه مقالات همایش جهانی شدن حقوق و چالش های آن، مشهد، دانشگاه فردوسی.
۶۲. حبیب زاده، محمدجعفر و اسماعیل رحیمی نژاد (۱۳۸۷). «مجازات های نامتناسب مجازاتهای مغایر با کرامت انسانی»، فصلنامه حقوق دانشگاه تهران، دوره ۳۸، ش ۲.
۶۳. حبیب زاده، محمدجعفر و سید مصطفی محقق داماد، اصل قانونی بودن جرائم و مجازات ها در حقوق ایران، نشریه دانشگاه شاهد، ش ۲۰، ۱۳۷۴.
۶۴. خرم آبادی، عبدالصمد، تاریخچه، تعریف و طبقه بندی جرم رایانه‌ای، مجموعه مقالات همایش بررسی جنبه های حقوقی فناوری اطلاعات، معاونت حقوقی و توسعه قضایی قوه قضاییه، نشر سلسبیل، چاپ اول، ۱۳۸۴.
۶۵. خرم آبادی، عبدالصمد، کلاهبرداری رایانه‌ای از دیدگاه بین المللی و وضعیت ایران، فصلنامه حقوق، دانشکده حقوق و علوم سیاسی دانشگاه تهران، سال ۳۷، شماره ۲، تابستان ۸۶.
۶۶. خسروی فارسانی، علی، بیراوند، شاهپور، مقایسه وجه التزام و خسارت تنبیهی، مجله حقوقی دادگستری، ۱۳۸۹.
۶۷. داودی گرمارودی، هما، مکتب نئوکلاسیک و احیاء رویکرد سزاده، مجله حقوق دانشکده حقوق و علوم سیاسی تهران، شماره ۶۸، تابستان ۱۳۸۴
۶۸. درگاهی، حسین و رضوی، سید منصور(1386). اعتیاد به اینترنت و عوامل مؤثر برآن در ساکنان منطقه 2 غرب تهران، فصلنامهٔ پایش، سال ششم، شمارهٔ سوم، صص272-265.
۶۹. ذوالفقاری، سهیل، توانگر، علی، سیاست تقنینی جمهوری اسلامی ایران در زمینه جرائم رایانه‌ای، نشریه PURE LIFE , پاییز ۱۳۹۸.
۷۰. ر ضوی، محمد و سیدعلی خزایی، حقوق شهروندی در فرایند کشف جرم، فصلنامه دانش انتظامی، سال نهم، شماره چهارم، ۱۳۸۹.
۷۱. رجبی پور، محمود(۱۳۸۲). راهبرد پیشگیری اجتماعی از جرم(تعامل پلیس ودانش آموزان)، فصلنامهٔ دانش انتظامی، سال پنجم، شمارهٔ سوم، صص 32-7.
۷۲. رحمدل، منصور، حق انسان بر حریم خصوصی، مجله دانشکده حقوق و علوم سیاسی دانشگاه تهران، شماره ۷، زمستان ۱۳۸۳.
۷۳. رحمدل، منصور، قانون اساسی ایران و اصل برائت، نشریه حقوق اساسی، سال چهارم، ششم و هفتم، زمستان ۱۳۸۵.
۷۴. رستمی، ولی(۱۳۸۶). «مشارکت مردم در فرایند کیفری» (بررسی سیاست جنایی کشورهای غربی)،فصلنامه حقوق دانشگاه تهران، سال ۳۷، ش ۲.
۷۵. رستمی، ولی، مشارکت مردم در فرایند کیفری، فصلنامه حقوق دانشگاه تهران، سال ۳۷، شماره ۲، ۱۳۸۶.

منابع انگلیسی

1. Schell, B. H., & C. Martin (2004), Cyber crime: A Reference Handbook, Santa Barbara, California: ABC-CLIO.

2. - Sharma, A. (2005), "World Seeks a Wider Web Role", Congressional Quarterly Weekly, Report Nov 14, pp. 3039-3047.
3. Simon, G. E. (1998), "Cyberporn and Censorship: Constitutional Barriers to Preventing Access to Internet Pornography by Minors", The Journal of Criminal Law and Criminology, 88(3), pp. 1033-1043.
4. Silver, O. (2001), "European Cyber Crime Proposal Released", Computer Fraud and Security, (5), pp. 3-17.
5. Sinrod, E. J. & W.P. Reilly (2000), "Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws", Santa Clara Computer and High Technology Law Journal, 16(2), pp. 3-51.
6. Speer, D. L. (2000), "Redefining Borders: The Challenges of Cyber Crime", Law and Social Change, 34, pp. 261-273.
7. Stolz, B. A. (1983), "Congress and Capital Punishment: An Exercise in Symbolic Politics", Law and Policy Quarterly, 5(2), pp. 153-165.
8. Swire, P. P. (2005), "Elephants and Mice Revisited: Law and Choice of Law on the Internet", University of Pennsylvania Law Review, 153(6), pp. 1979-1992.
9. U.S. Ratifies International Cyber Crime Treaty (2006), Computer Fraud and Security, November 5, pp. 1-27.
10. Walden, I. (2004), "Harmonising Computer Crime Laws in Europe", European Journal of Crime; Criminal Law and Criminal Justice, 12(4), pp. 325-335.
11. Wales, E. (2000), "Draft Council of Europe Cyber Crime Convention Upsets Civil Rights Bodies", Computer Fraud and Security Issue, 12, pp. 5-17.
12. Wible, B. (2003), "A Site Where Hackers Are Welcome: Using Hack-In Contests to Shape Preferences and Deter Computer Crime" The Yale Law Journal, 112(6), pp. 1573- 1581.
13. Wired Society (2002), The Nation, May 4.
14. Yam, J. T. (2001), "Cyber crime Treaty Under Way", Business Word, May 3, pp. 5-13.