Scientific-Research Quarterly Siasat-e Motalieh
13th Year, No. 50, 2025

Cyber Security; Capabilities and Capacities of Domestic and International Legal Systems

Farhad Moradi Haqgo[1], Bagher Shamloo[2], Alireza Saybani[3]

[1] *PhD., Student, Department of Criminal Law and Criminology, Qe.C., Islamic Azad University, Qeshm, Iran. fmh.lawyer@yahoo.com*
[2] *Associate Professor, Department of Criminal Law and Criminology, Faculty of Law, Shahid Beheshti University, Tehran, Iran* ***(Corresponding author).*** *baghershamloo@yahoo.com*
[3] *Assistant Professor, Department of Law, BA.C., Islamic Azad University, Bandar Abbas, Iran. saybani.a@gmail.com*

Abstract

Cyberspace has the capability for the entry of every human being regardless of age, gender, and nationality with different thoughts. The possibility of committing various crimes exists in this domain, just as all positive functions do. This matter necessitates the discussion of cyber security. One of the most important factors in addressing this subject is the necessity of protecting victims, especially considering the trans-spatial and trans-border dimensions of crimes committed in cyberspace. Indeed, on the one hand, due to the lack of access to the location of cyber criminals in some instances caused by changing or spoofing IPs, and on the other hand, due to the failure to discover crimes in a timely manner and the not-so-suitable speed in identifying the perpetrator, attention to protective approaches in this field within the framework of adopting passive jurisdiction in handling these crimes has made it inevitable. This research intends to answer the question of how the Iranian judicial system can resolve the challenges of cyber security. To answer this question, a data analysis method in a descriptive-analytical form has been used. The results indicate that the Iranian judicial system, in alignment with certain transnational documents and the capacity to utilize the provisions of Article 8 of the Islamic Penal Code and Article 664 of the Criminal Procedure Code, can resolve many legal challenges and loopholes to protect victims and facilitate the strengthening of security. Recourse to the principle of passive jurisdiction in international criminal law regulations and the expansion of national and regional jurisdictions is considered the most important solution in this arena.

Keywords: Cyber Crimes, Cyber Security, Iranian Legal System, International Law.

Received: 2025-02-25 ; **Received in revised form:** 2025-04-05 ; **Accepted:** 2025-04-29 ; **Published online:** 2025-07-01
https://doi.org/10.22034/sm.2025.1995716.2047

http://sm.psas.ir **Article type:** Research Article
Publisher: Political Studies Association of the Seminary

فصلنامه علمی - پژوهشی سیاست متعالیه
سال ۱۳، شماره ۵۰، ۱۴۰۴

امنیت سایبری؛ قابلیت‌ها و ظرفیت‌های نظام حقوق داخلی و بین‌المللی

فرهاد مرادی حقگو[۱]، باقر شاملو[۲]، علیرضا سایبانی[۳]

[۱] دانشجوی دکتری، گروه حقوق کیفری و جرم‌شناسی، واحد قشم، دانشگاه آزاد اسلامی، قشم، ایران.
fmh.lawyer@yahoo.com

[۲] دانشیار، گروه حقوق جزا و جرم‌شناسی، دانشکده حقوق، دانشگاه شهید بهشتی، تهران، ایران (**نویسنده مسئول**).
baghershamloo@yahoo.com

[۳] استادیار، گروه حقوق، واحد بندرعباس، دانشگاه آزاد اسلامی، بندرعباس، ایران. saybani.a@gmail.com

چکیده

فضای سایبری قابلیت ورود هر انسانی جدا از سن، جنس و ملیت را با اندیشه‌های متفاوت دارد. امکان ارتکاب جرائم مختلف در این حوزه مانند همه کارکردهای مثبت در آن، وجود دارد. این امر موجب بحث از امنیت سایبری می‌شود. یکی از مهم‌ترین عوامل پرداختن به این موضوع، ضرورت حمایت از بزه‌دیدگان، به‌ویژه با توجه به ابعاد فرامکانی و فرامرزی جرائم ارتکابی در فضای سایبر است. درواقع، از یک‌سو با توجه به عدم دسترسی به موقعیت مجرمان سایبری در بعضی مواقع به جهت تغییر و یا تقلب در IP و از سوی دیگر، عدم کشف به‌موقع و سرعت نه‌چندان مناسب در شناسایی مرتکب، توجه به رویکردهای حمایتی در این زمینه را در چارچوب اتخاذ صلاحیت منفعل در رسیدگی به این جرائم اجتناب‌ناپذیر ساخته است. این پژوهش درصدد پاسخ به این سوال است که نظام دادرسی ایران چگونه می‌تواند چالش‌های امنیت سایبری را رفع نماید؟ برای پاسخ به این سوال از روش تحلیل داده‌ها به صورت توصیفی- تحلیلی استفاده شده است. نتایج حاکی از آن است که نظام دادرسی ایران همسو با برخی اسناد فراملی و ظرفیت بهره‌مندی از مفاد ماده ۸ قانون مجازات اسلامی و ماده ۶۶۴ قانون آیین دادرسی کیفری، می‌تواند بسیاری از چالش‌ها و خلأهای قانونی را در جهت حمایت از بزه‌دیدگان رفع نموده و موجبات تقویت امنیت را فراهم سازد. توسل به اصل صلاحیت منفعل در مقررات حقوق بین‌الملل کیفری و توسعه صلاحیت‌های ملی و منطقه‌ای مهم‌ترین راه‌حل در این عرصه محسوب می‌شود.

واژه‌های کلیدی: جرائم سایبری، امنیت سایبری، نظام حقوقی ایران، حقوق بین‌الملل.

استناد به این مقاله: مرادی حقگو، فرهاد؛ شاملو، باقر؛ سایبانی، علیرضا (۱۴۰۴). امنیت سایبری؛ قابلیت‌ها و ظرفیت‌های نظام حقوق داخلی و بین‌المللی. *سیاست متعالیه*، ۱۳(۲): ص۲۹۳-۳۰۷. https://doi.org/10.22034/sm.2025.1995716.2047

تاریخ دریافت: ۱۴۰۳/۱۲/۰۷ ؛ **تاریخ اصلاح:** ۱۴۰۴/۰۱/۱۶ ؛ **تاریخ پذیرش:** ۱۴۰۴/۰۲/۰۹ ؛ **تاریخ انتشار:** ۱۴۰۴/۰۴/۱۰

ناشر: انجمن مطالعات سیاسی حوزه **نوع مقاله:** پژوهشی http://sm.psas.ir

۱. مقدمه

نگاهی گذرا به بحث «صلاحیت» در حوزهٔ دادرسی کیفری، بیانگر احترام به اصل سرزمینی بودن در چارچوب توجه به مکان وقوع جرم است. امری که اگرچه از حیث تاریخی قابل‌توجه است، در حال حاضر نیز مبنای اصلی صلاحیت مراجع قضایی در رسیدگی به جرائم را تشکیل می‌دهد. در این راستا، با شکل‌گیری و توسعهٔ فضای سایبر/مجازی و موضوعات کیفری پیرامون آن، صلاحیت رسیدگی به جرائم سایبری همواره به‌عنوان یکی از موضوعات اساسی در پهنهٔ نظام‌های دادرسی کیفری مطرح بوده است. این امر زمانی از اهمیت برخوردار می‌شود که ضرورت حمایت از بزه‌دیدگان، به مسئله‌ای کلیدی در این‌گونه از جرائم تبدیل شده است. ماهیت فرامرزی جرائم سایبری و احتمال بزه‌دیدگی اشخاص فراتر از مرزهای قانونی یک کشور، بازنگری در برخی اصول دادرسی کیفری و توجه به رویکردهای مساعد به حال بزه‌دیدگان را اجتناب‌ناپذیر و ضروری ساخته است. مکان در فضای سایبر تفاوتی ماهوی و معنادار با مکان در فضای حقیقی دارد؛ از این‌رو، توسل به اصل صلاحیت سرزمینی، کاربرد چندانی در رسیدگی به جرائم سایبری ندارد. بر این اساس، توجه به ضابطه تابعیت یا همان صلاحیت شخصی منفعل که مبنا را بر تابعیت بزه‌دیده قرار می‌دهد، مورد توجه اندیشمندان قرار گرفته است. در این راستا، گروهی از اندیشمندان با تفسیرهای مناسب از برخی قوانین و مقررات، مانند ماده ۸ قانون مجازات اسلامی و ماده ۶۶۴ قانون آیین دادرسی کیفری که در بندهای «پ» و «ت» به صلاحیت شخصی منفعل در راستای حمایت از بزه‌دیده پرداخته، توجه کرده‌اند و گروهی دیگر، درصدد طرح‌ریزی نظریه‌های جدیدی ازجمله «فضای سایبر به‌عنوان یک فضای آزاد بین‌المللی» و یا پیش‌بینی دادگاهی ویژه به نام «دادگاه دیجیتالی یا سایبری» و یا صلاحیت «دادگاه ذی‌ارتباط منطقی با جرم» هستند. اگرچه مورد اخیر، تا حدودی آرمان‌گرایانه به نظر می‌رسد؛ توجه و بازخوانی رویکرد صلاحیت شخصی منفعل را می‌توان در حال حاضر قابل‌اتکاء و منطبق با موازین حقوق بشری دانست. در قوانین کیفری ما اصل صلاحیت مبتنی‌بر تابعیت بزه‌دیده،[1] هم در آیین دادرسی جرائم الکترونیکی و هم در قانون مجازات اسلامی مورد اشاره قرار گرفته است. حال اِعمال این اصل در جرائم سایبری تحت ضوابط بعضاً کمتر مطالعه شده‌ای به‌جهات کمتر شناسایی شدن آنها و نوظهور بودن آن است. در قانون دادرسی جرائم الکترونیکی، هم به جنبهٔ سرزمینی بودن و هم به جنبهٔ حمایتی و مثبت و منفی اصل صلاحیت شخصی توجه شده است. اما به‌جهت دردسرساز بودن جرائم سایبری در صورتی‌که محل وقوع جرم هم کشف نشود، این امر

1. Passive Personality Principle

مانع از رسیدگی نیست و کیفرخواست و رسیدگی در محاکم صالح ایرانی نیز صورت می‌گیرد.[۱] نخست اینکه، باید مشخص شود که اِعمال صلاحیت منفعل در نظام حقوقی ایران تا چه میزان قابلیت اجرایی دارد و در جرائم سایبری چگونه است. دوم اینکه، قواعد بین‌المللی اعمال صلاحیت تا چه حد در روند رسیدگی به جرائم سایبری مؤثر بوده است و در چه مواردی می‌توان از اصول حقوق جزای بین‌المللی در این زمینه استفاده کرد. این پژوهش درصدد پاسخ به این سؤال است که نظام دادرسی ایران چگونه می‌تواند چالش‌های امنیت سایبری را رفع نماید؟ بر این اساس، هدف پژوهش حاضر بررسی تعارض صلاحیت منفعل با سایر صلاحیت‌ها در آیین رسیدگی به جرائم سایبری است.

۲. مبانی مفهومی و نظری

با توجه به نقش محوری مفاهیم، ضروری است ابتدا مبانی مفهومی و نظری پژوهش تبیین گردد:

۲-۱. مفهوم امنیت سایبری

قبل از تبیین مفهوم امنیت سایبری، لازم است مفهوم فضای سایبری مشخص شود. فضای سایبری ریشه در سایبرنتیک و سایبرنتیک به‌عنوان یک حوزه علمی است که بعد از جنگ جهانی دوم در ایالات متحده آمریکا مطرح بود و به نظام‌های اجتماعی حاصل از تعامل کاربران در بستر شبکه گفته می‌شود (Umpleby, 2005: p. 56). در مفهوم سنتی، امنیت در عدم خطرات فیزیکی و تهاجم فیزیکی تعریف می‌شد؛ اما در معنای امروزی، امنیت معنای وسیع‌تری پیدا کرده است. در دوران پسامدرن با پیچیده شدن روابط و شبکه‌های اجتماعی، اهمیت امنیت فضای سایبری افزایش یافته است. این خود ضرروت تبیین مدیریتی جامع برای تهدیدات امنیتی در فضای مجازی را بیشتر کرده است. با توجه به اینکه فضای مجازی یک فضای پویا و فعال و دارای ویژگی‌های خاص خود است، حفاظت از اطلاعات این فضا پیوستگی و پیچیدگی‌های خاص خود را دارد و دائم باید به‌روز و رو به پیشرفت باشد (برقعی، ۱۳۹۳: ص۸۶).

۲-۲. اهمیت امنیت فضای سایبری

در فضای سایبری، کاربران در سطح ملی و بین‌الملل با یکدیگر در ارتباط، تأثیرگذاری و تأثیرپذیری هستند. در فضای سایبری فاصله‌ها از بین رفته و تفکیک سخت شده است. هر کاربر، اهداف و انگیزه‌های مختلفی دارد و مواجهه با آنان سخت و پیچیده شده است. تأمین امنیت سایبری در بخش‌های مختلف دولتی،

---

۱. ر. ک. ماده ۶۶۵ قانون آیین دادرسی کیفری.

نظامی و خصوصی متفاوت است. فضای سایبری ایران در طی سال‌های گذشته هدف حملات سایبری مختلف از سوی افراد، گروه‌ها و دولت‌ها بوده است. ازجمله ویروس استاکس‌نت[1] در سال ۲۰۱۰ در تأسیسات هسته‌ای که می‌توانست پیامدهای مخرّبی برای اقتصاد ایران داشته باشد. با وجود تهدیدات امنیتی که از حملات سایبری ناشی می‌شود، در حقوق بین‌الملل، سازوکارهای لازم برای برخورد با این تهدیدات وجود ندارد. به این جهت است که برای تمام کشورها ازجمله جمهوری اسلامی ایران، تأمین امنیت سایبری از طریق شناخت نوع حملات سایبری، ویژگی‌ها و راهبردهای مقابله با آنها اهمیت زیادی پیدا می‌کند؛ تا علاوه‌بر تدوین قوانین لازم به مقابله با این حملات بپردازد (فیروزآبادی و آزادی احمدآبادی، ۱۳۹۹: ص۵۶۷).

۳. مفهوم و جایگاه صلاحیت منفعل در جرائم سایبری

روند حمایت از افراد بزه‌دیده، دربرگیرندهٔ پرداختن به آسیب و خسارت‌های وارد شده به‌واسطهٔ بزه مذکور و اصلاح موقعیت پدید آمده است. در نتیجه، چهارچوب عمده پرداختن به روند حمایت از فرد بزه‌دیده مربوط به اجبار فرد بزهکار برای اصلاح و جبران آن خسارتی است که به فرد بزه‌دیده وارد آورده است. بنابراین، می‌توان مبنای محکمی را برای برقراری تعهد در راستای پرداخت غرامت در راستای نقض‌های حقوق بین‌الملل در نظر گرفت. در واقع، از نظر حقوق بین‌الملل «هر دولتی که خسارتی را به طرف دیگر وارد کرده، باید به تمام آثار ناشی از نقض مقررات و قواعد حقوقی پایان دهد» (Gastorn, 2017: p. 13). بنابراین، عده‌ای خواسته‌اند تا مبانی بین‌المللی جبران خسارت و لزوم جبران ضرر زیان‌دیده را به قواعد کیفری بین‌المللی در این زمینه پیوند بزنند. از این‌رو، جستار در قواعد صلاحیت مبتنی‌بر حمایت از بزه‌دیده جرائم سایبری، در موضع بین‌رشته‌ای حقوق بین‌الملل و حقوق کیفری قابل پیگیری است. همچنین، قابل ذکر است که اسناد راجع‌به صلاحیت رسیدگی به جرائم سایبری در دو زمینهٔ بین‌المللی و منطقه‌ای قابل بررسی است. جرائم سایبری به جهات مختلف مانند مشخص‌نبودن مکان ارتکاب جرم، مجهول بودن مجرم و محل اقامت او و دیگر ابهامات مختص این فضا، از جهت مرجع صالح به رسیدگی، دارای ابهامات فراوانی است و تأمین امنیت در فضای سایبری را با چالش جدی مواجه می‌کند. رسیدگی به جرائم سایبری به‌طور کلی و توسعه صلاحیت مراجع قضایی به این جرائم به‌طور خاص، ازجمله مسائل مهمی است که در پهنه نظام‌های دادرسی کیفری قابل طرح است (حاجی ده‌آبادی و سلیمی، ۱۳۵۹: ص۷۷). لازم است تمامی جنبه‌های اصل

1. Stuxnet

صلاحیت شخصی منفعل، از قبیل ارتباط آن با سایر انواع صلاحیت‌ها در جرائم سایبر و جایگاه آن در اسناد بین‌المللی و همچنین مبانی آن شناخته شود تا بتوان نقایص آن را برطرف نمود. به نظر می‌رسد که اعمال صلاحیت شخصی منفعل در گیرودار تعارض صلاحیت‌ها در جرائم سایبر، دارای جایگاه مطمئنی نباشد؛ چراکه اولاً این نوع صلاحیت خود نوعی استثناء است و شرایط اعمال آن چندان متقن نیست و از سوی دیگر، ویژگی‌های خاص جرائم سایبری هم مزید بر علت شده که اصل صلاحیت منفعل را نتوان بدون مانع جدی به اجرا گذاشت.

٤. ارتباط صلاحیت منفعل در جرائم سایبری با سایر انواع صلاحیت‌ها

تحولات فوق‌العاده سریع کمّی و کیفی در عرصهٔ دنیای سایبر موجب شده است که نه‌تنها حقوق ماهوی این بخش تا حدود زیادی از همراهی ناکام بماند؛ بلکه قواعد شکلی و حتی اصول کلی حقوقی نیز از تفسیر این تحولات ناتوان بوده‌اند. هیچ عمل مجرمانه‌ای در غیر فضای سایبر نیست که بتواند فاصله‌ها را نادیده بگیرد و مرزهای صلاحیتی را این‌گونه درنوردد؛ بنابراین، باید صلاحیت‌های مختلف در حقوق شکلی سنتی به‌گونه‌ای به‌روز شوند و از سوی دیگر، معیارهای صلاحیتی جدیدی نیز مطرح شود. در ادامه این‌گونه از اصول صلاحیتی در ارتباط با صلاحیت منفعل بررسی شده و نشان داده خواهد شد که جایگاهمان کجاست و بحث از شرایط و مبانی آن بر چه اساسی منطقی است. صلاحیت واقعی و صلاحیت شخصی منفعل در فضای سایبر دقیقاً برمبنای اصول حمایتی و حفاظتی واقع می‌شود. به عبارت دیگر، اگر بزه‌دیدهٔ جرائم سایبری، دولت یا حکومت باشد؛ اعمال صلاحیت، واقعی و اگر بزه‌دیده یا مجنی‌علیه، شخص حقیقی یا حقوقی باشد، می‌تواند تحت عنوان صلاحیت شخصی منفعل مطرح شود. بنابراین، تفاوت این دو در نوع مجنی‌علیه آنان است و از جهت آثار و مبانی کاملاً مشترک هستند. همچنین صلاحیت واقعی معمولاً در جرائم امنیتی اعمال می‌شود که در فضای سایبر به وفور می‌توان مصادیق آن را سراغ گرفت (مرادی حقگو و همکاران، ۱۳۸۲: ص۸۸). جرائم سایبر به دلیل عدم محدودیت در سرزمین مشخص، لزوماً نمی‌توانند از اصل صلاحیت سرزمینی به‌تنهایی بهره گیرند. صلاحیت شخصی به دو نوع فعال و منفعل تقسیم می‌شود. در نوع فعال، ملیت بزهکار یا مرتکب جرم، اساس تعیین دادگاه صالح قلمداد می‌شود. صلاحیت شخصی فعال نیز در گروه صلاحیت فراسرزمین قرار می‌گیرد و از جهت مبانی و شرایط، شباهت بسیار به صلاحیت منفعل دارد. در جرائم سایبر، بسیار طبیعی است که مرتکب و مجنی‌علیه ممکن است ملیت‌های مختلفی داشته باشند و چون ملیت مرتکب در بیشتر موارد ناشناخته است؛ بنابراین، باید به صلاحیت منفعل اقبال بیشتری نشان داد.

در جرائم سایبری، اِعمال صلاحیت فراسرزمینی توسط نویسندگان حقوقی مقبول افتاده است. به‌عنوان مثال، در ارتباط با مطلق یا مقیّد بودن جرائم سایبری بحث‌هایی شده است. در عین‌حال، بعضی از افراد بر این باور هستند که عمدهٔ آنها اثرات نامناسب خود را نه‌تنها در یک نقطه، بلکه در بی‌شمار نقطه در کل جهان باقی می‌گذارند و چنین نقاطی از زوایای متعددی باید مورد تجزیه‌وتحلیل و بررسی قرار گیرند. باید در این راستا به رابطهٔ منطقی و معنادار بین محل‌های حادث شدن اثر سوء و حوضهٔ قضایی مربوطه، اشاره خاصی داشت. به‌طور عمده این نقاط، به‌عنوان مکان‌هایی برای پایه کردن محتویات شبکه سایبری در نظر گرفته می‌شوند که براساس دیدگاه برخی افراد، همان نقاط بروز جرائم سایبری به‌شمار می‌روند. درنتیجه، این موضوع اهمیت دارد که این نقاط را به‌عنوان نقاطی در نظر گرفته شوند که در آنها جرائم سایبری روی می‌دهند و حوزهٔ قضایی آن نقطهٔ مدنظر نظر، نهاد صالح به‌منظور رسیدگی به آن جرائم است.

در حال حاضر در فضای سایبری، مجرمان به‌طور کامل آزاد و رها بوده و از آزادی عمل عجیبی برخوردار هستند. دلیل این امر هم می‌تواند این موضوع باشد که هیچ نهاد قدرتمندی وجود ندارد که نیرو و ابزار مناسبی برای مقابله با چنین جرائمی را به‌طور کامل داشته باشد. در دنیای نوین می‌توان شاهد پدید آمدن موقعیت‌هایی بود که در بستر آنها، افراد بدون هیچ کنترل و نظارتی می‌توانند در حریم خلوت خود از رایانه استفاده کنند و به‌آسانی هرچه تمام‌تر وارد محیطی بدون کنترل شوند که در چنین محیطی هیچ اثری از عوامل دولتی و آن جامعه‌ای نیست که آزادی را محدود نماید (عالی‌پور، ۱۳۸۳: ص۹۹). همین امر، لزوم توجه به زیان‌دیدگان را در این فضا بیشتر نمایان می‌سازد. در صورتی‌که بخواهیم بر صلاحیت شخصی فعال متمرکز شویم، شاید بیشتر جرائم سایبری، قابلیت شناسایی مرتکب را نداشته باشد یا امکان دسترسی به آن وجود نداشته باشد. رویکرد دیگری در اعمال صلاحیت در فضای سایبری وجود دارد که به رویکرد ارتباط حداقلی[1] یا ارتباط منطقی[2] معروف است؛ که در آن معمولاً باید رفتارهای مختلف در نظر گرفته شود و بررسی شود که کدام حوزه قضایی حداقل ارتباط لازم جهت رسیدگی به اختلاف را دارد. در این صورت، یک رفتار منفرد و یا یک معامله، چنین رابطه‌ای را مشخص می‌سازد (Hakmeh, 2017: p. 100). مطابق با این رویکرد در جرائم فضای سایبر می‌توان عناصر مرتبط زیادی ازجمله تابعیت مرتکب و زیان‌دیده از جرم، محل وقوع جرم، محل کامپیوتر و امثال آن را پیدا کرد؛ ولی به نظر می‌رسد که باید عنصری که بیشترین ارتباط را دارد و یا حداقل عنصری که ارتباط منطقی دارد را برگزید. اصل صلاحیت جهانی به هریك از کشورها اجازه تعقیب مجرمینی

1. Minimum Contacts
2. Reasonable Contact

را می‌دهد که نه در قلمرو حاکمیت آنها مرتکب جرم شده‌اند، نه به منافع حیاتی و اساسی آنها تجاوز کرده‌اند، نه از اتباع آنها هستند و نه علیه اتباع آنها مرتکب جرم شده‌اند؛ تنها معیار مطرح برای اعمال صلاحیت در این مورد، محل دستگیری مجرم است (میرمحمد صادقی، ۱۳۹۲: ص۶۱-۷۶). با توجه به اینکه جرائم سایبری داخل در صلاحیت جهانی مشخص نیست و مورد توافق قرار نگرفته است، باید اولویت را با صلاحیت‌های دیگر ازجمله صلاحیت منفعل دانست. تاکنون در فضای سایبر نسبت به برخی جرائم نظیر هرزه‌نگاری کودکان، این اجماع و توافق به‌طور نسبی محقق شده؛ ولی هنوز قدرت اجرایی چندانی پیدا نکرده است. همچنین جرم نفوذ غیر که مادرِ جرائم سایبری محسوب می‌شود، به‌عنوان یک جرم موضوع صلاحیت جهانی مورد توجه قرار گرفته؛ ولی هنوز به‌عنوان یک جرم جهانی محض پذیرفته نشده است (شکفته گوهری، ۱۳۶۰: ص۵۴). صلاحیت نمایندگی می‌تواند به‌عنوان مبنایی برای اعمال صلاحیت شخصی منفعل در جرائم سایبری در نظر گرفته شود. به‌عبارت دیگر، همان‌گونه که اعطای نمایندگی برای اعمال صلاحیت کیفری امکان‌پذیر است، این اعطا می‌تواند براساس تابعیت مجنی‌علیه باشد؛ یعنی کشور متبوع مجنی‌علیه به کشور مقیم مجنی‌علیه نمایندگی اعطا نماید و یا اینکه کشور متبوع مجنی‌علیه نه براساس صلاحیت شخصی منفعل، بلکه براساس صلاحیت نمایندگی، اقدام به محاکمه نماید، که به‌هرحال نتیجه‌ای مشترک خواهد داشت. از این نوع صلاحیت می‌توان تحت عنوان همکاری بین‌المللی نیز یاد کرد.

۵. رویه قضایی در اعمال صلاحیت منفعل در جرائم سایبری

«تهدیدهای سایبری به‌علت برخورداری از ویژگی‌هایی چون قیمت پایین ورود، گمنامی و تأثیرگذاری شگرف، پدیده‌ای به نام انتشار قدرت را به‌وجود آورده که نه‌تنها باعث شده دولت‌های کوچک از ظرفیت بیشتری برای اعمال قدرت در این فضا برخوردار شوند؛ بلکه منجربه ورود بازیگران جدیدی همچون شرکت‌ها، گروه‌های سازمان‌یافته و افراد به معادلات قدرت جهانی شده است. بنابراین، این پدیده امنیت ملی را از ابعاد مفهوم امنیت، دولت‌محوری در امنیت، بعد جغرافیایی تهدید، گستردگی آسیب‌پذیری‌ها، شیوه مقابله با تهدیدها و تعدد بازیگران در این عرصه تحت‌تأثیر قرار داده است» (خلیلی پوررکن آبادی و نورعلی وند، ۱۳۹۱: ص۱۶۷). در این قسمت پژوهش، ابتدا به رویهٔ قضائی ایران در این رابطه خواهیم پرداخت و در ادامه به رویهٔ قضایی بین‌المللی و برخی از کشورها اشاره خواهیم کرد. پس از قانون مجازات ۱۳۹۲ مطابق با نظریاتی ذیل دیدگاه محاکم ایرانی، عمدتاً بر نفی صلاحیت منفعل تأکید داشتند. به همین خاطر، اداره حقوقی وزارت دادگستری تحت نظریه شماره ۷/۲۱۹۴ مورخ ۱۳۷۴/۵/۱ براساس مقررات آیین دادرسی

کیفری بیان داشته است که: «چنانچه جرم خارج از ایران اتفاق افتاده باشد، ولی از موارد منعکس در مواد ۵ الی ۸ قانون مجازات اسلامی مصوب ۱۳۷۰ نباشد؛ هرچند مجنی‌علیه ایرانی باشد، محاکم قضائی صالح به رسیدگی نیستند». دو: پیش از تصویب قانون مجازات ۱۳۹۲ اداره حقوقی قوه قضائیه در پاسخ به استعلامی در خصوص جرائم ارتکابی علیه اتباع ایرانی طی نظریهٔ مشورتی شماره ۷/۳۸۱۸ مورخ ۱۳۸۷/۶/۲۰ بیان کرده است: «نظر به اینکه محل به دریا انداختن مسافران ایرانی در خارج از قلمرو حاکمیت ایران بوده؛ به فرض وقوع بزه نیز مراجع قضائی ایران صالح به رسیدگی نمی‌باشند و چون مجرمین احتمالی نیز دارای تابعیت ایرانی نیستند، در صورت حضور در ایران نیز قابل‌تعقیب کیفری نیستند». کشورهای مختلف دنیا از جهت برخورد با اصل صلاحیت شخصی منفعل به دو دسته تقسیم می‌شوند. کشورهایی که این اصل را پذیرفته‌اند: فرانسه، آلمان، ایتالیا، یونان، ترکیه، مکزیك و سوئیس (Oleman, 2003: p. 129-141) و کشورهایی که اصل مذکور را نپذیرفته و مخالفت جدی با آن دارند: مانند امریکا و انگلستان، به‌عنوان نمایندگان نظام حقوقی کامن‌لا هستند. البته برخی از کشورها مانند آمریکا این موضوع را در جرائم تروریستی به اجرا می‌گذارند که اعمال تروریست سایبری از این دسته است (Shaw, 2008: p. 406). اصل صلاحیت مبتنی‌بر تابعیت مجنی‌علیه در قوانین جزائی آمریکا به‌شدت مورد مخالفت قرار می‌گرفت؛ ولی از سال ۱۹۷۰ برای اقدامات تروریستی تا حدودی پذیرفته شد (Watson, 1993: p. 3). در خصوص مخالفت آمریکا با اصل صلاحیت منفعل گفته شده که «نارضایتی ایالات متحده از اصل صلاحیت مبتنی‌بر تابعیت مجنی‌علیه، آنچنان قوی بوده که حتی حاضر نبوده است آن را در قالب حرکت‌های استعماری خود به اجرا گذارد» (Watson, 1993: p. 4-5).

با الحاق آمریکا به کنوانسیون‌های ضد تروریستی، اصل صلاحیت شخصی منفعل وارد نظام حقوقی این کشور شد. قوانینی متعاقب این کنوانسیون‌ها توسط ایالات متحده به تصویب رسیده‌اند که آن دسته از افرادی که جرائمی علیه مأموران و دیپلمات‌های آمریکائی در خارج انجام می‌دهند را قابل مجازات می‌داند (Watson, 1993: p. 9). البته نباید فراموش کرد که این‌گونه توجه به اصل صلاحیتی مذکور عموماً ناشی از این رویکرد است که اعمال اصل صلاحیت سرزمینی به دلایلی مانند فراملی بودنِ جرائم امکان‌پذیر نیست. شرایط بارز اعمال اصل صلاحیت شخصی منفعل در رویهٔ کشورهای مختلف نیز متّکی به چند شرط است که عبارتند از: اعمال در جرائم با اهمیت مانند آنچه در حقوق آمریکا دیده شد؛ عدم رسیدگی کشور محل وقوع جرم و امکان دستگیری یا استرداد مجرم که بیانگر مفید واقع شدن رسیدگی است (خالقی، ۱۳۸۳: ص۶۵).

٦. تعارض صلاحیت‌ها

در چهارچوب حقوق کیفری ایران به‌واسطه تصویب قانون سال ۱۳۹۲، می‌توان شاهد آن بود که در راستای هم‌سویی اصل صلاحیت شخصی با اصول مقبول در بطن حقوق جزای بین‌المللی، کارهای بسیار ارزشمندی انجام گرفته است.[1] در این راستا می‌توان تحولاتی مانند قبول منع محاکمهٔ مجدد و صلاحیت همسو با تابعیت مجنی‌علیه را مدنظر قرار داد (شریعت باقری، ۱۳۹۲: ص۳۹). همچنین می‌توان به تبعیت بند «ت» ماده ۶۶۴ از دستورالعمل اتحادیه اروپا در ماده ۱۷ آن اشاره کرد. همچنین باید دانست که در حقوق جزای بین‌الملل، اصل صلاحیت شخصی موجب نادیده گرفتن حاکمیت کشورها نیست؛ بلکه به‌نحوی است که براساس چنین اصول پذیرفته‌شده‌ای، دولت‌ها این حق را برای خود قائل هستند که در آن زمان که علیه فرد تبعهٔ آنها یا به‌واسطه افراد تبعهٔ آنها، یا در عین زمان علیه منافع حیاتی و اساسی آنها و یا علیه نظم بین‌المللی، جرمی حادث شد؛ در صورتی که دستگیری فردی که جرم مرتکب شده ممکن باشد، بتوانند به آن جرم مرتکب‌شده رسیدگی کنند و در عین‌حال نگذارند که مجرمینی که براساس اصل صلاحیت سرزمینی قابل مجازات نیستند، بدون مجازات بمانند و نتیجهٔ کارهای خود را ببینند (فرجی‌ها و آقائی، ۱۳۹۱: ص۱۵). هنگامی‌که در آیین دادرسی رسیدگی به جرائم سایبری در مبحث صلاحیت دادگاه‌ها در خصوص صلاحیت منفعل و تابعیت شخص بزه‌دیده بحث می‌گردد، با موضوع چالشی تعارض صلاحیت مواجه هستیم. هر زمان که شاهد ایجاد صلاحیت قضایی بیش از یک حوزهٔ قضایی یا صلاحیت قضایی کشورهای متعددی در رابطه با بررسی و رسیدگی به جرائم بودیم، تعارض موجود، تعارض سنتی و تبعیت‌کننده از قواعد آیین دادرسی رسیدگی به تعارضات جهان سنتی خواهد بود؛ با این توضیح که در جرائم سنتی، نسبتاً کلیه جوانب جرائم محدود و مشخص است و با بهره‌گیری از قانون و رویه و روش‌های مرسوم سنتی تا حد قابل‌توجهی موضوع تعارض قابل‌حل خواهد بود. اما با توجه به دامنه و وسعت جرائم سایبری به‌لحاظ ویژگی خاص آن یعنی فرامکانی و فرازمانی بودن جرائم و مجهول‌الهویه بودن مرتکب و امکان ورود خسارت‌های غیرقابل‌تصور همچون تروریسم سایبری که اهداف عمومی یک دولت را نشانه می‌گیرد، دیگر به‌راحتی نمی‌توان اختلاف صلاحیت خصوصاً اختلاف صلاحیت بین دولت‌ها را با قوانین و رویه‌ها و رویکردهای سنتی برطرف نمود (زررخ و همکاران، ۱۳۷۳: ص۳۲). در راستای یک چشم‌انداز جامع در رابطه با جرائم سایبری، این امر الزامی است که قانون‌گذار، ذهنی خارج از محیط فیزیکی و واقعی داشته و وارد دنیای کاملاً مجازی گردد. در

1. EU Directive on Child Exploitation, Article17 (2)

عین‌حال، طبیعت غیرواقعی جرائم سایبری باعث شده که دیگر مرزهای جداکننده کشورها معنا و مفهوم خود را از دست بدهند و مفاهیمی مانند «صلاحیت غیرمبتنی بر مرز» یا «صلاحیت فرامرزی» جای صلاحیت‌های تبعیت‌کننده از مرزبندهای جغرافیایی طبیعی و سیاسی را بگیرند. دلیل این امر را نیز می‌توان به این صورت شرح داد که ماهیت جرائم سایبری، ماهیتی خارج از مرزها بوده و باید محل ارتکاب جرم و سایر موارد مربوط به آن را ورای مکان و موقعیت فیزیکی ارتکاب جرم در نظر گرفت (دزیانی، ۱۳۸۵: ص۵۳). در نتیجه، در مبحث تعارض صلاحیت در جرائم سایبری به‌ناچار با تعارض قوانین و ایده‌ها و رَویه‌هایی مواجه هستیم که در جرائم سنتی قابل درک و اجرایی بوده؛ اما در جرائم سایبری، کاربری مفید و چندانی ندارد. اصل صلاحیت منفعل که برمبنای حفاظت از منافع اتباع دولت‌ها است، گویای این مطلب است که جامعه جهانی و خصوصاً دولت‌ها می‌بایست در اجرای اصول صلاحیت کیفری مذکور، راه اعتدال را در پیش بگیرند تا بدین طریق، از تعارض صلاحیتی جلوگیری گردد (اسلامی، ۱۳۸۰: ص۱۷۶). در خصوص تعارض صلاحیت در قانون دادرسی داخلی ایران می‌بایست وفق قانون آیین دادرسی مدنی عمل کرد؛ ولی برای رفع مشکل تعارضات صلاحیت و سهولت امر تحقیقات و رسیدگی می‌بایست با تصویب قانون در جهت پیش‌بینی تعارض صلاحیت‌های جرائم سایبری اقدام نمود. در انتها این نکته قابل ذکر است که جهت تعیین دادگاه صالح، تنها پیشنهادی که توان برداشتن چالش‌های تعارض صلاحیت را خواهد داشت، عبور از قواعد و قوانین رسیدگی کیفری سنتی به‌لحاظ موقعیت بزه‌دیده است (کتانچی و پورقهرمانی، ۱۳۷۰: ص۴۷). لذا، با پذیرش پیشنهاد موصوف چنانچه بزه‌دیدهٔ جرائم سایبر به دادگاه‌های کیفری محل زندگی و اقامت خود مراجعه و تقاضای رسیدگی کند دادگاه صالح به‌لحاظ تابعیت و محل اقامت بزه‌دیده می‌بایست در راستای رسیدگی، خود را به‌عنوان نهاد صالح بشناسد و روند رسیدگی و تحقیقات را با پذیرش شکایت، آغاز کند.

۷. راهکارهای تقویت امنیت سایبری

برای تقویت امنیت سایبری، راهکارهای زیادی مطرح شده است. در این قسمت پژوهش به مهم‌ترین راهکارها اشاره‌ای مختصر می‌گردد:

۷-۱. همکاری دولت‌ها در سطح بین‌الملل: دولت‌ها به‌علت افزایش استفاده از کامپیوتر و فناوری‌های اطلاعات، افزایش قدرت‌های سایبری در جهان، افزایش فزایندهٔ حملات سایبری در جهان و همچنین عدم قوانین روشن و شفاف برای این حوزه، لازم و ضروری است که با یکدیگر همکاری داشته باشند. «دنیای سایبری، بستر مشترک منافع و تهدیدهای جامعهٔ ملل امروز است و دولت‌ها را وارد کرده تا علی‌رغم افتراق‌ها و

اختلاف‌های دنیای فیزیکی به یکپارچگی روی آورند و از این نگاه، معاهده‌های فراملی سایبری نقش تعیین‌کننده‌ای را ایفا می‌کنند» (فقیهی و جلالی فراهانی، ۱۳۹۷: ص۱).

۷-۲. تغییرات راهبردی در معنا و مفهوم امنیت: در گذشته، امنیت مفهومی ملی و در محدودهٔ مرزها تعریف می‌شد. اما با وجود اینترنت و فناوری‌های فضای مجازی، مفهوم امنیت و امنیت ملی به یک مفهوم امنیت جهانی و بین‌الملل تغییر یافته است؛ زیرا تهدیدات جدید و فرامرزی به‌دنبال دارد. «فناوری اطلاعات و ارتباطات به‌عنوان متغیری جدید مطرح است که در قالب نظریات سایبر پلتیک و مبتنی‌بر مفهوم ارتباطات فراتر از آنچه پیش از این مطرح می‌شد، ابعاد و تعابیر مختلف امنیت نظامی، اقتصادی، سیاسی، اجتماعی، فرهنگی و زیست‌محیطی را تحت‌تأثیر قرار داده است» (سلطانی‌نژاد و همکاران، ۱۳۹۵: ص۸).

۸. نتیجه‌گیری

در مورد صلاحیت رسیدگی به جرائم سایبری در وهله اول با توجه به آنچه از مبانی و ضابطه‌های مورد رسیدگی ذکر شد، چندوجهی بودن سیاست مقنن در عرصهٔ بین‌المللی و حقوق داخلی مشخص می‌گردد؛ اما ابتدایی‌ترین و اصولی‌ترین سیاست در تقابل با جرائم سایبری، رویکرد ویژه به مهم‌ترین عنصر تعیین‌کننده در اعمال صلاحیت دولت‌ها یعنی همان حاکمیت دولت یا اصل سرزمینی بودن قوانین کیفری است. دولت‌ها براساس دستورالعملی که اتحادیه اروپا ارائه داده است و همچنین برخی از اسناد مربوطه در رابطه با استثمار کودکان، ملزم خواهند بود تا در راستای آن جرمی که بیرون از حیطهٔ قلمرو علیه افراد تبعهٔ خود یا افراد دیگری که به‌صورت عادی در کشور آنها سکونت دارند، صورت گرفته است، صلاحیت خود را اعمال کنند. مقرره‌ای در رابطه با اصل صلاحیت شخصی در دادگاه‌های ایران به‌چشم نمی‌خورد؛ ولی با توجه به ماده ۲۸ قانون جرائم رایانه‌ای که صلاحیت پیش‌بینی‌شدهٔ قوانین دیگر را می‌پذیرد (قانون مجازات اسلامی مصوب ۱۳۹۲)، برای اینکه آن دسته از مواردی که دادگاه‌های ایران براساس اصل صلاحیت شخصی، می‌توانند به جرائم سایبری رسیدگی کنند مشخص شوند، مقررات کلی در این راستا باید مدنظر قرار گیرند. قابل ذکر است که اسناد راجع‌به صلاحیت رسیدگی به جرائم سایبری در دو زمینه بین‌المللی و منطقه‌ای قابل بررسی است. کنوانسیون بین‌المللی جرائم سایبری که در سال ۲۰۰۹ به امضای ۴۲ کشور رسیده است، به‌صورت یک اهرم بسیار مهم بین‌المللی شناخته می‌شود که به‌واسطه آن می‌توان با جرائم سایبری مقابله نمود و سازمان‌های بین‌المللی مختلفی، حمایت خود را از آن اعلام می‌کنند؛ در عین‌حال، باید به این حقیقت تلخ اشاره داشت که در این کنوانسیون، هیچ‌گونه سازوکاری برای حمایت از آن دسته از افرادی که از جرائم سایبری

آسیب‌دیده‌اند وجود ندارد. به همین دلیل، به‌جز کنوانسیون بوداپست، اسنادی که در بالا به آنها اشاره شد، صراحت خاصی در رابطه با حمایت از آن دسته افرادی که تحت جرائم سایبری قرار گرفته‌اند، ندارند. ماهیت ویژه همین جرائم سایبری سبب شده تا در مورد آنها بیشتر به ملاک صلاحیت مبتنی‌بر تابعیت در میان کشورها توجه شود. کمااینکه کشور هلند در جرم سایبری مهم یعنی سابوتاژ کامپیوتری[1] و تخریب داده‌ها[2] در جایی که تبعهٔ خود، بزه‌دیده واقع شده است؛ خود را صالح به رسیدگی شناخته است. ایالات متحده آمریکا این قاعده را در جایی قابل اجرا دانسته است که دولت آمریکا بزه‌دیده واقع شده باشد. به‌واسطه تصویب قانون سال ۱۳۹۲ پیرامون حقوق کیفری ایران، هم‌سویی اصل صلاحیت شخصی با اصول مقبول در بستر حقوق جزا در سطح بین‌المللی، می‌توان شاهد پیشرفت‌های خوبی بود.[3] در این حالت، پذیرش عدم محاکمهٔ مجدّد و صلاحیت مبنی‌بر تابعیت فرد آسیب‌دیده باید مدنظر قرار گیرد. در همین راستا می‌توان به تبعیت بند «ت» ماده ۶۶۴ از دستورالعمل اتحادیه اروپا در ماده ۱۷ آن اشاره نمود. در عین‌حال باید به این موضوع نیز توجه داشت که در بستر حقوق جزای بین‌الملل، اصل صلاحیت شخصی موجب نادیده گرفتن حاکمیت کشورها نیست. در قوانین کیفری ما اصل صلاحیت مبتنی‌بر تابعیت بزه‌دیده، هم در آیین دادرسی جرائم الکترونیکی و هم در قانون مجازات اسلامی مورد اشاره قرار گرفته است. حال اعمال این اصل در جرائم سایبری تحت ضوابط بعضاً کمتر مطالعه‌شده‌ای به جهات کمتر شناسایی شدن آنها و نوظهور بودن آن است. قانون دادرسی جرائم الکترونیکی، هم به جنبه سرزمینی بودن و هم به جنبه حمایتی و مثبت و منفی اصل صلاحیت شخصی توجه نموده است. اما به‌جهت دردسرساز بودن جرائم سایبری، در صورتی‌که محل وقوع جرم هم کشف نشود؛ این امر مانع از رسیدگی نیست و کیفرخواست و رسیدگی در محاکم صالح ایرانی نیز صورت می‌گیرد. همچنین است شناسایی این صلاحیت در قانون مجازات اسلامی در ماده ۸ نسبت به غالب جرائم و مطلق حدود و قصاص و دیات و تعزیرات منصوص شرعی که می‌توان آنها را جرائم سنتی نامید.

1. Computer Sabotage
2. Data Damage
3. EU Directive on Child Exploitation, Article17 (2)

منـابـع

اسلامی، ابراهیم (۱۳۸۰). جایگاه حمایت از بزه‌دیدگان جرایم سایبری در مقررات کیفری حقوق داخلی و حقوق بین‌الملل. *پژوهشنامه حقوق اسلامی*، شماره ۹.

برقعی، حسن (۱۳۹۳). مروری بر امنیت سایبری؛ درس‌هایی برای جمهوری اسلامی ایران. *مطالعات انقلاب اسلامی*، شماره۳۸.

پوربافرانی، حسن (۱۳۸۸). اصل صلاحیت مبتنی بر تابعیت مجنی علیه در حقوق جزای بین‌الملل و ایران. *مفید*، شماره۳۷.

حاجی ده‌آبادی، احمد؛ سلیمی، احسان (۱۳۵۹). اصول جرم‌انگاری در فضای سایبر با رویکردی انتقادی به قانون جرائم رایانه‌ای. *مجلس و راهبرد*، شماره ۷۱.

حسینی‌نژاد، حسین قلی (۱۳۸۳). *حقوق کیفری بین‌المللی*. تهران: نشر میزان.

خالقی، علی (۱۳۸۳). بلژیک و پایان ده سال رویای صلاحیت جهانی در جرایم بین‌المللی. *پژوهش‌های حقوقی*، شماره۶.

خلیلی پوررکن آبادی، نورعلی وند، یاسر (۱۳۹۱). تهدیدات سایبری و تاثیر آن بر امنیت ملی. *مطالعات راهبردی*، ۱۵(۵۶).

دزیانی، محمدحسن (۱۳۸۵). مقدمه‌ای بر سیاست جنایی جرایم سایبری. *قضاوت*، شماره۴۰.

زررخ، احسان؛ کاظمی، قباد؛ جعفری، محمدجواد (۱۳۷۳). راهبردهای تقنینی ملی و فراملی در مقابله با جرایم سازمان‌یافته سایبری. *جامعه‌شناسی سیاسی ایران*، ۴(۹).

سلطانی‌نژاد، احمد؛ جمشیدی، محمدحسین؛ محسنی، سجاد (۱۳۹۵). تحول مفهوم امنیت در پرتو جهانی شدن و فناوری اطلاعات و ارتباطات نوین. *سیاست جهانی*، ۵(۲).

شریعت باقری، محمدجواد (۱۳۹۲). *حقوق کیفری بین‌المللی*. تهران: نشر جنگل، چاپ چهاردهم.

شکفته گوهری، معصومه (۱۳۶۰). *مبانی، شرایط و آثار اصل صلاحیت شخصی در حقوق کیفری ایران*. پایان‌نامه کارشناسی ارشد. دانشگاه گیلان.

عالی‌پور، حسن (۱۳۸۳). واقعیت جرم. *پژوهش حقوق عمومی*، شماره۱۳.

فرجی‌ها، محمد؛ آقایی، امین (۱۳۹۱). جنبه‌های منفی و مثبت اصل صلاحیت شخصی در حقوق جزای بین‌الملل. *مطالعات بین‌المللی پلیس*، ۲(۹).

فقیهی، مهدی، جلالی فراهانی، امیرحسین (۱۳۹۷). *مروری بر معاهده‌های فراملی سایبری*. معاونت پژوهش‌های زیربنایی و امور تولیدی. تهران: دفتر مطالعات ارتباطات و فناوری‌های نوین.

فیروزآبادی، ابوالحسن؛ آزادی احمدآبادی، جواد (۱۳۹۹). تحلیل پیشینه حکمرانی فضای مجازی جمهوری اسلامی ایران. *دانش سیاسی*، ۱۶(۳۳).

کتانچی، الناز؛ پورقهرمانی، بابک (۱۳۷۰). سیاست‌های نمادین معاهده جرایم سایبری شورای اروپا. *مطالعات بین‌المللی*، ۱۶(۲).

مرادی حقگو، فرهاد؛ شاملو، باقر؛ سایبانی، علیرضا (۱۳۸۲). ارتباط و جایگاه صلاحیت منفعل در جرایم سایبری با سایر انواع صلاحیت‌ها در نظام حقوقی ایران. *کارآگاه*، ۱۹(۲۱).

میر محمدصادقی، حسین (۱۳۸۶). *حقوق جزای بین‌المللی (مجموعه مقالات)*. تهران: نشر میزان، چاپ دوم.

میرمحمدصادقی، حسین (۱۳۹۲). صلاحیت مبتنی بر تابعیت مجنی علیه با تاکید بر قانون جدید مجازات اسلامی. *آموزه‌های حقوق کیفری*، شماره۵.

نجفی توانا، علی (۱۳۹۳). *حقوق جزای عمومی (تحلیلی انتقادی تطبیقی)*، جنگل، ج۱.

Gastorn, K. (2017). *Relevance of international law in combating cybercrimes: current issues and aalco's approach.* Wuzhen Summit.

Hakmeh, J. (2017). *Cybercrime and the Digital Economy in the GCC Countries.* International Security Department, Chatham House.

Oleman, C. (2003). Security Cyberspace - New Laws and Developing Strategies. *Computer Law and Security Report*, 19(2).

Shaw, M. (2008). *International law*. New York: Cambridge University Press, 6ed.

Umpleby, S.A. (2005). A history of the cybernetics movement in the United States. *Journal of the Washington Academy of Sciences*, 91(2).

Watson, G.R. (1993). The passive personality principle. *Texas international law journal*, vol. 28.