شناسه دیجیتال (DOI): 10.22106/JLJ.2017.27617

محدودیت‌ها و راهبردهای صلاحیت در جرایم سایبری

بهزاد رضوی‌فرد*
سید نعمت‌اله موسوی**

چکیده

فضای سایبر به عنوان مجموعه‌ای از ارتباطات انسانی که از طریق رایانه و وسایل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی به آن نگریسته می‌شود، افزون بر فراهم آوردن منافع بسیار، بستری جدید برایِ ارتکاب رفتارهای مجرمانه است. هدف این نوشتار بررسی معیارهای تعیین صلاحیت کیفری در جرایم سایبری است. در واقع از آنجا که جرایم سایبری به طور مادی و در یک فضای فیزیکی مشخص محقّق نمی‌شود، تعیین مرجع قضایی صالح را دشوار می‌کند. در این راستا، به‌منظورِ تعیین معیارهای قابل اعمال در جرایم سایبری، دو دسته از معیارهای ناظر به تعیین صلاحیت مدنظر قرار گرفته است. یکی تعیین صلاحیت در جرایم سایبری با توجه به معیارهای معمول و دیگری تعیین صلاحیت در جرایم سایبری با توجه به ویژگی‌های این دسته از جرایم. برآیند اینکه گرچه با توجه به معیارهای مورد بحث تعیین مرجع قضایی صالح به رسیدگیِ جرایم سایبری به نحوی از انحاء محقّق می‌شود، اما همچنان در مواردی نظیر اینکه متهم در خارج از قلمرو حاکمیتی است یا جرم خارج از قلمرو حاکمیتی است اما بنابر برخی معیارها قابل رسیدگی در مراجع داخلی است، محدودیت‌هایی وجود دارد که برای رفع آن و در نهایت آغاز رسیدگی در مرجع قضایی صالح، به لحاظ راهبردی، می‌بایست همکاری کیفری بین‌المللی به طور جدی مورد امعان‌نظر قرار گیرد.

کلیدواژه‌ها: صلاحیت کیفری، فضای سایبر، جرایم سایبری، همکاری بین‌المللی.

* عضو هیأت علمی دانشکده حقوق دانشگاه علامه طباطبائی (نویسنده مسئول) Razavi1351@yahoo.com
** دانشجوی دکتری حقوق جزا و جرم‌شناسی دانشگاه علامه طباطبائی Snm.1396@yahoo.com
تاریخ دریافت: ۹۴/۰۴/۱۸ تاریخ پذیرش: ۹۴/۱۰/۲۹

مقدمه

فضای سایبر با وجودِ منافع بسیار، بستری را فراهم کرده که امنیت اجتماعی، اقتصادی و حتی امنیت ملی را به خطر می‌اندازد. با تدوین و وضع مقررات معرِّف جرایم و مجازات‌های سایبری، نظام عدالت کیفری هر کشوری در پیِ حفظ امنیت داده‌ها و سیستم‌ها بوده و بدین جهت تأمین امنیت اجتماعی و فرهنگی و اقتصادی و حتی امنیت ملی در برابر رخدادهای غیرعمدی یا حملات عمدی را در نظر دارد. ایجاد و تقویت نظام حقوقی و قضایی متناسب و همگام با توسعهٔ فضای سایبر، به‌ویژه در جهت مقابلهٔ کارآمد با جرایم آن، باید همواره مدنظر بوده و با توجه به رشد بسیار سریع فضای سایبری و تکنولوژی‌های مرتبط با آن، نظام حقوقی ما همگام با آن حرکت کند. از جمله ابعاد و مسائل اساسی و البته راهبردی جرایم سایبری چگونگی تعقیب و رسیدگی آن به لحاظ تعیین مرجع قضایی صالح است. روی‌هم‌رفته، در تعیین مرجع قضایی صالح برای رسیدگی اصولاً محل ارتکاب جرم یا محل کشف جرم و محل دستگیری یا محل اقامت مرتکب معیار است و اگر موضوع جنبه بین‌المللی پیدا کند، معیارهای صلاحیت سرزمینی، تابعیت مرتکب، تابعیت بزه‌دیده، اخلال در نظم و امنیت کشور یا اخلال در نظم و امنیت بین‌المللی مدنظر قرار می‌گیرد. افزون بر آن، با توجه به ویژگی جرایم سایبری معیارهای دیگری را هم می‌توان برای تعیین مرجع قضایی صالح ارائه داد؛ نظیر محل بارگذاری یا محل پیاده‌سازی داده‌ها. در رابطه با جرایم سایبری باید توجه داشت که نظر به امکان ارتکاب این جرایم از هر نقطه مکانی و همچنین نظر به مسائلی نظیر حاکمیت ملی کشورها و عدم مداخله در امور داخلی آنها، در فرضی که جرایم سایبری در کشوری دیگر رخ داده باشد، رسیدگی آن در نظام حقوقی داخلی با چالشی اساسی مواجه است. در واقع، ویژگی برجسته جرایم سایبری امکان ارتکاب آن در فضایی مجازی از هر نقطه مکانی است و از این روست که اصولاً جنبه فراملی پیدا می‌کند.

کشف و تعقیب جرایم سایبری و محاکمه مرتکبان به لحاظ ویژگی پیش‌گفته این جرایم به دلالیل مختلف با موانعی اساسی مواجهه است. نخست اینکه حقوق کیفری اصولاً به امور داخلی کشورها مربوط است و بدین‌سان است که اصولاً کشورها نه می‌توانند تعقیب جرمی را به عهده بگیرند که در سرزمین آنها رخ نداده و نه می‌توانند مرتکبی را مورد تعقیب و رسیدگی قرار دهند که تبعه آنها نیست؛ مگر در مواد استثنایی که البته این هم با محدودیت‌هایی مواجه است. در واقع، اگرچه با پیش‌بینی صلاحیت مبتنی بر تابعیت مرتکب و تابعیت بزه‌دیده و نیز صلاحیت واقعی یا صلاحیت جهانی امکان تعقیب و رسیدگی به جرایمی که خارج از محدوده سرزمینی کشور رخ داده ممکن است، اما توسل به این معیارها به تنهایی کفایت نمی‌کند؛ به ویژه اینکه جرایم سایبری در یک محیط مجازی رخ می‌دهند.

البته برخی از عناصر مربوط جنبه فیزیکی و مادی دارند که در تعیین صلاحیت کیفری هم مورد امعان‌نظر قرار گرفته‌اند. بنابر آنچه گفته شد، دو مسأله اساسی در ارتباط با جرایم سایبری باید روشن شود: نخست آنکه با توجه به ویژگی فضای سایبری و جرایم سایبری، چه معیارهایی برای تعیین مرجع قضایی صالح وجود دارد؟ دوم آنکه معیارهای صلاحیت کیفری سایبری با چه محدودیتی روبرو است و راهکار آن چیست؟

برایِ پاسخ به پرسش‌های پیش‌گفته، در این نوشتار تلاش بر آن است که ضمن اشاره به فضای سایبر و جرایم سایبری (شماره ۱)، صلاحیت کیفری (شماره ۲) و چگونگی امکان تعقیب این جرایم به لحاظ معیارهای گوناگون و نیز به لحاظ مقررات آیین دادرسی کیفری در خصوص دادرسی الکترونیکی مورد شاره قرار گیرد (شماره ۳) و سرانجام با اشاره به محدودیت صلاحیت کیفری سایبری (شماره ۴)، با مطالعه تطبیقی اسناد راهبردی سایبری برخی کشورها (شماره ۵)، راهکار راهبردی چگونگی تعقیب جرایم سایبری هم توضیح و تبیین شود.

۱. فضای سایبری و جرایم سایبری

در یک معنای مختصر فضای سایبری ناظر است به «فضای برخط شبکه‌های رایانه‌ای به ویژه اینترنت»[1] یا «فضایی مجازی و غیرواقعی است که در آن داده‌های الکترونیکی بین رایانه‌ها مبادله می‌شود.»[2] همچنین در تعاریف دیگر فضای سایبر ناظر است به «فضای مجازی که جامعه کاربران اینترنت در آن بوده و منابع داده‌های الکترونیکی به واسطه شبکه‌های رایانه‌ای قابل دسترس هستند»[3] یا «مجموعه‌ای از سامانه‌های به هم پیوسته داده‌ها و کاربران انسانی که با این سامانه‌های در تعامل هستند.»[4] بنابراین می‌توان گفت فضا سایبر فضایی غیرملموس و مجازی و غیرواقعی است که به واسطه اتصال و ارتباط بین رایانه‌ها و ابزارهای اینترنتی و اینترنت ایجاد شده است.[5]

باری، با مداقه در تعاریف پیش‌گفته می‌توان سه عنصر اساسی تشکیل‌دهنده فضای سایبر را چنین گزیده آورد: نخست سامانه‌ای رایانه‌ای؛ دوم شبکه اینترنت؛ و سوم کاربران. آنچه باید بدان توجه داشت آن است که گرچه عنصر اول و سوم در فضای مادی موجود و

1. Merriam-webster, Accessed 14 May 2017, [https://www.merriam-webster.com/dictionary/cyberspace].
2. Oxford dictionaries learner's, Accessed 14 May 2017, [http://www.oxfordlearnersdictionaries.com/definition/english/cyberspace?q=cyberspace].
3. Larousse, Consulté le 14 Mai 2017, [http://www.larousse.fr/dictionnaires/francais/cybermonde/21258].
4. NATO Cooperative Cyber Defence Centre of Excellence, Accessed 17 May 2017, [https://ccdcoe.org/multimedia/cyberspace-definition-and-implications.html].
5. Bussell, Jennifer, (2013), Cyberspace, Encyclopædia Britannica, Accessed 25 June 2017, [https://www.britannica.com/topic/cyberspace].

ملموس است اما عنصر سوم موجودیت مادی و ملموسی ندارد و از این روست که تمام کنش‌های انجام‌یافته در این فضایِ مجازی و غیرملموس بعد مکانی مشخص و معینی ندارد؛ چنان که برخی در تعریف فضای سایبر بدان نکته توجه داشته و چنین تعریفی ارایه داده‌اند که «فضای سایبر به مجموعه‌هایی از ارتباطات درونی انسان‌ها از طریق رایانه و وسایل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می‌شود.»[1] وانگهی، در فضای مجازی جدای از فعالیت‌های گوناگون مفید و مشروع، فعالیت‌هایی که خلاف اخلاق بوده و یا به نحوی از انحا خلاف مصالح اجتماعی بوده و منجر به صدمه و زیان می‌شوند هم ظهور و بروز کرده است. انجام این فعالیت‌های بزهکارانه در محیطی مجازی و بدون بُعد مکانی فیزیکی ، تعقیب و رسیدگی جزایی را با چالشی اساسی مواجه کرده است. از این رو حقوق جزا چه در بُعد ماهوی و چه در بُعد شکلی ناگزیر به تحول است. در واقع، تمامی قواعد و مقررات حقوق کیفری اصولاً ناظر به رفتارهای فیزیکی و ملموس بوده اما موضوع مطروحه فاقد این ویژگی است و افزون بر آن بُعد مکانی هم ندارد. در واقع، می‌توان در یک تقسیم‌بندی کلی جرایم را به جرایم سنتی و جرایم الکترونیکی[2] یا سایبری[3] تقسیم نمود که هر یک از این انواع بنا به ماهیت و ویژگی‌ها و آثار، به فراخور، نیازمندِ سازوکاری ویژه و متناسب برای تعقیب، رسیدگی و محاکمه و اعمال و اجرای کیفر هستند.[4] بنابراین هم به تعریف جرایم مربوط نیاز هست و هم به بازتعریف قواعد ناظر به دادرسی از جمله قواعد مربوط به صلاحیت نیاز هست؛ چنین است که موضوعی تحت عنوان «صلاحیت سایبری»[5] به میان آمده است.[6]

برآیند اینکه با توجه به ارتکاب جرایمی نظیر دسترسی غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای، شنود غیرمجاز محتوای در حال انتقال ارتباطات رایانه‌ای و مخابراتی، جاسوسی رایانه‌ای، تخریب و اخلال در داده‌ها و نیز ارتکاب جرایم سنتی نظیر جرایم علیه عفت و اخلاق عمومی، هتک حیثیت و نشر اکاذیب، سرقت و کلاهبرداری توسط سامانه‌های رایانه‌ای و افزون بر و مهم‌تر از اینها تروریسم سایبری و نیز جنگ سایبری[7] که ممکن است کشورها علیه یکدیگر به منظور اختلال و تخریب سامانه‌ای و تأسیسات یکدیگر انجام دهند[8] و لحاظ امکان لطمه‌های فرهنگی و اقتصادی و حتی تهدید امنیت

۱. زندی، محمدرضا، تحقیقات مقدماتی در جرایم سایبری، تهران، انتشارات جنگل، ۱۳۹۳، ص. ۲۲.

2. E-Crime

3. Cyber Crime

4. Jewkes, Yvonne; and Majid Yar, Hand book of Internet Crime, USA: Willan Publishing, 2010, pp. 42-43.

5. Cyber Jurisdiction

۶. زندی، محمدرضا، منبع پیشین، ص. ۲۶.

7. Cyber War

8. Sheldon, John, (2016), cyberwar, Encyclopædia Britannica, Accessed 17 May 2017, [https://www.britannica.com/topic/cyberwar]

ملی، تعقیب و رسیدگی جرایم سایبری در مقایسه با جـرایم عـادی اهمیتـی اساسـی و دو چندان پیدا می‌کند. نکته اساسی اینکه با توجه به ارتکاب این جـرایم از هـر نقطـه مکـانی جهان باید چگونگی تعیین صلاحیت را مشخص نمود. اما بنا به دلایلـی کـه توضـیح آن از نظر خواهد گذشت نمی‌بایست در حـل مسـأله چگـونگی تعقیـب و رسـیدگی بـه جـرایم سایبری تنها به قواعد صلاحیت کیفری توجه داشت. از این روست که به لحاظ راهبردی و به منظور مقابله مؤثر با این دسته از جرایم، در کنار تعیـین قواعـد صـلاحیت کیفـری بـه راهکارهای راهبردی دیگر هم می‌بایست توجه داشت.

۲. صلاحیت کیفری

صلاحیت در لغت به معنای «شایستگی»، «اهلیت»، «قابلیت» و «توانایی یـک مقـام در انجام یک عمل» آمده است. صلاحیت در معنای اصطلاحی و فنی ناظر است به توانایی به‌کارگیری و اعمال قانون در مورد موضوعاتی که به موجب قانون در قلمرو صلاحیت یـک مرجع مشخص قـرار مـی‌گیـرد. از ایـن رو صـلاحیت بـه لحـاظ کیفـری عبـارت اسـت از شایستگی و اختیاری که به موجب قـانون بـرای مرجـع کیفـری بـه‌منظـورِ رسـیدگی بـه موضوعات کیفری پیش‌بینی شده است.[۱] به طور کلی قاعده اصلی در مورد تعیـین مرجـع صالح در امور کیفری توجه به محل وقوع جـرم اسـت؛ چنانکـه کـه یکـی از ویژگـی‌هـای برجسته حقوق کیفری درون مرزی بودن آن است بدین معنا که قواعد آن به مرزهای یک کشور محدود می‌گردد و ناظر به روابط اشخاص یک جامعـه در محـدود سـرزمینی واحـد است.[۲] در این باره، قانون مجازات اسلامی مصوب ۱ اردیبهشـت ۱۳۹۲ (زیـن پـس: ق.م.ا) چنین مقرر کرده است: «قوانین جزایی ایران درباره کلیه اشخاصی که در قلمرو حاکمیـت زمینی، دریایی و هوایی جمهوری اسلامی ایران مرتکب جرم شوند اعمال مـی شـود». لازم به ذکر است که اگر محل وقوع جرم نامعلوم باشد، اصولاً به اعتبار محل کشف جرم، محـل دستگیری متهم، محل اقامت متهم هم مرجع قضایی می‌تواند اقـدام بـه رسـیدگی کنـد.[۳] افزون بر معیارهای پیش‌گفته، گاه عنصر خارجی به صـلاحیت کیفـری جنبـه بـین‌المللـی می‌بخشد چنانکه گاه تبعه یک کشور در کشوری دیگر مرتکب جرم می‌شود یـا تبعـه یـک کشور در کشوری دیگر بزه‌دیده می‌شود و گاه ارتکاب جرم خـارج از مرزهـای سـرزمینی و فارغ از اینکه توسط تبعه یا علیه تبعه کشور باشد، علیه منافع عـالی کشـور یعنـی نظـم و امنیت آن صورت می‌گیرد و نیز گاه شدت جرم به حدّی است که فارغ از معیار سـرزمینی، تابعیت و منافع عالی کشورها مدنظر قرار گرفته و مرتکب آن در هر کشوری که یافت شود

۱. آخوندی، محمود، آیین دادرسی کیفری، چاپ هشتم، تهران، وزارت فرهنگ و ارشاد اسلامی، ۱۳۸۴، ص. ۲۷۴.
۲. اردبیلی، محمدعلی، حقوق جزای عمومی، چاپ هجدهم، تهران، میزان، ۱۳۸۶، ص. ۴۱.
۳. ماده ۱۱۶ قانون آیین دادرسی کیفری مصوب ۴ اسفند ۱۳۹۲.

قابل تعقیب و رسیدگی در محاکم همان کشور خواهد بود. با توجه به معیارهای گفته شده، افزون بر صلاحیت سرزمینی، صلاحیت مبتنی بر تابعیت متهم، صلاحیت مبتنی بر تابعیت بزه‌دیده، صلاحیت مبتنی بر منافع عالی کشور و صلاحیت جهانی تشکیل‌دهنده مجموعه معیارهایی است که به موجب آن می‌توان مرجع صالح کیفری برای رسیدگی به جرمی را تعیین نمود. اما در مورد موضوع مسئله یعنی جرایم سایبری با توجه به ویژگی‌های مورد اشاره این نوع از جرایم باید با بررسی و تحلیل هر یک از این معیارها صلاحیت کیفری سایبری را توضیح و تبیین نمود. به بیان دیگر، از آنجایی که کنش‌های انجام‌یافته مجازی غیرمادی و غیرملموس بوده و در فضای مکانی مشخص و معینی صورت نمی‌گیرد باید با تحلیل معیارهای ناظر به صلاحیت کیفری ضمن توجه به ویژگی جرایم سایبری، معیار صلاحیت کیفری سایبری را معلوم نمود.

۳. معیارهای صلاحیت

در خصوص جرایم سایبری به عنوان بزهکاری بدون مرز[1] می‌توان قائل بر این نظر بود که از لحاظ صلاحیت چندبُعدی[2] است. به بیان دیگر، با توجه به عدم تعیین مکانی جرم سایبری، برایِ تعیین معیار صلاحیت این نوع از جرایم می‌توان جنبه‌های مختلفی را لحاظ نمود. با مداقه در عناصر جرم سایبری نظیر بستر ارتکاب جرم سایبری و چگونگی انجام آن، کاربر یا مرتکب و نیز بزه‌دیده جرم سایبری[3] و جز اینها می‌توان فروض مختلفی را چنین گزیده آورد: محلی که وسیله ارتکاب نظیر کامپیوتر در آن مستقر است؛ محلی که سرویس‌دهنده خدمات اینترتی در آن مستقر است؛ محلی که کاربر در آن اقامت است؛ محلی که بزه‌دیده در آن اقامت دارد؛ محلی که بارگذاری و پیاده‌سازی داده‌ها در آن انجام می‌گیرد؛ محلی که جرم در آن محقق می‌شود و جز اینها. وانگهی، درباره چگونگی تعیین صلاحیت کیفری سایبری دو فرض کلی را می‌توان چنین لحاظ نمود: نخست؛ تعیین صلاحیت کیفری سایبری به اعتبار قواعد معمول صلاحیت؛ و دوم؛ تعیین صلاحین کیفری سایبری به اعتبار ویژگی‌های جرم سایبری.

۳ـ۱. تعیین صلاحیت به اعتبار قواعد معمول صلاحیت کیفری

در تبیین و تعیین معیار صلاحیت کیفری جرایم سایبری نخستین فروض متبادر به ذهن ناظر به قواعد معمول صلاحیت کیفری است. از این رو، بررسی آن قواعد و تطبیق آن بر موضوع مسئله به عنوان یکی از فروض ممکن در چگونگی تعیین صلاحیت کیفری در جرایم سایبری مفید خواهد بود. بنابراین، امکان تعیین صلاحیت جرایم سایبری به

1. Borderless Criminality
2. Multi-Jurisdictional
3. Singh, Shikhs, Cyber Laws, New Delhi, Global India Publications, 2011, p. 13.

اعتبار صلاحیت سرزمینی، صلاحیت مبتنی بر تابعیت متهم، صلاحیت مبتنی بـر تابعیـت بزه‌دیده، صلاحیت حمایتی و صلاحیت جهانی مورد بررسی قـرار مـی‌گیـرد. لازم بـه ذکـر است که هر یک از معیارها با توجه به یک جنبه از موضوع بوده و این موارد در مقابل هـم نبوده بلکه باید در کنار هم به طور تلفیقی مورد امعان‌نظر قرار گیرد.

۳ـ۱ـ۱. صلاحیت سرزمینی

قاعده اصلی در تعیین صلاحیت محل ارتکاب جرم است و از این روسـت کـه مرجـع قضایی محل ارتکاب صالح به رسیدگی است. اما همان طور که پـیش‌تـر مـورد بحـث قـرار گرفت، جرم سایبری به لحاظ ماهیّت مجازی و غیرواقعی خود همانند جـرایم سـنتی نظیـر قتل، سرقت و جز اینها در بستر مکانی مشخصی رخ نمی‌دهد و از این جهت نمی‌توان گفـت که به طور دقیق محل وقوع جرم سایبری کجاست تا بدین‌سان مرجع صالح هم تعیین شود. با وجود این، می‌توان به بستر ارتباطات و مبادلات الکترونیکی شاره نموده که در واقع همین بستر تشکیل‌دهنده فضای سایبر بوده و داده‌های مختلف در آن مورد پردازش قرار می‌گیرند. بدین‌سان می‌توان گفت مراکز تولید بسترهای الکترونیکی که به عنوان مراکز داده بـه ارایـه خدمات میزمانی می‌پردازند محلی است که جرم سایبری در آن واقـع شـده و محـل ایـن مراکز در قلمرو حاکمیت هر کشوری که باشند تابع قوانین کیفری آن کشور بوده و از ایـن رو بنا به معیار صلاحیت سرزمینی مراجع قضایی آن کشور صالح به رسیدگی خواهند بـود. در این باره، ماده ۶۴۴ قانون آیین دادرسی کیفری (زین پس: ق.آ.د.ک) چنین مقرر کـرده است که «علاوه بر موارد پیش‌بینی شده در دیگـر قـوانین، دادگـاه‌هـای ایـران صـلاحیت رسیدگی به موارد زیر را دارند: الف ـ داده‌های مجرمانه یا داده‌هایی که برای ارتکـاب جـرم به کار رفته‌اند که به هر نحو در سامانه‌های رایانه‌ای و مخابراتی یا حامل‌هـای داده موجـود در قلمرو حاکمیت زمینی، دریایی و هوایی جمهوری اسلامی ایران ذخیره شود». این نکته را هم بایـد افـزود کـه بـه اسـتناد ۶۵۵ ق.آ.د.ک «چنانچـه جـرم رایانـه‌ای در صـلاحیت دادگاه های ایران در محلی کشف یـا گـزارش شـود، ولـی محـل وقـوع آن معلـوم نباشـد، دادسرای محل کشف مکلف است تحقیقات مقدماتی را انجام دهد. در صـورتی کـه محـل وقوع جرم مشخص نشود، دادسرا پس از اتمام تحقیقات مبادرت به صدور قرار و در صورت اقتضاء صدور کیفرخواست می‌کند و دادگاه مربوط نیز رأی مقتضی را صادر می‌کند.»

۳ـ۱ـ۲. صلاحیت مبتنی بر تابعیت متهم

یکی دیگر از معیارهای درخور توجه در صلاحیت کیفری سایبری ناظر به معیار قـرار دادن تابعیت متهم است. بنابراین دولت‌ها می‌تواند قوانین خود را نسبت به اتباع خود فارغ از اینکه محل ارتکاب جرم کجا بوده است، اعمال کنند. در این بـاره، مـاده ۷ ق.م.ا چنـین مقرر نموده است که «... هر یک از اتباع ایران در خارج از کشور مرتکـب جرمـی شـود، در

صورتی که در ایران یافت و یا به ایران اعاده گردد، طبق قوانین جمهوری اسلامی ایران محاکمه و مجازات می‌شود ...». بنابراین، با توجه به جرم بودن برخی رفتاری سایبری در قوانین جمهوری اسلامی ایران (بند الف ماده ۷ ق.م.ا) و نیز تعزیری بودن این دسته از جرایم (بند ب ماده ۷ ق.م.ا) و لحاظ باقی شرایط مقرر یعنی اینکه متهم در محل وقوع جرم محاکمه و تبرئه نشده یا در صورت محکومیت، مجازات کلاً یا بعضاً درباره او اجراء نشده باشد (بند ب ماده ۷ ق.م.ا) و اینکه طبق قوانین ایران موجبی برای منع یا موقوفی تعقیب یا موقوفی اجرای مجازات یا سقوط آن نباشد (بند پ ماده ۷ ق.م.ا)، پس از یافت شدن متهم یا اعاده او به کشور و در نهایت با توجه به مقررات قانون آیین دادرسی کیفری، مرجع قضایی محل دستگیری یا محل اقامت متهم صالح به رسیدگی خواهد بود.

۳ـ۱ـ۳. صلاحیت مبتنی بر تابعیت بزه‌دیده

معیار دیگری که برای صلاحیت کیفری سایبری می‌تواند مورد استفاده قرار گیرد معیار تابعیت بزه‌دیده است، چنانکه در این معیار محل ارتکاب جرم سایبری و یا تابعیت متهم ملاک نیست بلکه کافی است جرمی سایبری علیه یکی از اتباع رخ داده باشد تا مراجع قضایی کشور صلاحیت رسیدگی داشته باشد. در این باره، ماده ۸ ق.م.ا مقرر نموده است که «هر گاه شخص غیر ایرانی در خارج از ایران علیه شخصی ایرانی یا علیه کشور ایران مرتکب جرمی ... شود و در ایران یافت و یا به ایران اعاده گردد، طبق قوانین جزایی جمهوری اسلامی ایران به جرم او رسیدگی می‌شود». بنابراین، با تحقق سایر شرایط یعنی اینکه رفتار ارتکابی در جرایم موجب تعزیر به موجب قانون جمهوری اسلامی ایران و قانون محل وقوع، جرم باشد (بند ب ماده ۸ ق.م.ا) و اینکه متهم در جرایم موجب تعزیر در محل وقوع جرم، محاکمه و تبرئه نشده یا در صورت محکومیت، مجازات کلاً یا بعضاً درباره او اجراء نشده باشد (بند الف ماده ۸ ق.م.ا)، پس از یافت شدن یا اعاده متهم به کشور فارغ از اینکه تابعیت او چیست و در نهایت با توجه به مقررات قانون آیین دادرسی کیفری، مرجع قضایی محل دستگیری یا محل اقامت متهم صالح به رسیدگی خواهد بود.

لازم به ذکر است که در یک مورد ویژگی بزه‌دیده به لحاظ سن و نه تابعیت می‌تواند معیار صلاحیت محاکم ایران باشد. بند (ت) ماده ۶۴۴ ق.آ.د.ک چنین مقرر کرده است که اگر «جرایم رایانه‌ای متضمن سوءاستفاده از اشخاص کمتر از هجده سال، اعم از اینکه بزه‌دیده یا مرتکب ایرانی یا غیر ایرانی باشد و مرتکب در ایران یافت شود»، در این صورت وفق صدر ماده ۶۴۴ دادگاه‌های ایران صلاحیت رسیدگی خواهند داشت. بنابراین، اگر جرایم رایانه‌ای متضمن سوءاستفاده از اشخاص کمتر از هجده سال باشد، در این صورت تابعیت مدنظر نبوده و به صرف همان ویژگی سنی، محاکم ایران دارای صلاحیت خواهند بود. در فرض اخیر اگر جرم در بستر سامانه‌های رایانه‌ای و مخابراتی یا حامل‌های داده

موجود در قلمرو حاکمیت زمینی، دریایی و هوایی جمهوری اسلامی ایران ارتکاب یافته باشد، مراجع قضایی مستقر در محل این سامانه‌ها به عنوان محل ارتکاب جرم صلاحیت خواهند داشت. در غیر صورت، به شرط یافت شدن یا اعاده متهم به کشور، با توجه به مقررات قانون آیین دادرسی کیفری، مرجع قضایی محل دستگیری یا اقامت متهم صلاحیت رسیدگی خواهد داشت.

۳ـ۱ـ۴. صلاحیت حمایتی

در برخی موارد جرایم سایبری می‌توان قائل به صلاحیت حمایتی بود. در واقع، به موجب اصل صلاحیت حمایتی هرگاه جرم ارتکابی فارغ از تابعیت مرتکب و محل ارتکاب منجر به لطمه به منافع عالی کشور شود؛ در این صورت، مراجع قضایی کشور نسبت به چنین جرمی صلاحیت خواهند داشتند.[۱] از این رو، در خصوص ارتکاب برخی از جرایم سایبری نظیر تروریسم سایبری می‌توان با توجه به این نوع از صلاحیت، برای مراجع قضایی قایل به صلاحیت بود. البته وصف سایبری برای جرایم خصوصیتی ندارد و کافی است که یکی از منافع عالی نظیر امنیت داخلی و خارجی مورد لطمه باشد (ماده ۵ ق.م.ا). بنابراین، در فرض ارتکاب جرم سایبری که به منافع عالی لطمه می‌زند با حصول سایر شرایط یعنی ارتکاب جرم خارج از قلمرو حاکمیتی ایران و فارغ از اینکه مرتکب تابعیت ایرانی یا غیرایرانی داشته باشد (ماده ۵ ق.م.ا) امکان استناد به صلاحیت حمایتی برای رسیدگی به جرایم سایبری در محاکم داخلی فراهم می‌شود. در این باره بنده (پ) ماده ۶۴۴ ق.آ.د.ک هم چینن مقرر کرده است: «جرم توسط تبعه ایران یا غیر آن در خارج از ایران علیه سامانه‌های رایانه‌ای و مخابراتی و تارنماهای مورد استفاده یا تحت کنترل قوای سه‌گانه یا نهاد رهبری یا نمایندگی‌های رسمی دولت یا هر نهاد یا مؤسسه‌ای که خدمات عمومی ارائه می‌دهد یا علیه تارنماهای دارای دامنه مرتبه بالای کد کشوری ایران در سطح گسترده ارتکاب یابد». در این صورت، با توجه به مقررات قانون آیین دادرسی کیفری مرجع قضایی محل دستگیری یا اقامت مرتکب صالح به رسیدگی خواهد بود.

۳ـ۱ـ۵. صلاحیت جهانی

برخی جرایم حسب شدّت به عنوان جرم علیه تمام بشریت تلقی می‌شوند که در این صورت مراجع قضایی همه کشورها فارغ از محل ارتکاب جرم، تابعیت متهم، تابعیت بزه‌دیده، صالح به رسیدگی خواهند بود.[۲] برای نمونه جرایمی نظیر نسل‌کشی و جنایات علیه بشریت قابل اشاره است که به لحاظ شدّت قابل رسیدگی توسط تمام کشورهاست.

۱. پوربافرانی، حسن، «تحول اصل صلاحیت واقعی در لایحهٔ جدید مجازات اسلامی»، فصلنامه دیدگاه‌های حقوق قضایی، شماره ۵۸، ۱۳۹۱، صص. ۷۷ ـ ۷۵.

۲. پوربافرانی، حسن، حقوق جزای بین‌المللی، تهران، جنگل، ۱۳۹۰، ص. ۱۶۸.

در این باره باید گفت کمینه امکان استفاده از صلاحیت جهانی امکان استناد به آن در حالتی است که مرتکب در سرزمین کشور باشد بدون در نظر گرفتن اینکه ملیّت مرتکب چیست و مکان ارتکاب جرم کجاست. در این راستا، برخی بر این باروند که اجرای بدون محدودیت اصل صلاحیت جهانی ناقض اصل حاکمیت سایر کشورها خواهد بود.[1] به‌ویژه در مورد کشوری که مرتکب تابع آن است و یا جرم در سرزمین آن رخ داده است. فراروی آن، برخی در رد این استدلال این گونه پاسخ گفته‌اند که جرایمی همانند نسل‌کشی و جنایات علیه بشریت تمام جامعه بین‌المللی را متأثر می‌کند، از این رو، چنین جرایمی در پیوند با امور داخلی کشورها نبوده و ناقض حق حاکمیت آنها نخواهد بود، بلکه چنین جرایمی آنچنان سرزنش‌پذیر هستند که مرتکب آن دشمن تمام ملل فرض شده و از این جهت هر دولتی حق تعقیب این جرایم را خواهد داشت.[2و3] با توجه به نکته پیشین، محدود ماندن در سایر گونه های صلاحیت پذیرفتنی نبوده[4] و همه دولت ها بدون لحاظ اینکه ارتباطی با جرم داشته باشند، نسبت به پیگرد جرایم بین‌المللی بنابر اصل صلاحیت جهانی، صلاحیت خواهند داشت.[5]

باید بدین نکته توجه داشت که امکان استناد به صلاحیت جهانی زمانی امکان‌پذیر است که اجماع یا توافقی بین‌المللی در مورد شدید بودن جرم وجود داشته باشد چنانکه پذیرفته شود همه کشورها می‌توانند بنابر صلاحیت جهانی اقدام به رسیدگی کنند. گفتنی است بر خلاف جرایمی نظیر نسل‌کشی، هنوز در مورد جرایم سایبری چنین اجماع و توافقی ایجاد نشده و کنوانسیونی در این باره به تصویب نرسیده است.[6] با این همه، باید توجه داشت که صلاحیت جهانی در دو مفهوم موسع و مضیق به کار رفته است. صلاحیت جهانی در مفهوم موسّع بدین معناست که مراجع قضایی همه کشورها فارغ از محل ارتکاب جرم، تابعیت متهم، تابعیت بزه‌دیده و بدون هیچ قید دیگر می‌توانند رسیدگی کنند. اما صلاحیت جهانی در مفهوم مضیق بدین معناست که مراجع قضایی کشورها زمانی می‌توانند فارغ از محل ارتکاب جرم، تابعیت متهم، تابعیت بزه‌دیده اقدام به رسیدگی

۱. مومنی، مهدی، مبانی حقوق جزای بین‌الملل ایران، تهران، شهر دانش، ۱۳۸۸، ص. ۱۱۵.

۲. میرمحمد صادقی، حسین، «صلاحیت دولت‌ها در رسیدگی به جرایم بین‌المللی»، فصلنامه دیدگاه‌های حقوق قضایی، شماره ۸، ۱۳۷۶، صص. ۱۴۹ ـ ۱۳۶.

۳. رضوی‌فرد، بهزاد؛ و محمد فرجی، «بایستگی جرم‌انگاری جرایم بین‌المللی و الگوهای آن»، راهبرد، شماره ۸، ۱۳۹۶، صص. ۲۸ ـ ۵.

4. Bantekas, Llias; and Susan Nash, International Criminal Law, Third Edition. UK, Routledge-Cavendish, 2007. p. 71.

5. Kreicker, Helmut, National Prosecution of International Crimes from a Comparative Perspective, Germany, Max Planck Institute for Foreign and International Criminal Law, 2006, p. 7.

۶. فروغی، فضل‌الله؛ و امیر البوعلی، «صلاحیت کیفری مراجع قضایی در فضای سایبر»، مجله تحقیقات حقوقی، شماره ۵۸، ۱۳۹۱، صص. ۳۵۶ ـ ۳۱۱.

کنند که متهم در قلمرو حاکمیت کشور اقدام‌کننده یافت شود. بنابراین، به نظر می‌رسد در فرض پذیرش جرایم سایبری به عنوان جرایم بین‌المللی قابل تعقیب بر اساس اصل صلاحیت جهانی، با توجه به مسائلی نظیر اصل حاکمیت دولت‌ها، استناد به اصل صلاحیت جهانی زمانی امکان‌پذیر است که متهم در قلمرو حاکمیتی یافت شود. قانون مجازات اسلامی هم مفهوم مضیق صلاحیت جهانی را پذیرفته است.[1]

۳ـ۲. تعیین صلاحیت به اعتبار ویژگی‌های جرم سایبری

افزون بر توجه به معیارهای معمول تعیین صلاحیت، از چشم‌اندازی دیگر می‌توان با توجه به برخی ویژگی‌های جرایم سایبری معیارهای دیگری را هم برای تعیین صلاحیت کیفری این دسته از جرم پیش‌بینی کرد. از این رو، می‌توان مراجع قضایی محل استقرار سیستم رایانه‌ای یا سرور، محل بارگذاری و محل پیاده‌سازی را به عنوان مرجع قضایی صالح مورد شناسایی قرار داد.

۳ـ۲ـ۱. صلاحیت مرجع قضایی محل استقرار سامانه رایانه‌ای

در خصوص مورد نخست یعنی محل استقرار سامانه رایانه‌ای «جایی که کامپیوتر تأثیرگذار در وقوع جرایم رایانه‌ای قرار دارد و یا جایی که ماهواره وسیله ارتکاب جرم ثبت شده است، محل ارتکاب جرم محسوب شده و نظام قضایی همان محل جهت تعقیب جرم ارتکابی صالح خواهد بود.»[2] در این راستا، قانون جرایم رایانه‌ای به موجب بند الف ماده ۶۴۴ ق.آ.د.ک در مواردی که داده‌های مجرمانه یا داده‌هایی که برای ارتکاب جرم به کار رفته است به هر نحو در سامانه‌های رایانه‌ای و مخابراتی یا حامل‌های داده موجود در قلمرو حاکمیت زمینی، دریایی و هوایی جمهوری اسلامی ایران ذخیره شده باشد، دادگاه‌های ایران را صالح دانسته است. وانگهی، این معیار بازنمودی از همان معیار صلاحیت سرزمینی است که اما ایراد اساسی آنست که از آنجایی که اغلب این سیستم‌ها یا سرورها در امریکای شمالی و اروپا مستقر هستند، باید گفت اعمال صلاحیت به شکل پیش‌گفته به عنوان معیار مناسبی نمی‌تواند انگاشته شود، زیرا بزه‌دیدگان سراسر جهان برای اقامه دعوی ناگزیر خواهند بود بدین کشورها مراجعه کنند که غیرعملی بودن این امر آشکار است. در این باره، گفتنی است قانون آیین دادرسی کیفری به ارتکاب جرم از طریق تارنماهای دارای دامنه مرتبه بالای کد کشوری معیاری برای اعمال صلاحیت دادگاه‌های

۱. در این باره ماده ۹ قانون مجازات اسلامی چنین مقرر کرده است: «مرتکب جرایمی که به موجب قانون خاص یا عهدنامه‌ها و مقررات بین‌المللی در هر کشوری یافت شود در همان کشور محاکمه می‌شود، اگر در ایران یافت شود طبق قوانین جزایی جمهوری اسلامی ایران محاکمه و مجازات می‌گردد.»

۲. همان.

ایران قرار داده است. بند (ب) ماده ۶۴۴ ق.آ.د.ک در این خصوص چنین مقرر کرده است: «جرم از طریق تارنماهای دارای دامنه مرتبه بالای کد کشوری ایران (ir.) ارتکاب یابد». نکته قابل ذکر اینکه دامنه مرتبه بالای کد کشوری[1] یک دامنه‌اینترنتی است که برای یک کشور، یا منطقه وابسته به قلمرو یک کشور و ... مورد استفاده قرار گرفته یا رزرو شده است. در نتیجه ویژگی قابل ذکر در خصوص دامنه مرتبه بالای کد کشوری ارتباط آن با یک منطقه جغرافیایی است. گویی ارتکاب جرم از طریق تارنماهای دارای دامنه مرتبه بالای کد کشوری ایران به منزله ارتکاب جرم در قلمرو حاکمیتی ایران است که در این صورت دادگاه‌های ایران صلاحیت خواهند داشت.

۳ـ۲ـ۲. صلاحیت مرجع محل بارگذاری یا محل پیاده‌سازی

در خصوص مورد دوم و سوم یعنی محل بارگذاری و محل پیاده‌سازی باید گفت که فعالیت در فضای سایبر از دو حال خارج نیست؛ یا اطلاعات وارد این فضا می‌شود که به این امر بارگذاری اطلاق می‌گردد یا اطلاعات از آن برداشته می‌شود که به این امر پیاده‌سازی اطلاق می‌گردد. بر این اساس، اگر بارگذاری متضمن رفتاری مجرمانه باشد، در این صورت مراجع قضایی محل بارگذاری صالح به رسیدگی خواهند بود و اگر پیاده‌سازی متضمن رفتاری مجرمانه باشد، در این صورت مراجع قضایی محل پیاده‌سازی صالح به رسیدگی خواهند بود.[2] البته این معیارها هم در پیوند با معیارهای معمول صلاحیت کیفری قابل اعمال است چنانکه برای نمونه اگر این رفتارها اعم از بارگذاری یا پیاده‌سازی در قلمرو حاکمیتی کشور باشد معیار صلاحیت سرزمینی اعمال می‌شود. اما اگر این رفتارها در خارج از قلمرو حاکمیتی باشد به لحاظ قانونی باید به معیارهای دیگر برای تعیین صلاحیت توجه داشت. وانگهی، با توجه به بند (ب) ماده ۶۴۴ ق.آ.د.ک که مقرر کرده است که «جرم از طریق تارنماهای دارای دامنه مرتبه بالای کد کشوری ایران (ir.) ارتکاب یابد»، گویی اگر رفتارهای مورد بحث وفق این بند انجام شود، چنانکه پیش‌تر بحث شد، به منزله این است که محل بارگذاری یا پیاده‌سازی محدود جغرافیایی ایران است. در نتیجه، مقرره پیش‌گفته به نوعی بر معیار مورد بحث یعنی محل بارگذاری یا محل پیاده‌سازی هم دلالت دارد.

۴. محدودیت

اگرچه در فرض ارتکاب جرایم سایبری به لحاظ معیارهای گوناگون، صلاحیت کیفری سایبری مشخص می‌شود اما محدودیت‌هایی وجود دارد که بدون رفع آنها توسل صرف به آن معیارها منتهی به رسیدگی و محاکمه و مجازات جرایم سایبری نخواهد شد.

1. Country Code Top Level Domain

۲. فروغی، فضل‌الله؛ و امیر البوعلی، منبع پیشین.

محدودیت اساسی در این باره ناظر به حالتی است که مرتکب خارج از قلمرو حاکمیتی است؛ چنانکه برای نمونه در صلاحیت مبتنی بر تابعیت متهم دولت‌ها می‌توانند قوانین خود را نسبت به اتباع خود فارغ از اینکه محل ارتکاب جرم کجا بوده است اعمال کنند اما پیش‌شرط ضروری آن «یافت شدن» مرتکب در قلمرو حاکمیتی کشور است. همچنین است در صلاحیت مبتنی بر تابعیت بزه‌دیده که پیش‌شرط اعمال آن «یافت شدن» یا «اعاده شدن» متهم به کشور است. در نتیجه گرچه با معیارهایی مشخص مرجع قضایی صالح تعیین می‌گردد، اما در برخی موارد به تنهایی برای اعمال صلاحیت و تحقق رسیدگی کفایت نمی‌کند. به بیان دیگر، اصولاً «دسترسی» به متهم شرط رسیدگی و محاکمه و مجازات است. گفتنی است که بین‌المللی شدن بزهکاری خاص جرایم سایبری نیست اما بنا به سهولت ارتکاب این جرایم از هر نقطه مکانی و تأثیر آن در مناطق مختلف، مسئله دسترسی به متهم اهمیت بیشتری دارد. از این رو، لازم است که با توجه به شیوع جرایم سایبری و تهدید فزاینده آن برای امنیت کشور در راستای تقویت نظام قضایی و به‌منظورِ تحقق صلاحیت مراجع قضایی داخلی و تمهید امکان رسیدگی توسط آنها، چالش عدم دسترسی به متهمان جرایم سایبری مورد توجه جدی قرار گرفته و به لحاظ راهبردی مدنظر قرار گیرد.

۵. راهبرد تحققِ صلاحیت سایبری

چنانکه گفته شد، صلاحیت یعنی توانایی به‌کارگیری و اعمال قانون در مورد موضوعاتی که به موجب قانون در قلمرو صلاحیت یک مرجع مشخص قرار می‌گیرد؛ با توجه به توضیحات پیشین در مواردی به رغم صلاحیت مراجع قضایی «توانایی اعمال قانون» وجود ندارد. در این باره، مطالعه راهبردهای جرایم سایبری برخی کشورها نظیر بریتانیا، فرانسه و آلمان و حتی در سطح اتحادیه اروپا حاکی از آنست که در این سیاست‌های راهبردی سایبری آنها به همکاری بین‌المللی توجه جدّی شده است. اهمیت این موضوع به لحاظ امر صلاحیت کیفری ناظر به تحقق آنست به واسطه دسترسی به متهم و در نتیجه فراهم آمدن امکان «اعمال قانون» چنانکه در تعریف صلاحیت آمد.

۵ـ۱. مطالعه تطبیقی راهبردهای سایبری

در این باره، در راهبردهای جرایم سایبری بریتانیا به همکاری بین‌المللی به عنوان یکی از راهبردهای این موضوع در خصوص انجام تحقیقات مقدماتی نظیر کسب داده‌های مربوط به جرم ارتکابی و استرداد متهمان اشاره شده و به همکاری این کشور با گروه کشورهای جی ـ هشت و اتحادیه اروپا اشاره کرده است.[1] در راهبردهای جرایم سایبری

1. Home Office (2010), Cyber crime strategy, Accessed 14 June 2017, [https://www.gov.uk/government/publications/cyber-crime-strategy]

کشور آلمان نیز به همکاری بین‌المللی در سطوح مذکور و همچنین در سازمان امنیت و همکاری در اروپا اشاره کرده و پیشنهاد داده است که باید یک کد سایبری تهیه و در سطح بین‌المللی اجرا شود.[1] در کشور فرانسه نیز در خصوص راهبردهای حفاظت و امنیت سیستم‌های داده‌ها به راهبرد اتّحاد در برابر مسائل جمعی[2] که جرایم سایبری از جمله این مسائل است اشاره شده و همکاری بین‌المللی در زمینه سایبری را مدنظر قرار داده است.[3] در سطح اروپا نیز یکی از راهبردهای مورد توجه، همکاری مؤثر بین‌المللی ذکر شده است، چنانکه اساساً جرایم سایبری را به عنوان جرایم فراملی لحاظ کرده که رسیدگی به آن نیازمند همکاری پلیسی و قضایی است.[4] همچنین، در سطح اروپا، کنوانسیون بوداپست در ماده ۲۳ مقرر نموده است که «اعضای کنوانسیون باید ... از طریق اجرای اسناد بین المللی مربوط به همکاری بین المللی در موضوعات کیفری، ترتیبات توافق شده راجع به قانونگذاری متحدالشکل یا متقابل و قوانین داخلی و برای رسیدن به وسیع‌ترین حوزه پی‌جویی یا رسیدگی قضایی راجع به جرایم مرتبط با سیستم‌های رایانه‌ای و داده‌ها یا جمع‌آوری ادله الکترونیک در جرایم ، با یکدیگر همکاری کنند.»[5]

۵ـ۲. تقویت همکاری‌های بین‌المللی

مشخص شد که در رسیدگی و محاکمه و مجازات جرایم سایبری تعیین معیار صلاحیت و در نتیجه تعیین مرجع قضایی صالح کفایت نمی‌کند. چنان که در تعریف نوشته آمد توانایی به کارگیری و اعمال قانون هم بخشی از صلاحیت است و تحقق آن منوط به این توانایی. از این رو، در مواردی که مراجع قضایی صلاحیت دارند اما متهم یا حتی ادله جرم در دسترس نیست؛ بی‌گمان مشخص بودن مرجع قضایی صالح به تنهایی کافی نبوده و در این باره لازم است اقداماتی صورت گیرد تا توانایی به‌کارگیری و اعمال قانون توسط مرجع قضایی صالح فراهم شود. لازم به ذکر است با توجه به ویژگی جرایم سایبری که اصولاً می‌تواند به عنوان جرایم فراملی لحاظ گردد، توجه به همکاری بین‌المللی به عنوان راهبردی اساسی و کارآمد امری ضروری است. گفتنی است در نظام حقوقی جمهوری اسلامی ایران گرچه تاکنون اقدامی جدی درباره صورت نگرفته اما

1. Federal Ministry of the Interior (2011), Cyber Security Strategy for Germany, Accessed 14 June 2017, [https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?_blob=publicationFile]
2. Une stratégie unifiée face à des menaces communes.
3. Agence nationale de la sécurité des systèmes d'information (2011), Défense et sécurité des systèmes d'information; Stratégie de la France, Accessed 14 June 2017, [https://www.enisa.europa.eu/media/news-items/French-cyber-security-strategy-2011].
4. Council of Europe (2001), Convention on Cybercrime, Budapest, 23.XI.2001, Accessed 14 June 2017, [http://www.coe.int/en/web/cybercrime/the-budapest-convention]
5. Ibid.

به‌لحاظ سیاستی با خلاء مواجه نیستیم چنانکه در این باره، در یک مورد، در سیاست‌های کلی نظام جمهوری اسلامی ایران در موردشبکه‌های اطلاع‌رسانی رایانه‌ای، ابلاغی مقام معظم رهبری مصوب ۱۳۷۷/۷/۱۱، بر اقدام مناسب برای دستیابی به میثاق‌ها و مقررات بین‌المللی تأکید شده است. در نتیجه با توجه به ویژگی برجسته جرایم سایبری یعنی امکان ارتکاب آن در فضایی مجازی، از هر نقطه مکانی و جنبه بین‌المللی آن؛ مقابله کارآمد با چنین جرایمی در سطح ملی و صرف تعیین معیارهای صلاحیت، امکان‌پذیر نبوده و نیازمند همکاری‌های کیفری بین‌المللی است. از این رو، با تعریف جرایم سایبری و معلوم ساختن معیارهای صلاحیت کیفری در این دسته از جرایم و در نهایت پیش‌بینی سازوکارهای همکاری بین‌المللی برای تعقیب و تحقیق و رسیدگی، مراجع قضایی صالح به جرایم مربوط رسیدگی می‌کنند.[۱] در نتیجه، مشارکت و همکاری کشورها به دلیل جهانی شدن مسأله بزهکاری باید مدنظر بوده و اساساً از این روست که امضاء و تصویب موافقت‌نامه‌ها و تفاهم‌نامه‌ها و عهدنامه‌های پلیسی ـ قضایی ـ امنیتی دو یا چندجانبه در دهه‌های اخیر مورد توجه قرار گرفته است[۲و۳]. نتیجه آنکه جرایم سایبری نیز از مسأله اخیر یعنی جهانی‌شدن بزهکاری مستثنی نبوده و از این جهت تعقیب و رسیدگی به این دسته از جرایم اصولاً منوط به یافت شدن متهمان این جرایم در قلمرو حاکمیتی کشور یا اعاده آنهاست. از این رو، افزون بر شناسایی معیارهای صلاحیت کیفری در جرایم سایبری، باید به تحقق صلاحیت مراجع قضایی توجه داشت و برایِ این منظور و امکان تعقیب و تحقیق و رسیدگی و محاکمه و در نهایت اجرای مجازات، همکاری کیفری بین‌المللی را مورد توجه قرار داد. بدین‌سان است که محدودیت‌های ناظر به اعمال صلاحیت در جرایم با جنبه بین‌المللی از جمله جرایم سایبری حل‌وفصل خواهد شد. در این زمینه و در خصوص جرایم سایبری بستر همکاری‌های پلیسی و قضایی فراهم به نظر می‌رسد چنانکه پیرو برخی موافقنامه‌های دوجانبه از جمله موافقت‌نامه همکاری‌های امنیتی ایران و روسیه، گسترش همکاری‌ها در زمینه‌های مختلف امنیتی و پلیسی از جمله مقابله با جرایم مدنظر قرار گرفته است.[۴]

۱. فروغی، فضل‌الله، «موانع و محدودیت‌های تعقیب داخلی جرایم بین‌المللی»، مطالعات حقوقی (ویژه‌نامه حقوق جزا و جرم‌شناسی)، شماره ۲، ۱۳۸۹، صص. ۱۶۴ ـ ۱۲۹.

۲. نجفی ابرندآبادی، علی‌حسین، جهانی شدن حقوق کیفری و تعاملات دانشگاهی بین‌المللی، دیباچه در: رضوی‌فرد، بهزاد، جلوه‌هایی از حقوق کیفری فرانسه، تهران، انتشارات دانشگاه علامه طباطبایی، ۱۳۹۵.

۳. کلانتری، کیومرث، مجموعه قوانین و مقررات همکاری‌های بین‌المللی ایران و کشورهای جهان در زمینه کیفری، تهران، انتشارات مجد، ۱۳۹۴.

4. Iranian Students' News Agency, Accessed 18 June 2017, [http://www.isna.ir/news/94031709582].

نتیجه‌گیری

صلاحیت ناظر است به توانایی به‌کارگیری و اعمال قانون در مورد موضوعاتی کـه بـه موجب قانون در قلمرو صلاحیت یک مرجع مشخص قرار می‌گیرد. از این رو صـلاحیت بـه لحاظ کیفری عبارت است از شایستگی و اختیاری که به موجب قانون برای مرجع کیفـری به‌منظورِ رسیدگی به موضوعات کیفـری پـیش‌بینـی شـده اسـت. در ایـن میـان، یکـی از موضوعات کیفری ناظر است به فضای سایبری و جرایم سایبری. نکته اساسی در ایـن بـاره آنست که با مداقه در تعاریف ناظر به فضای سایبری می‌توان به سه عنصـر اساسـی اشـاره کرد. نخست؛ سامانه‌ای رایانه‌ای دوم؛ شبکه اینترنت و سوم؛ کاربران. در این خصوص آنچـه باید بدان توجه داشت آن است که گرچـه عنصـر اول و سـوم در فضـای مـادی موجـود و ملموس است اما عنصر سوم موجودیت مادی و ملموسی ندارد و از ایـن روسـت کـه تمـام کنش‌های انجام‌یافته در این فضای مجازی و غیرملمـوس بعـد مکـانی مشـخص و معینـی ندارد چنانکه برخی در تعریف فضای سایبر بدان نکته توجه داشته و چنـین تعریفـی ارائـه داده‌اند که فضای سایبر به مجموعه‌هایی از ارتباطات درونـی انسـان‌هـا از طریـق رایانـه و وسایل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می‌شود. در نتیجه، با توجـه به ویژگی فضای سایبری، تعیین مرجع صالح قضایی مشکل به نظر می‌رسد. افزون بر ایـن، مشکل دیگر با توجه به امکان ارتکاب این دسته از جرایم از هر نقطه مکانی و تـأثیر آن در مکانی دیگر است. در خصوص مشکل اول باید متذکر شد کـه اصـولاً بـا توجـه بـه قواعـد تعیین صلاحیت، مسأله تعیین مرجع صـالح قضـایی ممکـن مـی‌شـود. در ایـن خصـوص می‌توان به تعیین مرجع قضایی صالح به اعتبار قواعد معمـول تعیـین صـلاحیت و نیـز بـه تعیین مرجع قضایی صالح به اعتبار ویژگی‌های نحوه ارتکاب جرایم سایبری توجه کرد. بـه اعتبار اوّل محل ارتکاب جرم، تابعیت متهم، تابعیت بزه‌دیده، لطمه به منـافع عـالی کشـور معیارهای صلاحیت سایبری تواند بود و به اعتبار دوم محل بارگذاری و پیاده‌سازی داده‌ها. اما مشکل دوم یعنی امکان ارتکاب جرایم سایبری از هر نقطه مکانی و تأثیر آن در منطقـه مکانی دیگر باید توجه داشت که گرچه به اعتبارات مختلف مرجـع قضـایی صـالح تعیـین می‌گردد اما به تنهایی راهگشا نیست. در واقع، اساساً نظر به ویژگی فضای سایبر و ویژگـی جرایم سایبری می‌توان گفت این دسته از جرایم را اصولاً می‌توان به عنوان جـرایم فراملـی مورد امعان‌نظر قرار داد. از این رو، اگر بدین نکته اشـارت رود کـه توانـایی بـه‌کـارگیری و اعمال قانون در مورد موضوعاتی کـه بـه موجـب قـانون در قلمـرو صـلاحیت یـک مرجـع مشخص قرار می‌گیرد از عناصر متشکله تعریف صلاحیت است و تحقق صلاحیت منوط به آن، آنگاه به لحاظ راهبردی ایجاد و امکان این توانایی لازم می‌آید.

با توجه به آنچه گفته شد، نتیجه آن است که نظر به ویژگی برجسته جرایم سایبری یعنی امکان ارتکاب از هر نقطه مکانی و فراملّی بودن آن، تحقق صلاحیت کیفری مراجع قضایی در توجه به معیارهای صلاحیت مقصور نمی‌شود؛ و اما تحقق این منوط است به ایجاد توانایی لازم جهت اعمال قانون مربوط در این زمینه. راهبرد امر مذکور در تقویت همکاری کیفری بین‌المللی است، چنانکه با مطالعه تطبیقی راهبردهای سایبری برخی کشورهای توسعه‌یافته این نکته مشاهده می‌شود که آنها با توجه به ویژگی جرایم سایبری، به راهبرد پیش‌گفته یعنی تقویت همکاری کیفری بین‌المللی در زمینه تعقیب و تحقیق و رسیدگی مربوط به جرایم سایبری توجه ویژه داشته‌اند. کوتاه سخن آنکه نظر به نکات پیش‌گفته و نظر به رهنمود موجود در نظام حقوقی کشور مبنی بر اقدام مناسب برای دستیابی به میثاق‌ها و مقررات بین‌المللی، توجه به اقدام در سطح بین‌المللی برای تعقیب و رسیدگی موثر به جرایم سایبری امری ضروری است که لاجرم باید مورد پیگیری قرار گیرد. به ویژه آنکه در برخی موارد مربوط موافقت‌نامه‌های اولیه امنیتی موجود است و از این جهت امکان پیگیری امر برای تعیین چارچوب همکاری کیفری بین‌المللی در راستای تحقق صلاحیت کیفری و در نتیجه تعقیب و رسیدگی و محاکمه و اجرای مجازات می‌تواند محقق شود.

منابع

الف ـ مکتوب

- آخوندی، محمود، آیین دادرسی کیفری، چاپ هشتم، تهران، وزارت فرهنگ و ارشاد اسلامی، ۱۳۸۴.
- اردبیلی، محمدعلی، حقوق جزای عمومی، چاپ هجدهم، تهران، میزان، ۱۳۸۶.
- پوربافرانی، حسن، «تحول اصل صلاحیت واقعی در لایحه جدید مجازات اسلامی»، فصلنامه دیدگاه‌های حقوق قضایی، شماره ۵۸، ۱۳۹۱.
- ـــــــــــــ ، حقوق جزای بین‌المللی، تهران، جنگل، ۱۳۹۰.
- جعفری لنگرودی، محمدجعفر، ترمینولوژی حقوق، تهران، گنج دانش، ۱۳۸۸.
- خالقی، علی، نکته‌ها در قانون آیین دادرسی کیفری، تهران، شهر دانش، ۱۳۹۵.
- رضوی‌فرد، بهزاد؛ و محمد فرجی، «بایستگی جرم‌انگاری جرایم بین‌المللی و الگوهای آن»، راهبرد، شماره ۸، ۱۳۹۶.
- زندی، محمدرضا، تحقیقات مقدماتی در جرایم سایبری، تهران، انتشارات جنگل، ۱۳۹۳.
- فروغی، فضل‌الله، «موانع و محدودیت‌های تعقیب داخلی جرایم بین‌المللی»، مطالعات حقوقی (ویژه‌نامه حقوق جزا و جرم‌شناسی)، شماره ۲، ۱۳۸۹.
- فروغی، فضل‌الله؛ و امیر البوعلی، «صلاحیت کیفری مراجع قضایی در فضای سایبر»، مجله تحقیقات حقوقی، شماره ۵۸، ۱۳۹۱.
- کامینگا، منوتی، «اعمال صلاحیت جهانی در رابطه با جرایم سنگین حقوق بشری»، ترجمه محمد جواد شریعت باقری، مجله حقوقی بین‌المللی، شماره ۲۸، ۱۳۸۲.
- کلانتری، کیومرث، مجموعه قوانین و مقررات همکاری‌های بین‌المللی ایران و کشورهای جهان در زمینه کیفری، تهران، انتشارات مجد، ۱۳۹۴.
- مؤمنی، مهدی، مبانی حقوق جزای بین‌الملل ایران، تهران، شهر دانش، ۱۳۸۸.
- میرمحمد صادقی، حسین، «صلاحیت دولت‌ها در رسیدگی به جرایم بین‌المللی»، فصلنامه دیدگاه‌های حقوق قضایی، شماره ۸، ۱۳۷۶.
- ـــــــــــــ ، حقوق جزای بین‌الملل، تهران، بنیاد حقوقی میزان، ۱۳۹۳.
- نجفی ابرندآبادی، علی‌حسین، جهانی شدن حقوق کیفری و تعاملات دانشگاهی بین‌المللی، دیباچه در: رضوی‌فرد، بهزاد، جلوه‌هایی از حقوق کیفری فرانسه، تهران، انتشارات دانشگاه علامه طباطبایی، ۱۳۹۵.
- هولمز، دیانا، آشنایی با تکنولوژی اطلاعاتی، ترجمه مجید آذرخش و جعفر مهرداد، تهران، انتشارات سمت، ۱۳۷۷.

- Bajpai, G. S, On Cyber Crime & Cyber Law, India, Serials Publications, 2011.
- Bantekas, Llias; and Susan Nash, International Criminal Law, Third Edition. UK, Routledge-Cavendish, 2007.
- Cowles, Willard, "Universal Jurisdiction over War Crimes", California Law Review, Vol. 33, Issue 2, 1945.
- Jewkes, Yvonne; and Majid Yar, Hand book of Internet Crime, USA: Willan Publishing, 2010.
- Kreicker, Helmut, National Prosecution of International Crimes from a Comparative Perspective, Germany, Max Planck Institute for Foreign and International Criminal Law, 2006.
- Macedo, Stephen, Universal Jurisdiction: National Courts and the Prosecution of Serious Crimes Under International Law, USA, University of Pennsylvania Press, 2006.
- Ploug, Thomas, Ethics in Cyberspace: How Cyberspace May Influence Interpersonal Interaction, Ballerup, Denmark, Springer Pub, 2009.
- Singh, Shikhs, Cyber Laws, New Delhi, Global India Publications, 2011.

ب ـ اینترنتی

- Agence nationale de la sécurité des systèmes d'information (2011), Défense et sécurité des systèmes d'information; Stratégie de la France, Accessed 14 June 2017, [https://www.enisa.europa.eu/media/news-items/french-cyber-security-strategy-2011].
- Compétence universelle, Législation belge, Consulté le 7 Juin 2017. [https://competenceuniverselle.wordpress.com/legislation-belge/].
- Council of Europe (2001), Convention on Cybercrime, Budapest, 23.XI.2001, Accessed 14 June 2017, [http://www.coe.int/en/web/cybercrime/the-budapest-convention].
- Council of Europe (2012), Global Project Cybercrime @Octopus, Accessed 14 June 2017, [https://rm.coe.int/16802fa34f].
- DaviD'Agostino, Greg Wilshusen (2011), Defense Department Cyber Efforts: DoD Faces Challenges in Its Cyber Activities, DIANE Publishing, P 28. Accessed 25 June 2017,

[http://www.gao.gov/products/GAO-11-75].

- Federal Ministry of the Interior (2011), Cyber Security Strategy for Germany, Accessed 14 June 2017, [https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?_blob=publicationFile].
- Home Office (2010), Cyber crime strategy, Accessed 14 June 2017, [https://www.gov.uk/government/publications/cyber-crime-strategy].
- Iranian Students' News Agency, Accessed 18 June 2017, [http://www.isna.ir/news/94031709582].
- Bussell, Jennifer, (2013), Cyberspace, Encyclopædia Britannica, Accessed 25 June 2017, [https://www.britannica.com/topic/cyberspace].
- Sheldon, John, (2016), cyberwar, Encyclopædia Britannica, accessed 17 May 2017, [https://www.britannica.com/topic/cyberwar]
- Larousse, Consulté le 14 Mai 2017, [http://www.larousse.fr/dictionnaires/francais/cybermonde/21258].
- Larousse, consulté Le 28 mai 2017, [http://www.larousse.fr/dictionnaires/francais/comp%C3%A9tence/17648?q=competence#17517].
- Merriam-webster, accessed 14 May 2017,[https://www.merriam-webster.com/dictionary/cyberspace].
- Merriam-Webster, accessed 28 May 2017,[https://www.merriam-webster.com/dictionary/jurisdiction].
- NATO Cooperative Cyber Defence Centre of Excellence, accessed 17 May 2017, [https://ccdcoe.org/multimedia/cyberspace-definition-and-implications.html].
- Oxford dictionaries learner's, accessed 14 May 2017, [http://www.oxfordlearnersdictionaries.com/definition/english/cyberspace?q=cyberspace]