




University of Tehran Press

The solution to the conflict of criminal jurisdiction regarding cyber crimes

Esmail Baghban¹ | Babak Pourgharamani²  | Fatemeh Ahadi³

1. Ph.D Student in Criminal Law and Criminology, Maragheh Branch, Islamic Azad University, Maragheh, Iran. Email: es.baghban@gmail.com
2. Corresponding Author; Associate Professor, Department of Criminal Law and Criminology, Maragheh Branch, Islamic Azad University, Maragheh, Iran. Email: b.pourgharamani@yahoo.com
3. Assistant Professor, Department of Criminal Law and Criminology, Maragheh Branch, Islamic Azad University, Maragheh, Iran. Email: ahadi-223@yahoo.com

Article Info	Abstract
<p>Article Type: Research Article</p> <p>Pages: 1-19</p> <p>Received: 2021/04/16</p> <p>Received in Revised form: 2022/03/14</p> <p>Accepted: 2023/05/22</p> <p>Published online: ----/--/--</p> <p>Keywords: <i>conflict of laws, cyber jurisdiction, positive conflict, negative conflict, prohibition of double punishment.</i></p>	<p>Conflict of laws in Cyber space is a very fundamental challenge; Because the lack of clear demarcation in this area and ultimately the impossibility of implementing "territorial jurisdiction" as a key factor in determining jurisdiction, leads to the application of other principles of jurisdiction in this area, and when this applies to several countries and two or more different countries consider themselves competent to prosecute a crime, we will face a "positive conflict of laws" in cyberspace. And this will be a major dilemma as to which country's courts have jurisdiction. The present article examines this issue with the help of analytical-descriptive method and seeks to find out what are the causes of these conflicts and what are the solutions to solve this problem? And whether the establishment of rules in this field is conceivable or should the conflict be resolved by case-by-case instructions.</p>
<p>How To Cite</p>	<p>Baghban, Esmail; Pourgharamani, Babak; Ahadi, Fatemeh (2023). The Relationship between Teachings of the Most Highly Publicist and Doctrine in International Law. <i>Public Law Studies Quarterly</i>, -- (--), 1-19. DOI: https://doi.com/10.22059/JPLSQ.2022.335813.2971</p>
<p>DOI</p>	<p>10.22059/JPLSQ.2022.335813.2971</p>
<p>Publisher</p>	<p>The University of Tehran Press. </p>



راهکار حل تعارض صلاحیت کیفری نسبت به جرائم سایبری

اسماعیل باغبان^۱ | بابک پورقهرمانی^۲ | فاطمه احدی^۳

۱. دانشجوی دکتری تخصصی پژوهش محور رشته حقوق کیفری و جرم‌شناسی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران.

رایانامه: es.baghban@gmail.com

۲. نویسنده مسئول؛ دانشیار، گروه آموزشی حقوق جزا و جرم‌شناسی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران.

رایانامه: b.pourghahramani@yahoo.com۳. استادیار، گروه آموزشی حقوق جزا و جرم‌شناسی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران. رایانامه: ahadi-223@yahoo.com

اطلاعات مقاله	چکیده
نوع مقاله: پژوهشی	تعارض قوانین در فضای سایبر چالشی بسیار اساسی است، چراکه نبود مرزبندی مشخص در این فضا و در نهایت عدم امکان اجرای «صلاحیت سرزمینی» به‌عنوان عامل اساسی در تعیین صلاحیت، به اعمال سایر اصول صلاحیتی در این زمینه منجر می‌شود و زمانی که این مورد در ارتباط با چند کشور مصداق یابد و دو یا چندین کشور مختلف خود را در رسیدگی به جرمی صالح بدانند، ما با «تعارض مثبت قوانین» در فضای سایبری مواجه خواهیم بود و این موضوع که دادگاه‌های کدام کشور صالح به رسیدگی هستند، به‌عنوان معضلی اساسی مطرح خواهد شد. مقاله حاضر با یاری جستن از روش تحلیلی-توصیفی به بررسی این مسئله پرداخته و در جست‌وجوی آن است که عوامل به‌وجودآورنده این تعارضات چیست و چه راهکارهایی برای حل این معضل وجود دارد؟ و آیا ایجاد قواعدی متقن در این زمینه قابل تصور است یا باید تعارض مذکور با دستورالعمل‌های موردی مرتفع شود.
صفحات: ۱۹-۱	
تاریخ دریافت: ۱۴۰۰/۰۹/۲۷	
تاریخ بازنگری: ۱۴۰۰/۱۲/۲۳	
تاریخ پذیرش: ۱۴۰۱/۰۳/۰۱	
تاریخ انتشار برخط: ---/-----	
کلیدواژه‌ها: تعارض قوانین، تعارض مثبت، تعارض منفی، صلاحیت کیفری، ممنوعیت مجازات مضاعف.	
استناد	باغبان، اسماعیل؛ پورقهرمانی، بابک؛ احدی، فاطمه (۱۴۰۲). راهکار حل تعارض صلاحیت کیفری نسبت به جرائم سایبری. <i>مطالعات حقوق عمومی</i> ، -- (۱)، ۱۹-۱. DOI: https://doi.com/10.22059/JPLSQ.2022.335813.2971
DOI	10.22059/JPLSQ.2022.335813.2971
ناشر	مؤسسه انتشارات دانشگاه تهران.



۱. مقدمه

اصطلاح «فضای سایبر»^۱ یا فضای هدایت‌شده، نخستین بار در سال ۱۹۲۸ میلادی در یک داستان علمی-تخیلی به کار برده شد. از آن زمان تاکنون فضای سایبر را به معنای مکانی غیر فیزیکی و مجازی می‌شناسیم که واقعیت‌ها را با عنوان واقعیت مجازی در فضای الکترونیکی بازتاب می‌دهد (مسعودی، ۱۳۸۳: ۱۶). این فضا توهم و تصور باطل توافقی نیست که انسان‌ها خلق کرده‌اند، یک ناحیه واقعی است که فعالیت‌هایی در این فضا اتفاق می‌افتد از جمله تبادل و تجمیع اطلاعات (بای و پورقهرمانی، ۱۳۸۸: ۲۱). در واقع فضای سایبر محیطی است مجازی و غیر ملموس که در فضای شبکه‌های بین‌المللی (که از طریق اینترنت به هم وصل می‌شوند) وجود دارد. در این محیط، تمام اطلاعات مربوط به روابط افراد، ملت‌ها، فرهنگ‌ها، کشورها، به صورت ملموس و فیزیکی (به صورت نوشته، تصویر، صوت و اسناد) در یک فضای مجازی و به شکل دیجیتال وجود داشته و قابل استفاده و در دسترس استفاده‌کنندگان و کاربران است، کاربرانی که از طریق کامپیوتر، اجزای آن و شبکه‌های بین‌المللی به هم مرتبط‌اند (باستانی، ۱۳۸۳: ۵۶). از این تعاریف و ویژگی‌ها به وضوح فهمیده می‌شود که این فضا در واقع محیطی بسیار حساس و فضایی است که قوانین خاص خود را دارد (پورقهرمانی و صابر نژاد، ۱۳۹۲: ۲۹) و در تعریف این فضا نیز چالش‌هایی اساسی وجود دارد و از این رو بعضی مواقع صورت مصداقی تحلیل می‌شود (پورقهرمانی و صابر نژاد، ۱۳۹۲: ۹۵). طرح این مصداق‌ها به تحولات کاربردی منجر شده است و در همین زمینه در دهه ۱۹۹۰ واژه سایبر جایگزین عناوین دیگری مانند فناوری اطلاعات و ارتباطات و حقوق داده‌ورزی شده و مشتقات زیادی از آن مانند «سایبر کافی»^۲ و «سایبر لا»^۳ ساخته است (حسین‌پور و صابر نژاد، ۱۳۹۴: ۳۲).

جرائم این فضا از جنبه‌های مختلف با جرائم سنتی مانند قتل، تجاوز و سرقت متفاوت است. این جرائم را می‌توان از یک مکان دور در خارج از مرزها انجام داد که این امر چالش‌های بیشتری را برای مقامات مجری قانون ایجاد می‌کند. یادگیری نحوه ارتکاب یک جرم سایبری خاص دشوار نیست و ارتکاب آن ممکن است منابع کمی در مقایسه با آسیب احتمالی که می‌تواند ایجاد کند، نیاز داشته باشد و اغلب به وضوح غیرقانونی نیست (Goodman & Brenner, 2002: 142).

هیچ‌گونه تعریف مورد پذیرش عمومی بین‌المللی از جرائم رایانه‌ای، جرائم با فناوری بالا و کلاه‌برداری سایبری وجود ندارد، زیرا معانی متفاوتی برای متخصصان عدالت کیفری در سراسر جهان دارند. بنابراین، به جای تعریف جرائم سایبری، اسناد بین‌المللی اعم از جهانی یا منطقه‌ای در خصوص جرائم سایبری اقداماتی را به عنوان مصداق این جرائم ذکر کرده‌اند. برای مثال کنوانسیون شورای اروپا در

1. Cyber space
2. Cyber Coffee
3. Cyber Law

مورد جرائم سایبری (کنوانسیون بوداپست) این اقدامات را به عنوان جرائم سایبری تلقی کرده است: جرائم علیه تمامیت، محرمانه بودن و در دسترس بودن داده‌ها و سامانه‌های رایانه‌ای که شامل رهگیری غیرقانونی، دسترسی غیرقانونی، تداخل داده‌ها، تداخل سیستم و سوءاستفاده از دستگاه‌ها، جعل مربوط به رایانه؛ کلاه برداری مربوط به رایانه؛ جرائم مربوط به پورنوگرافی کودکان و جرائم مربوط به نقض حق چاپ و حقوق مربوطه (Council of Europe Convention on Cybercrime, 2001, Arts. 2-6).

به دلیل معماری خاص فضای سایبر، هیچ محدودیتی وجود ندارد تا مانع از پراکندگی داده‌های مجرمانه در سراسر گیتی شود. بنابراین این جرائم جنبه فراملی دارند، زیرا مرتکب می‌تواند بدون خروج از خانه آسیب‌های زیادی به قربانیان متعدد در کشورهای مختلف وارد کند. علاوه بر این، تصمیم‌گیری در مورد محل وقوع جرائم رایانه‌ای دشوار است. دلیل این مسئله آن است که فناوری‌های دیجیتالی کنونی به عامل جرم سایبری اجازه می‌دهد نامش فاش نشود، چراکه می‌تواند با ارائه داده‌های نادرست یک حساب ایمیل ایجاد کند، از چندین برنامه پیچیده اینترنتی برای تغییر آدرس IP واقعی استفاده کرده و از فناوری رمزگذاری برای پنهان کردن هرگونه اثری از جرم استفاده کند. همه این چالش‌ها، ردیابی جرائم سایبری را برای مقامات مجری قانون بسیار دشوار و زمان‌بر می‌کند (Clough, 2015: 476). در نتیجه، این‌گونه ویژگی‌های جرائم سایبری، دولت‌ها را ناگزیر می‌سازد که برای مقابله با این جرائم با یکدیگر همکاری کنند. حال اگر در این شرایط جرمی رخ دهد که صلاحیت را در مناطق مختلف درگیر سازد و در واقع محاکم محل‌های متعددی به خاطر معلوم نبودن دقیق محل ارتکاب جرم، خود را صالح به رسیدگی بدانند، موضوع «تعارض قوانین در فضای سایبری»^۱ مطرح می‌شود که می‌تواند در داخل یک کشور و فضای بین‌المللی مصداق یابد که پژوهش حاضر با یاری جستن از روش توصیفی-تحلیلی به بررسی این موضوع می‌پردازد.

۲. جرم سایبری

جرائم سایبری در اصطلاح به جرائمی گفته می‌شود که در محیطی غیرفیزیکی علیه فناوری اطلاعات با حالات شبیه‌سازی و مجازی‌سازی ارتکاب می‌یابد (بیابانی و هادیان‌فر، ۱۳۸۴: ۲۲۵).

امروزه بسیاری از جرائم سنتی، همزمان با پیشرفت فناوری اطلاعات و ارتباطات به شدت متحول شده و به صورت جرائم سایبری هم ارتکاب می‌یابند. عنوان جرائم سایبری نیز به سبب گسترش خود، رفته‌رفته جانشین عباراتی چون جرم‌های رایانه‌ای و جرم‌های اینترنتی می‌شوند. به جرائم سایبر، جرائم علیه فناوری اطلاعات نیز گفته می‌شود (زندى، ۱۳۸۹: ۴۰).

واژه رایانه به گونه‌ای دقیق و جامع نمی‌تواند گستردگی این محیط را نشان دهد، زیرا بسیاری از ابزار

و وسایل امروزی با داده‌هایی کار می‌کنند که اساساً به آنها رایانه اطلاق نمی‌شود. از این رو عبارتهایی مانند جرم‌های رایانه‌ای یا جرم‌های اینترنتی نیز نمی‌توانند به گونه‌ای دقیق جرم‌های ارتكابی مربوط به این حوزه را پوشش دهند. برای نمونه یک سامانه ضبط و پخش الکترونیکی، رایانه نیست؛ اما به طور کلی در زیرمجموعه فضای سایبر قرار می‌گیرد.

در جرائم سایبری، هیچ تأکیدی بر واسطه وجود ندارد. وسایل مختلفی ساخته شده‌اند که هر کدام روش جدیدی را در راه‌یابی به این فضا، بدون نیاز مستقیم به رایانه پدید آورده‌اند، برای مثال تلفن همراه یکی از این وسایل است (زندى، ۱۳۸۹: ۴۱).

۱.۲. تاریخچه جرائم سایبری

جرائم سایبری از زمان پیدایش تانکون، با سه نسل یا تیپ مواجه شده است. دهه‌های ۶۰ و ۷۰ و اوایل ۸۰ زمان حاکمیت نسل اول تحت عنوان جرائم رایانه‌ای است. در این زمان در خصوص جرائم، محوریت بحث با رایانه بود، از این رو تعداد توصیف‌های مجرمانه بسیار کم بود.

به تدریج در دهه ۸۰ تا اوایل دهه ۹۰ نسل دوم به میان آمد. بحث محتوا به کار رفت، یعنی به موضوع جرائم داده و اطلاعات توجه شد. از این رو نسل دوم تحت عنوان جرائم علیه داده‌ها مطرح شد.

پس از چهار یا پنج سال، حاکمیت نسل سوم که از آن به جرائم سایبری یاد می‌کنیم، فرا رسید که ویژگی این نسل، تجمیع رایانه با مودم و مخابرات (اعم از ماهواره) با حالات شبیه‌سازی و مجازی‌سازی است. در این نسل تأکید بر رایانه نیست، بلکه رایانه خود وسیله ارتكاب جرم است.

جرائم نسل سوم در بستر ابر شاهراه‌های الکترونیکی ارتباطی و اطلاعاتی به وقوع می‌پیوندند. اگر در چهار دهه حاکمیت جرائم رایانه، شاهد جرائم انگشت‌شمار بودیم؛ اما در فضای سایبر پنج دسته اصلی جرم وجود دارد که هر کدام بالغ بر چندین عنوان مادر و عمده می‌شوند و شاید تعداد مصادیق عمد و غیرعمد آن بالغ بر ۲۰۰ عنوان مجرمانه شود (شیرزاد، ۱۳۸۸: ۲۳).

اولین جرم سایبری در ایران به سال ۱۳۸۱ و ناظر بر عمل دانشجویان برای اسکن اسکانس و پرینت رنگی از آن عطف شده، اما گزارش‌های غیررسمی حاکی از این است که در دهه ۶۰ تغییر نمرات درسی و تغییر برخی اسامی پذیرفته‌شده در کنکور ۶۴ رخ داده است (زندى، ۱۳۸۹: ۵۰).

۲.۲. ویژگی‌های منحصربه‌فرد جرائم سایبری

جرائم سایبری جزو جرائم ناشی از فناوری مدرن است؛ از این رو دارای ویژگی‌های منحصربه‌فردی است که آن را از جرائم کلاسیک و سنتی جدا می‌کند. در این بخش برخی از این تفاوت‌ها را برمی‌شمایم (زندى، ۱۳۸۹: ۵۷).

۱.۲.۲. زمان ارتکاب جرم

بر خلاف جرائم سنتی که زمان در آن مشهود است، در جرائم سایبری زمان به چند ثانیه یا کسری از ثانیه تبدیل می‌شود.

۲.۲.۲. مکان ارتکاب جرم

مکان نیز در جرائم سایبری به واسطه زیرساخت مخابرات و شبکه‌ای شدن رایانه‌ها و گسترش اینترنت، تغییر یافته است. برای مثال اگر فرد قبلاً برای ارتکاب کلاهبرداری باید مراحل ارتکاب جرم را تکمیل می‌کرد و در تهران موفق به کلاهبرداری می‌شد و در نهایت می‌توانست به اصفهان یا شهر دیگری برود و عمل را تکرار کند؛ اما در کلاهبرداری در فضای سایبر، این تعدد مکانی بیش از حد زیاد می‌شود.

۳.۲.۲. بزه دیده

در حالت سنتی بزه دیده انسان است، به عبارت دیگر، جرم علیه تمامیت جسمی یا روانی شخص و یا علیه اموال اشخاص حقیقی یا حقوقی صورت می‌گیرد. برای مثال در جرائم علیه اشخاص، تمامیت جسمانی و روانی فرد یا اموال او، هدف ارتکاب جرم است؛ اما در جرائم سایبری، در بسیاری موارد، بزه دیده، ماشین است که بیشترین مورد تحقق آن در جرائم الکترونیک و جرائم بانکداری الکترونیک است؛ هرچند که ممکن است نتیجه عمل همان اموال شخص باشد، ولی نکته تمایز هدف‌گیری این موضوع توسط وسیله‌ای به نام فضای سایبری است.

۴.۲.۲. تعداد قربانیان

تعداد قربانی در جرائم کلاسیک، تعدادی خاص و محدودند، درحالی‌که امروز در فضای سایبر، تعداد زیادی قربانی می‌شوند. برای مثال هنگام انتشار یک ویروس، میلیون‌ها سایت و در پی آن میلیون‌ها کاربر، متضرر یا قربانی می‌شوند یا با راه‌اندازی یک وب‌سایت یا ارسال پیام‌های تبلیغاتی فریب‌کارانه به آدرس‌های الکترونیکی کاربران، میلیون‌ها مخاطب فریب می‌خورند (جلالی فراهانی، ۱۳۸۴: ۵).

۳.۲. انواع جرائم سایبری

جرائم سایبر را در چهار دسته یا طبقه کلی می‌توان جای داد:

۲.۳.۱. جرائم کلاسیک با توصیف سایبری

«جرائمی در این دسته قرار می‌گیرند که جرائم سنتی تلقی می‌شوند، اما در حال حاضر به‌علت پیشرفت فناوری، با وسایل نوینی انجام می‌شوند. از جمله این جرائم می‌توان به کلاه‌برداری سایبری، جعل سایبری، تخریب سایبری، جاسوسی سایبری و ... اشاره نمود» (راجی، ۱۳۸۵: ۹۶).

۲.۳.۲. جرائم علیه محرمانه بودن داده‌ها و سامانه‌ها

«هر نمادی از موضوع‌ها، مفاهیم یا دستورالعمل‌ها از جمله متن، صوت یا تصویر را که برای برقراری ارتباط میان سامانه‌های رایانه‌ای با پردازش توسط شخص یا سیستم رایانه‌ای به کار گرفته شده و به‌وسیله سیستم رایانه‌ای ایجاد می‌گردد، داده محتوا گویند. از جمله جرائمی که در این دسته جای می‌گیرند می‌توان به شنود غیرمجاز داده‌های مخابراتی در یک ارتباط خصوصی یا داده‌های سری که واجد ارزش برای امنیت داخلی و خارجی کشور می‌باشند، اشاره کرد» (رضوی، ۱۳۸۶: ۱۲۳).

۲.۳.۳. جرائم علیه صحت و تمامیت داده‌ها و سامانه‌ها

«تغییر، ایجاد، محو یا متوقف کردن رایانه‌ای و مخابراتی به‌قصد تقلب، غیرقابل استفاده کردن، تخریب یا ایجاد اختلال در داده‌ها یا ارسال امواج الکترومغناطیسی، ممانعت از دستیابی اشخاص مجاز به داده‌ها با تغییر رمز ورود و یا رمزنگاری از جمله جرائمی هستند که در این دسته قرار می‌گیرند» (رضوی، ۱۳۸۶: ۱۲۴).

۲.۳.۴. جرائم مرتبط با محتوا

«این دسته جرائمی را تحت شمول خود قرار می‌دهد که در آنها، رایانه به‌عنوان ابزار و وسیله توسط مجرم برای ارتکاب جرم به کار گرفته می‌شود و صرفاً فناوری اطلاعات، زمینه ارتکاب آنها را فراهم می‌سازد. برای مثال انتشار محتویات مستهجن از قبیل نمایش اندام جنسی زن و مرد یا نمایش آمیزش جنسی انسان، تبلیغ یا تحریک یا تشویق به انحرافات جنسی یا خودکشی از طریق سیستم رایانه‌ای یا مخابراتی در این دسته قرار می‌گیرند» (رضوی، ۱۳۸۶: ۱۲۴).

۳. گسترش صلاحیت ملی به فضای فراملی در جرائم سایبری و بروز تعارض

به موازات تحول فناوری در زمینه اطلاعات و رایانه، جهان با پدیده دنیای مجازی به نام فضای سایبر مواجه شده است. از مهم‌ترین مسائلی که باید در این حوزه مورد توجه قرار داد، تعیین تکلیف راجع به چگونگی تعیین مرجع قضایی صالح برای رسیدگی به جرائم ارتکابی در فضای سایبر، یعنی صلاحیت

کیفری مراجع قضایی است. با وجود اختلافات در خصوص محل وقوع جرم و ضابطه تشخیص آن جهت تعیین دادگاه یا دادرسی صالح، مسئله مهمی که در این زمینه به ویژه در دهه های اخیر به وجود آمده است، دشواری تشخیص محل وقوع جرم در فضای سایبر است. چون فضای الکترونیکی و اینترنت با فضای فیزیکی و جغرافیایی ملموس که حقوق سنتی ناظر بر آن است، تفاوت دارد؛ به طوری که این فضا کاملاً غیرملموس و مجازی است و مرز جغرافیایی نمی شناسد. این امر تفاوت صلاحیت مراجع قضایی مختلف در رابطه با آن جرائم در حقوق کیفری را برانگیخته است (عبداللهی و مرادی، ۱۳۹۴: ۴۰) که یکی از راهکارها در این مسیر گسترش صلاحیت ملی به فضایی فراملی در این زمینه است.

در سطح بین المللی، یکی از اهداف اصلی کنوانسیون مبارزه با جرائم سازمان یافته فراملی و سایر کنوانسیون های جرائم سایبری این است که اطمینان حاصل شود که هیچ پناهگاه امنی برای مجرمان وجود ندارد و هر اقدام غیرقانونی مورد دادرسی و قضاوت قرار خواهد گرفت. بنابراین، بیشتر این کنوانسیون ها رویکردی گسترده در رابطه با صلاحیت قضایی ارائه می دهند. برای مثال مطابق ماده ۲۲ کنوانسیون بوداپست، هر دولت عضو آن، قوانین و سایر اقداماتی را که ممکن است برای ایجاد صلاحیت در مورد هر جرم پیش بینی شده در مواد ۲ تا ۱۱ این کنوانسیون لازم باشد، اتخاذ خواهد کرد، هرگاه جرم ارتکاب یافته باشد:

- در قلمرو آن،
- در یک کشتی که پرچم آن عضو را برافراشته است،
- در هواپیمایی که طبق قوانین آن طرف ثبت شده است و
- توسط تبعه دولت عضو در صورتی که جرم مطابق قوانین داخلی در محل ارتکاب جرم قابل مجازات باشد، یا در صورتی که در خارج از حوزه صلاحیت هر دولت ارتکاب یافته باشد.
- نمونه دیگر: طبق ماده ۳۰ «کنوانسیون عربی مبارزه با تخلفات فناوری اطلاعات (کنوانسیون عربی)»^۱، هر دولت عضو متعهد شده است روش های لازم برای گسترش صلاحیت خود به هریک از جرائم مندرج در فصل ۲ کنوانسیون را اتخاذ کند، در صورتی که جرم، به طور جزئی یا کامل، ارتکاب یافته یا محقق شده باشد در:
- قلمرو سرزمینی طرفین،
- یک کشتی که پرچم دولت عضو را برافراشته است،
- هواپیمایی که طبق قانون دولت عضو ثبت شده است،
- توسط تبعه دولت عضو در صورتی که جرم مطابق قوانین داخلی در محل ارتکاب جرم قابل مجازات باشد، یا در صورتی که در حوزه صلاحیت هر دولت ارتکاب یافته باشد،
- اگر جرم بر منافع اصلی دولت تأثیر بگذارد.

1. The Arab Convention on Combating Information Technology Offenses (Arab Convention)

به همین ترتیب، در سطح ملی، چندین کشور با گسترش صلاحیت خود برای رسیدگی به این جرائم به چالش جرائم سایبری بین‌المللی پاسخ داده‌اند (Grabosky, 2004: 147). در قوانین داخلی ایران نیز، در ماده ۶۶۴ قانون آیین دادرسی کیفری ایران در قسمت مربوط به جرائم رایانه‌ای مقرر شده است که علاوه بر موارد پیش‌بینی شده در دیگر قوانین، دادگاه‌های ایران صلاحیت رسیدگی به موارد زیر را دارند:

الف) داده‌های مجرمانه یا داده‌هایی که برای ارتکاب جرم به کار رفته‌اند که به هر نحو در سامانه‌های رایانه‌ای و مخابراتی یا حامل‌های داده موجود در قلمرو حاکمیت زمینی، دریایی و هوایی جمهوری اسلامی ایران ذخیره شود؛

ب) جرم از طریق تارنماهای دارای دامنه مرتبه بالای کد کشوری ایران (IR) ارتکاب یابد؛

ج) 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؛

د) جرائم رایانه‌ای متضمن سوءاستفاده از اشخاص کمتر از هجده سال، اعم از اینکه بزه‌دیده یا مرتکب ایرانی یا غیرایرانی باشد و مرتکب در ایران یافت شود.

همچنین در ماده ۶۶۵ قید شده است:

«چنانچه جرم رایانه‌ای در صلاحیت دادگاه‌های ایران در محلی کشف یا گزارش شود، ولی محل وقوع آن معلوم نباشد، دادرسی محل کشف مکلف است تحقیقات مقدماتی را انجام دهد. در صورتی که محل وقوع جرم مشخص نشود، دادرسی پس از اتمام تحقیقات مبادرت به صدور قرار و در صورت اقتضاء صدور کیفرخواست می‌کند و دادگاه مربوط نیز رأی مقتضی را صادر می‌نماید.»

با بررسی در کنوانسیون‌های مذکور و قوانین کیفری داخلی ایران در خصوص موضوع مذکور، مبرهن و مشخص است که موضوع گسترش صلاحیت ملی در فضای سایبری به‌عنوان رویکردی اساسی برای پایان دادن به بسیاری از تعارض‌های قوانین در این فضا به کار می‌رود و با تعیین تکلیف برای دولتی که جرم بنا بر موارد بیان شده مرتبط با آن است، از ادعای صلاحیت دولت‌های دیگر جلوگیری می‌کند. هرچند که در برخی موارد بر اساس تفسیرهای متفاوت از قلمرو یا تبعه و موارد دیگر، می‌تواند به بروز تعارض منجر شود.

۴. علل بروز تعارض در صلاحیت

رویکرد وسیعی که در بند قبل برای اعمال صلاحیت در مورد جرائم سایبری بیان شد، می‌تواند به وضعیتی منجر شود که دو یا چند کشور بر اساس اعمال ادعاهای قضایی مشابه یا متفاوت در مورد جرم

سایبری، صلاحیت خود را اعلام کنند؛ سپس رسیدگی موازی را برای همان حقایقی آغاز کنند که به «تعارض صلاحیت مثبت»^۱ بین آنها منجر می‌شود.

بر خلاف «تعارض صلاحیتی مثبت»، «تعارض صلاحیتی منفی»^۲ زمانی ممکن است رخ دهد که هیچ کشوری صلاحیت خود را در مورد یک جرم سایبری خاص اعلام نکند. در حقیقت، این وضعیت به دلیل افزایش تعداد موافقت‌نامه‌های بین‌المللی و منطقه‌ای در مورد جرائم سایبری که دولت را ملزم به جرم‌انگاری انواع مختلف جرائم سایبری می‌کند، بسیار نادر است؛ چراکه بیشتر کشورهای جهان در حال حاضر قانونی برای مقابله با جرائم سایبری وضع کرده‌اند (Brenner & Koops, 2004: 40).

یکی از نمونه‌های «تعارض صلاحیتی مثبت» می‌تواند این باشد که یک نفر در ایران و پیروسی خطرناک را در اینترنت پخش کند که سبب ورود آسیب عظیم به بسیاری از اتباع ایران و نهادهای دولتی در چند کشور شود. در این حالت هر کشوری که اتباع یا نهادهای آن درگیر موضوع بوده‌اند صلاحیت خود را برای تحقیق، تعقیب و محاکمه این جنایت طبق مقررات صلاحیت در قوانین داخلی خود اعلام می‌کند. در واقع ایران بر مبنای «صلاحیت سرزمینی»^۳ صلاحیت رسیدگی به این جرم را دارد و کشورهای دیگری که اتباعشان درگیر شده‌اند، بر مبنای «صلاحیت شخصی منفعل»^۴ و کشورهایی که نهادهای آن‌ها زیان دیده‌اند بر مبنای «صلاحیت حمایتی»^۵ صالح به رسیدگی می‌باشند. در این زمان که یک تعارض مثبت بین چند کشور به وجود آمده است، مهم‌ترین و اصلی‌ترین دغدغه راهکاری است که بتواند این چالش را حل کند.

در واقع، دولت‌های طرف چند کنوانسیون بین‌المللی که حاوی شرط صلاحیت گسترده (مذکور در مبحث قبل) برای جلوگیری از بی‌کیفرمانی متهمان است، ناچار با چالش تعارض مثبت مواجه خواهند شد. با وجود این، آنها معتقدند که این وضعیت نادر است و می‌تواند از طریق مذاکره بین دولت‌های مربوط حل شود تا بهترین صلاحیت برای تعقیب موفق و قضاوت در مورد یک پرونده خاص تعیین شود (Clark, 2004: 168). با این حال، در واقع این تعارض به‌عنوان مانع بسیاری از مسائل عملی از جمله همکاری بین‌المللی مؤثر و سریع بین کشورهای رقیب، مطرح می‌شود. این امر به‌ویژه در مورد استرداد و درخواست‌های حقوقی متقابل صادق است، زیرا هریک از دولت‌های ذی‌صلاح، صلاحیت خود را در مورد این جرائم اعلام کرده و صلاحیت دولت‌های دیگر را رد می‌کنند. بنابراین، یک دولت از ارائه کمک‌های خود از طریق کمک حقوقی متقابل یا استرداد خودداری می‌کند. افزون بر این این مسئله پیچیده‌تر

1. positive jurisdictional conflict
2. negative jurisdictional conflict
3. territorial principle
4. passive nationality principle
5. protective principle

می‌شود اگر مرتکب در کشوری باشد که ادعای صلاحیت قضایی ندارد و همه کشورهای مربوطه درخواست استرداد از این کشور را دارند. برای نمونه در مثال پیش گفته، اگر فرد متهم از ایران به ترکیه فرار کند، وضعیتی بسیار بحرانی در مورد اینکه فرد متهم باید به کدام کشور تحویل داده شود، به وجود خواهد آمد. همچنین، این درگیری می‌تواند به نقض اصل «قاعده منع محاکمه و مجازات مضاعف»^۱ منجر شود^۲ که اجازه نمی‌دهد مرتکب ادعایی، بیش از یک بار به خاطر همان عمل مجرمانه تحت تعقیب و مجازات قرار گیرد (Schomburg, 2012: 311-312). علاوه بر این، چنین تعارضی ممکن است موجب تلاش مضاعف یا رقابت بین مقامات مجری قانون کشورهای مربوطه شود که باید از آن اجتناب شود. بنابراین، لازم است با تصمیم‌گیری در مورد این که کدام کشور باید حق انحصاری تعقیب و قضاوت در مورد جرائم سایبری مرتبط را داشته باشد، راه‌حلی برای جلوگیری از طرح دعاوی قضایی همزمان یافته شود (Explanatory Report to the Convention on Cybercrime, 2001: No. 185).

دستیابی به چنین راه‌حلی به چند دلیل کار آسانی نیست:

اولاً، اصل حاکمیت به‌عنوان اصلی شناخته‌شده و به‌شدت مورد حمایت حقوق بین‌الملل و استقلال‌یابی حاضر تأکید دارد که هر دولت صلاحیت خود را بر رفتارهایی که در قلمرو خود، فراتر از آن و سایر رفتارهایی که بر منافع مشروع آن تأثیر می‌گذارد، اعمال کند (Bassiouni, 1974: 2)؛ ثانیاً، حقوق بین‌الملل برابری همه دولت‌های جهان را به رسمیت می‌شناسد و به هیچ‌یک از آنها اقتدار سلسله‌مراتبی بر سایر کشورها را نمی‌دهد (Bassiouni, 1974: 6)؛ ثالثاً، حقوق بین‌الملل عمومی سیستم اولویت‌بندی را در بین پایگاه‌های قضایی مختلف ایجاد نکرده است (Roger & Clark, 2004: 181). و اصول صلاحیت به موجب حقوق بین‌الملل معضل دعاوی قضایی همزمان را حل نمی‌کند.

برخی محققان با در نظر گرفتن اولویت اصل سرزمینی نسبت به سایر ادعاهای صلاحیت، در بین نظریه‌های مختلف صلاحیت سلسله‌مراتبی را پیشنهاد می‌کنند؛ مبنی بر اینکه اول «صلاحیت سرزمینی»، بعد «صلاحیت جهانی»، «صلاحیت حمایتی»، «صلاحیت بر اساس تابعیت بزهکار» و سرانجام «صلاحیت مبتنی بر تابعیت مجنی علیه یا صلاحیت شخصی منفعل». با وجود این آنها تأیید می‌کنند که هنوز هیچ قاعده روشنی وجود ندارد که چنین سلسله‌مراتبی را در مورد دعاوی قضایی همزمان در حقوق بین‌الملل

1. Non bis in idem

۲. اصل «منع دو بار محاکمه یا مجازات یک شخص برای عمل غیرقانونی واحد»، اصل اساسی عدالت کیفری اروپایی و بین‌المللی و همچنین حقوق کیفری ملی است. برای مثال ماده ۱۴(۷) میثاق بین‌المللی حقوق مدنی و سیاسی اشعار می‌دارد که هیچ کس نباید به‌خاطر جرمی که قبلاً در قانون و رویه کیفری هر کشور مورد تعقیب قرار گرفته و در نهایت مطابق آن محکوم یا تبرئه شده است، مجدداً محاکمه یا مجازات شود.

ایجاد کند (Bassiouni, 1974: 60). در مجموع می‌توان گفت که هیچ توافق قطعی در مورد یک راه‌حل مناسب برای «تعارض مثبت صلاحیت» در موارد جرائم سایبری در اسناد بین‌المللی یا در ادبیات حقوقی وجود ندارد، از این رو در مبحث بعدی به بررسی دگترین موجود در این زمینه خواهیم پرداخت.

۵. رویکردهای مختلف در مورد تعارض مثبت صلاحیت

به‌طور کلی، در مورد دعاوی مدنی و تجاری، جامعه بین‌الملل به‌ویژه اتحادیه اروپا، مجموعه کاملی از مقررات مربوط به حوزه قضایی را وضع کرده است که به طرف‌های اختلاف این امکان را می‌دهد که از قبل بدانند آیا یک دادگاه خاص اختیار رسیدگی به پرونده‌ای را که نزد آن مطرح شده است، دارد. ولی در نقطه‌ی مقابل آن و در خصوص جرائم و مسائل کیفری هیچ مجموعه از قوانین مورد توافق وجود ندارد که بتوان بر اساس آن تصمیم گرفت که کدام کشور باید در جرائم در شرایط تعارض مثبت یا حتی در درون سامانه‌های حقوقی سازمان ملل متحد یا اتحادیه اروپا صلاحیت رسیدگی را داشته باشد (Patrone, 2013: 215). با حرکت به سمت جرائم سایبری، همان معضل، هنگامی که بین دو یا چند کشور بر سر صلاحیت اختلاف به‌وجود آید، خودنمایی می‌کند. به‌نظر می‌رسد که دعاوی قضایی همزمان می‌تواند بر همکاری بین‌المللی در مبارزه با جرائم سایبری تأثیر منفی بگذارد و منتهی به نقض «قاعده منع مجازات مضاعف» و سایر پیامدهای جدی شود. با انتخاب بهترین حوزه قضایی به روش شفاف و عینی به‌منظور بهبود همکاری قضایی در امور کیفری، باید از چنین منازعه‌ای به نفع عدالت اجتناب کرد (Mihaela & Ion, 2010: 204). علاوه بر این، دستیابی به یک راه‌حل برای چنین تعارضی در ابتدای رسیدگی کیفری ضروری است، زیرا اینکه قاضی پس از تحقیقات طولانی و پیچیده تصمیم بگیرد که هیچ صلاحیتی در زمینه جرمی خاص ندارد، به‌وضوح کافی نیست. با وجود این هیچ‌گونه توافق قطعی در مورد یک راه‌حل مورد توافق برای تعارض مثبت قضایی وجود ندارد. با نگاهی به ادبیات، سه راه متفاوت برای مقابله با چنین معضلی ارائه شده است:

۵.۱. نظریه همکاری و مشورت برای حل مشکل

این نظریه تأیید می‌کند که حقوق بین‌الملل عمومی سیستمی اولوی را در بین نظریه‌های قضایی مختلف ایجاد نکرده است. بنابراین، برای اجتناب از طرح دعاوی قضایی موازی در دو یا چند کشور، بهترین راه‌حل، مذاکره ثمربخش بین دولت‌های مربوطه به‌منظور تصمیم‌گیری در مورد بهترین حوزه قضایی برای پیگیری موفقیت‌آمیز و قضاوت در مورد پرونده است (Mihaela & Ion, 2010: 217). در حقیقت، چنین موضعی در بسیاری از اسناد بین‌المللی اتخاذ شده است. برای مثال ماده (۱۵) «کنوانسیون مبارزه با جرائم

سازمان یافته فراملی^۱ مقرر می‌دارد، در صورتی که یک دولت عضو که صلاحیت خود را بر اساس بند ۱ یا ۲ این ماده اعمال می‌کند یا در غیر این صورت، مطلع شده باشد که یک یا چند کشور عضو در حال انجام تحقیقات، تعقیب یا رسیدگی قضایی در مورد همان رفتارند، مقامات صلاحیت‌دار کشورهای عضو در صورت لزوم، باید برای هماهنگی اقدامات خود با یکدیگر مشورت کنند. به این ترتیب، این ماده مذاکره و هماهنگی بین کشورهای متعاقد را در صورت تعارض مثبت صلاحیت تشویق می‌کند. همین موضع در ماده ۲۲(۵) کنوانسیون بوداپست پذیرفته و تصریح شده است، هنگامی که بیش از یک طرف مدعی صلاحیت رسیدگی به جرمی است که مطابق این کنوانسیون ایجاد شده است، طرف‌های ذی‌ربط در صورت اقتضا به‌منظور تعیین مناسب‌ترین صلاحیت برای پیگرد مشورت خواهند کرد.

در واقع، طرفداران این دیدگاه ادعا می‌کنند که چنین مذاکره‌ای مزایای بسیاری دارد، زیرا به دولت‌های مربوط اجازه می‌دهد تا محلی واحد را برای رسیدگی‌های حقوقی انتخاب کنند یا به یک دولت اجازه می‌دهد که مجرمانی خاص را تحت تعقیب قرار دهد و دولت دیگری به مجازات گروه دیگری از مجرمان در صورت وجود چنین شرایطی بپردازد، که راه‌حل بسیار مناسبی جهت رسیدگی‌های قانونی به جرم ارتكابی است (Cottim, 2010: 69). علاوه بر این، می‌توان استدلال کرد که چنین مذاکراتی ممکن است به‌صورت طرحی تشویقی، انجام انواع مختلف همکاری‌های بین‌المللی را به‌ویژه در زمینه ایجاد یک گروه تحقیقاتی مشترک بین مقامات کشورهای ذی‌ربط به‌منظور همکاری مؤثر در خصوص جرائم سایبری دارای ماهیت فراملی در زمینه جمع‌آوری شواهد و دستگیری مجرمان را تشویق کند.

علاوه بر این، طرفداران این نظر تأیید می‌کنند که توافق حاصل از مشورت و مذاکره بین کشورهای درگیر، می‌تواند با توسل به مکانیسم انتقال پرونده‌های جنایی که تعقیب در مورد آنها در یک کشور آغاز شده است و در دولتی دیگر انجام می‌شود، به‌صورت قانونی اجرا شود. برای مثال طبق ماده ۳ «کنوانسیون اروپایی انتقال رسیدگی قضایی در امور کیفری»^۲ هر یک از دولت‌های متعاقد که طبق قوانین خود دارای صلاحیت تعقیب یک جرم است، می‌تواند به‌منظور اعمال این کنوانسیون، از رسیدگی علیه شخص مظنون که به‌دلیل همان جرم توسط دولت متعاقد دیگر تحت تعقیب قرار گرفته یا خواهد بود، صرف‌نظر کند یا از انجام آن خودداری ورزد.^۳ البته باید خاطر نشان کرد نظر مذکور که بر مذاکره برای حل این تعارض مبتنی است، معایب بسیاری دارد:

۱. این روش دولت‌های مربوط را تشویق می‌کند تا معضل مربوط به حوزه قضایی را از طریق

1. United Nations Convention Against Transnational Organized Crime

2. European Convention on the Transfer of Proceedings in Criminal Matters

3. Council of Europe, European Convention on the Transfer of Proceedings in Criminal Matters, May. 15, 1972, (entered into force Mar. 30, 1978).

مشورت و توافق متقابل حل کنند که در عمل بدون ارائه دستورالعمل‌های مشخصی به دولت‌ها برای ایجاد مکانیسم اولویت‌بندی دعاوی قضایی که عوامل خاصی را برای تصمیم‌گیری در مورد حل چنین تعارضی در نظر بگیرد، امری تقریباً غیرممکن خواهد بود.

۲. تا زمانی که تعارض بین حوزه‌های قضایی دولت‌ها رایج باشد، مذاکره به احتمال زیاد رضایت‌بخش نخواهد بود، زیرا دولت‌های درگیر را قادر به پیش‌بینی نتیجه نمی‌کند و زمان بر است (Brenner & Koops, 2004: 42).

۳. طبق گزارش توضیحی کنوانسیون بوداپست، مشورت اجباری نیست. بنابراین، اگر دولتی معتقد باشد که مشاوره ممکن است تحقیقات یا روند تحقیقات آن را مختل نموده یا به تأخیر بیندازد، ممکن است از انجام هرگونه مشورت با دولتی دیگر خودداری نماید. لذا از این باب که کنوانسیون بوداپست وسیله مؤثری برای حل تعارض مثبت قضایی احتمالی با تعیین دستورالعمل‌های مشخص و روشن یا ایجاد مکانیسمی برای اولویت‌بندی دعاوی قضایی ایجاد نمی‌کند، مورد انتقاد قرار می‌گیرد (Brenner & Koops, 2004: 45).

پس با توجه به دلایل سه‌گانه مشروح، می‌توان گفت که تنها وابستگی به مذاکره برای حل این معضل مناسب نیست.

۵.۱. ایجاد قاعده‌ای حقوقی

بر خلاف رویکرد قبلی، این نظریه معتقد است که مؤثرترین راه‌حل برای چنین تعارضی، ایجاد یک قاعده آشکار، ملموس و الزام‌آور است که اولویت را بین نظریه‌های قضایی ملی درگیر تعیین کند (Hopkins, 2003: 116). ماده ۳۰(۳) کنوانسیون اتحادیه عرب چنین موضعی را دنبال کرده و در آن اولویت صریح برای دعاوی قضایی موازی به شرح زیر پیش‌بینی شده است:

۱. دولتی که امنیت یا منافع آن بر اثر جرم مختل شده است؛

۲. دولتی که جرم در قلمرو آنها ارتکاب یافته است؛

۳. دولتی که شخص مورد تقاضای استرداد تابعیت آن را دارد؛

۴. در صورت وجود شرایط مشابه، اولویت با اولین دولتی خواهد بود که درخواست استرداد کرده است» (The Arab Convention on Combating Information Technology Offenses, 2010, art. 30(3)).

همچنین ماده ۱۰ تصمیم «چارچوب شورای اتحادیه اروپا در مورد حملات علیه سامانه‌های اطلاعاتی»^۱ مصوب ۲۰۰۵، به هر دولت عضو اجازه می‌دهد که در صورت ارتکاب جرم: ۱. به‌طور کامل یا جزئی در قلمرو آن، ۲. توسط یکی از اتباعش، ۳. یا به نفع یک شخص حقوقی که دفتر مرکزی آن در قلمرو آن واقع است یا علیه یک سیستم اطلاعاتی در قلمرو آن ارتکاب یافته باشد. در حالت نخست، هر

1. EU Council Framework Decision 2005/222/JHA, art. 10/4, 2005 O.J. (L 69/67)

دولت عضو هنگام احراز صلاحیت خود، باید اطمینان حاصل کند که مجرم در هنگام ارتکاب جرم در سرزمینش حضور فیزیکی داشته است. در مورد دعاوی قضایی همزمان، دولت‌های مربوط باید برای متمرکز کردن رسیدگی در یک کشور همکاری کنند. در همین زمینه طرفین می‌توانند برای تسهیل همکاری قضایی خود به یک نهاد یا مکانیزمی در اتحادیه اروپا مراجعه کنند که در این صورت اعطای صلاحیت به ترتیب به کشوری که جرم در آنجا واقع شده، دولت متبوع مرتکب جرم و در نهایت محلی که مجرم یافت شده است، خواهد بود.

این رویکرد در مرحله عملیاتی مورد انتقاد قرار می‌گیرد، زیرا ایجاد سلسله مراتب در بین حوزه‌های قضایی مختلف کار ساده‌ای نیست. علاوه بر این، چنین قاعده‌ای بسیار سفت‌وسخت بوده و نمی‌تواند با شرایط و ویژگی‌های هر مورد مطابقت داشته باشد. تعیین اینکه کدام حوزه قضایی بهترین محل برای تحقیق و تعقیب است باید بر اساس حقایق و شرایط هر پرونده باشد. بنابراین، این رویکرد برای تصمیم‌گیری در مورد بهترین حوزه قضایی برای محاکمه کافی نیست و برای همه گونه‌های جرائم سایبری کارایی نخواهد داشت. باید توجه داشت که بین دولت‌های مختلف، نیل به توافقی جامع برای قاعده‌سازی در فضای مذکور با چالشی اساسی روبه‌رو خواهد بود؛ از طرف دیگر، در فضای وستفالیایی کنونی حاکم بر روابط بین‌المللی که با وجود حدوث برخی تحولات هنوز دولت‌ها حاکمیت خود را «هیولایی»^۱ مصون از انتقاد می‌دانند، انتظار التزام به قاعده تحمیلی حقوقی خواسته‌ای بیهوده خواهد بود.

۵.۳. ارائه دستورالعمل‌های موردی

بر اساس رویکرد سوم، وجود یک دستورالعملی که عوامل خاصی را برای تصمیم‌گیری در مورد تعارض مثبت صلاحیت بین کشورها در نظر بگیرد، لازم است. علاوه بر این، حامیان این نظریه معتقدند که عوامل مذکور باید غیر حصری بوده و بسته به مورد دعوا باید عاملی که منطقی‌تر است و به دولت‌ها امکان حل اختلاف در صلاحیت را می‌دهد، برگزیده شود.

در مرحله عمل «واحد همکاری قضایی اتحادیه اروپا»^۲ چنین نظری را در ماده ۷ تصویب‌نامه سال ۲۰۰۹ خویش، درج کرده و مقرر می‌دارد در صورتی که دو یا چند عضو ملی نتوانند در مورد چگونگی حل پرونده تعارض صلاحیت در زمینه انجام تحقیقات یا تعقیب، توافق کنند؛ از «واحد همکاری قضایی اتحادیه اروپا» خواسته می‌شود که در مورد این پرونده به کشورهای عضو مربوطه نظر کتبی غیرالزام‌آور

۱. استفاده از واژه مذکور وامداری از نظریه توماس هابز در کتاب لویاتان (Leviathan) است که در ۱۶۵۱ به زبان انگلیسی در لندن انتشار یافت.

۲. European Union's Judicial Cooperation Unit (Eurojust)

ارائه کند.^۱ به همین منظور، در سال ۲۰۱۶، نظرهای واحد همکاری قضایی اتحادیه اروپا برای تصمیم‌گیری در مورد اینکه کدام حوزه قضایی باید تعقیب کند - به منظور تلاش برای سازماندهی موضوع دعوی قضایی همزمان در اروپا - اعلام شد. این اعلام تأکیدی بود بر اینکه عواملی باید هنگام صدور دستورالعمل تعیین حوزه قضایی صالح در نظر گرفته شود.^۲ این عوامل عبارت‌اند از:

- قلمرو سرزمینی،
 - موقعیت شخص متهم،
 - در دسترس بودن و پذیرفتن شواهد،
 - اخذ شواهد از شهود، کارشناسان و قربانیان،
 - حمایت از شهود،
 - مراحل رسیدگی و طول مدت آن،
 - الزامات قانونی، اختیارات مجازات، عواید ناشی از جرم و هزینه‌های آن.
- البته شایان ذکر است که اولویت و ارزشی که به هر یک از این عوامل، با توجه به مزایای هر مورد متفاوت است.

بی تردید باید ضرورت‌ها و ویژگی‌های هر مورد به‌طور خاص و جداگانه سنجیده شود تا راهکار موردی ارائه شده دارای آستانه پذیرشی که دولت‌ها خود را ملزم به اجرای آن بدانند باشد؛ چراکه در غیر این صورت دستورالعمل ابلاغی با مشکل نافرمانی طرف یا طرفین درگیر تعارض صلاحیت قرار می‌گیرد و در مرحله عملیاتی، اقبالی در حل معضل به‌وجودآمده نخواهد داشت.

۶. نتیجه

با توجه به آنچه گفته شد، اینترنت از مهم‌ترین نوآوری‌های فناورانه در سال‌های اخیر بوده است که تأثیر مثبت زیادی بر ارتباطات، معاملات مالی و عملکرد ده‌ها مؤسسه در سراسر جهان دارد. با این حال، چنین توسعه‌ای در استفاده از اینترنت و فناوری‌های رایانه‌ای، امکان سوءاستفاده از آنها را با ارتکاب اشکال مختلف جرائم سایبری مانند انتشار ویروس‌ها و همچنین دسترسی غیرمجاز و دستکاری غیرقانونی در سامانه‌ها، برنامه‌ها یا داده‌ها افزایش داده است. علاوه بر این، جرائم سنتی مانند کلاه‌برداری، جعل و سرقت را می‌توان با کمک رایانه‌ها، اینترنت و فناوری‌های ارتباطی مرتبط انجام داد. ابعاد فرامرزی جرائم سایبری به اتخاذ رویکردی گسترده در زمینه اعمال صلاحیت به‌عنوان روشی

1. EU Council Framework Decision 2009/426/JHA, art. 7(2), 2009 O.J. (L 138/14).

2. See: https://www.eurojust.europa.eu/sites/default/files/Publications/Reports/2016_Jurisdiction-Guidelines_EN.pdf

برای مقابله با این گونه جنایات فراسرزمینی منجر شده است. بنابراین، صلاحیت رسیدگی به جرائم سایبری را می‌توان بر اساس چندین عامل شامل صلاحیت سرزمینی، تابعیت فعال، تابعیت منفعل و اصول حمایتی مشخص کرد. چنین رویکرد وسیعی ممکن است به معضل «تعارض مثبت صلاحیت» در مورد حوزه قضایی منجر شود که ممکن است به سهم خود مانعی برای همکاری بین‌المللی مؤثر و نقض اصل اساسی «قاعده منع مجازات مضاعف» باشد.

امروزه سه رویکرد متفاوت برای حل تعارض صلاحیت قضایی وجود دارد:

۱. نظر اول طرفدار مذاکره بین دولت‌های مربوطه با هدف متمرکز کردن روند کیفری در یک کشور

واحد است؛

۲. دیدگاه دوم ایجاد یک قانون واضح و الزام‌آور را ترجیح می‌دهد که اولویت را در بین دعاوی

قضایی رقیب تعیین می‌کند؛

۳. نظر سوم از ارائه دستورالعملی پشتیبانی می‌کند که شامل عوامل غیرحصری است که باید در نظر

گرفته و ارزیابی شوند، تا بتوان به این موضوع رسیدگی کرد.

برای هریک از نظریه‌های مشروح می‌توان شرایط و انتقادهایی را مطرح کرد. در بحث مشورت و همکاری برای نیل به راهکار حل تعارض، دشواری نیل به همکاری با عطف به تعارض منافع و ضرورت توجه به نهادینه کردن این همکاری جلوه‌گری می‌کند. در خصوص ایجاد قواعد حقوقی نیز باید دشواری نیل به قاعده‌ای که بتواند مورد الزام و پذیرش حاکمیت‌های درگیر تعارض باشد، مدنظر باشد. در نهایت امر در خصوص ارائه دستورالعمل‌های موردی نیز توجه به این نکته که باید ارائه هر راهکار خاص، بر اساس توجه به ویژگی‌های موضوع و تأثیرگذاری جرم ارتكابی بر طرفین باشد، ضروری و اجتناب‌ناپذیر است.

با در نظر گرفتن همین عوامل و تحلیل این رویکردها می‌توان گفت که مؤثرترین راه‌حل، تعیین عوامل خاصی است که باید مورد توجه و ارزیابی قرار گیرند تا بهترین حوزه قضایی برای اعمال صلاحیت انحصاری در مورد جرائم سایبری با توجه به حقایق و شایستگی‌های هر مورد و با در نظر گرفتن موارد فراملی تعیین شود. این راه‌حل پیشنهادی بهتر از تلاش برای حل چنین مناقشه‌ای از طریق مذاکره بین دولت‌های مربوطه بدون ارائه عوامل تعیین شده در آنها برای تصمیم‌گیری در این زمینه است. بنابراین، رویکرد پیشنهادی باید شامل منافع قربانی(ها)، مرتکب(ها)، دولت محل ارتکاب جرم، وضعیت ملیت مجرم، وضعیت ملیت قربانی و کشوری که منافع حیاتی آن تحت تأثیر جرم قرار گرفته است، باشد و منافع رسیدگی‌های کیفری برای دستیابی به منافع همه ذینفعان ضروری تلقی شود. علاوه بر این، این عوامل باید غیرحصری باشند تا به دولت‌هایی درگیر صلاحیت معارض، توانایی پیش‌بینی در تعیین صلاحیت را ارائه کند تا شاید موضوع تعیین صلاحیت قضایی به معضل تبدیل نشود.

در خاتمه باید توجه داشت که بر اساس توازن مجموع همه این عوامل تصمیم گرفته شده و

صلاحیت به کشوری داده شود که توانایی برآورده کردن بسیاری از این عوامل را داشته باشد. این تصمیم می‌تواند توسط خود دولت‌های ذی‌ربط یا نهادی بین‌المللی که بر اساس سندی بین‌المللی تأسیس شده و مأموریت اجباری برای صدور دستورالعمل موردی لازم‌الاجرا در مورد اختلاف بین دولت‌ها بر سر صلاحیت در جرائم سایبری دارد، اتخاذ شود.

منابع

۱. فارسی

الف) کتاب‌ها

۱. باستانی، برومند (۱۳۸۳). جرائم کامپیوتری و اینترنتی، جلوه‌ای نوین از بزهکاری. بهنامی.
۲. بای، حسین علی و پورقهرمانی، بابک (۱۳۸۸). بررسی فقهی و حقوقی جرائم رایانه‌ای. تهران: پژوهشگاه علوم و فرهنگ اسلامی.
۳. بیابانی، غلامحسین و هادیان‌فر، سیدرضا (۱۳۸۴). فرهنگ توصیفی علوم جنایی. انتشارات مرکز تحقیقات کاربردی کشف جرائم و امنیت معاونت آگاهی ناجا.
۴. پورقهرمانی، بابک و صابرزاد، علی (۱۳۹۳). حریم خصوصی در فضای سایبر از منظر حقوق بین‌الملل. تهران: مجد.
۵. حسین پور، پری و صابرزاد، علی (۱۳۹۴). آزادی اطلاعات در فضای سایبر از منظر حقوق بین‌الملل. تهران: مجد.
۶. عزندی، محمدرضا (۱۳۸۹). تحقیقات مقدماتی در جرائم سایبری. تهران: جنگل.
۷. شیرزاد، کامران (۱۳۸۸). جرائم رایانه‌ای. بهینه فراگیر.
۸. مسعودی، امیر (۱۳۸۳). امنیت اطلاعات در فضای سایبر. نشریه کتاب ماه.

ب) مقالات

۹. پورقهرمانی، بابک و صابرزاد، علی (۱۳۹۲). ضرورت تدوین قواعد بین‌المللی برای مبارزه با جنگ سایبری. چهارمین همایش مجازی بین‌المللی تحولات ایران و جهان. قزوین، فروردین.
۱۰. جلالی فراهانی، امیرحسین (۱۳۸۴). اسپم، جلوه سیاه تبلیغات در سیستم‌های پیام‌رسان الکترونیکی. مرکز پژوهش‌های مجلس شورای اسلامی، ۸۴۵۱.
۱۱. راجی، سیدمحمدهادی (۱۳۸۵). نگاهی به قانون تجارت الکترونیک. فصلنامه نشریه حقوقی گواه، (۶-۷)، ۶۵-۶۹.
۱۲. رضوی، محمد (۱۳۸۶). جرائم سایبری و نقش پلیس در پیشگیری از این جرائم و کشف آنها. فصلنامه دانش انتظامی، (۳۲)، ۱۲۰-۱۴۰.
۱۳. عبدالحی، اسماعیل و مرادی، سکینه (۱۳۹۴). صلاحیت کیفری در فضای سایبری. فصلنامه علمی دانش انتظامی بوشهر، (۲۰)، ۴۰-۵۹.

۲. انگلیسی

A) Books

1. Clough, J. (2011). *Principles of Cybercrime*. London:Cambridge University Press. 2nd edition.
2. Clark, R. S. (2004). *The United Nations Convention against Transnational Organized Crime*. Wayne L. Rev.

B) Articles

3. Bassiouni, M. C. (1974). Theories of Jurisdiction and Their Application in Extradition Law and Practice. *International Law Journal*, 5(2), 1-61.
4. Brenner, S. W., Koops, J. (2004). Approaches to Cybercrime Jurisdiction. *Journal of High Technology Law*, IV (1), 1-46.
5. Cottim, A. A. (2010). Cybercrime, Cyber terrorism and Jurisdiction: An Analysis of Article 22 of the COE Convention on Cybercrime. *European Journal of Legal Studies*, 2(3), 56-71.
6. Goodman, M.D., Brenner, S.W. (2002).The Emerging Consensus on Criminal Conduct in Cyberspace. *International Journal of Law and Information Technology*, 10(2), 139-153.
7. Grabosky, P. (2004). The Global Dimension of Cybercrime. *Global Crime*, 6(1), 146-157.
8. Hopkins, S. L. (2003). Cybercrime Convention: A Positive Beginning to a Long Road Ahead. *Journal of High Technology Law*, 2(1),101-122.
9. Mihaela, A., Ion, Flamanzeanu(2010). Analysis Conflicts of Jurisdiction in Criminal Proceedings to the European Union Legal Framework. *Agora international journal of juridical sciences*, 4(2), 201-219.
10. Patrone, I. (2013). Conflicts of jurisdiction and judicial cooperation instruments: Eurojust's role. *ERA Forum*, 14(2), 215-225.
11. Schomburg Wolfgang (2012).Criminal matters: transnational ne bis in idem in Europe—conflict of jurisdictions—transfer of proceedings. *ERA Forum*, 13(3), 311 -324.

C) Documents

12. *Council of Europe, Explanatory Report to the Convention on Cybercrime* (2001).
13. *EU Council Framework Decision 2005/222/JHA*, art. 10/4, 2005 O.J. (L 69/67).
14. *EU Council Framework Decision 2009/426/JHA*, art. 7/2, 2009 O.J. (L 138/14).
15. *United Nation Office on Drugs and Crime, Comprehensive Study on Cybercrime*. xvii, (February 2013).

References in Persian:**A) Books**

1. Bastani, B. (2003) .*computer and Internet crimes, a new manifestation of delinquency* . Tehran: Behnam Publications ([In Persian](#)).
2. Bay, H. A., & Pourghahramani, B. (2008) .*jurisprudence and legal review of computer crimes* .Tehran: Research Institute of Islamic Sciences and Culture ([In Persian](#)).
3. Biabani, G., & Hadian Far, S. R. (2004) .*Descriptive Dictionary of Criminal Sciences* . Tehran: Publications of the Applied Research Center for Crime Detection and Security of the Naja Intelligence Agency ([In Persian](#)).
4. Hosseinpour, P., & Sabernejad, A. (2014) .*Freedom of Information in Cyber Space from the Perspective of International Law* .Tehran: Majd Publications ([In Persian](#)).
5. Masoudi, A. (2003) .*Information security in cyber space* .Tehran: Kitab Mah publication ([In Persian](#)).
6. Pourghahramani, Babak and Sabernejad, Ali (2013) .*privacy in cyberspace from the perspective of international law*, Tehran: Majd Publishing House ([In Persian](#)).
7. Shirzad, K. (2008) .*Computer Crimes* .Tehran: Behineh Faragir Publishing ([In Persian](#)).
8. Zandi, M. R. (2009) .*preliminary research in cyber crimes* .Tehran: Jungle Publications ([In Persian](#)).

B) Articles

9. Abdolahi, Esmail and Moradi, Sakineh (2014). Criminal Jurisdiction in Cyber Space.*Bushehr Police Science Quarterly*, 6(20), 40-59 ([In Persian](#)).
10. Jalali Farahani, Amirhossein (2004).Spam, the black effect of advertising in electronic messaging systems .*Research Center of the Islamic Council*, No. 8451 ([In Persian](#)).
11. Pourghahramani, B., & Sabernejad, A. (2012).The necessity of developing international law to fight against cyber war .*4th International Virtual Conference on Iran and World Developments* .Qazvin :Farvardin ([In Persian](#)).
12. Raji, S. M. H. (2006).Looking at the Law of Electronic Commerce .*Gowah Legal Journal Quarterly* .6-7, 65-69 ([In Persian](#)).
13. Razavi, M. (2016).Cybercrimes and the role of the police in preventing these crimes and detecting them. *Police Science Quarterly*. 32, 120-140 ([In Persian](#)).