

The Challenge of the Conflict of Criminal Jurisdiction in Cybercrimes and Its Solution in the Judicial Procedure of the United States of America

Esmail Baghban

Ph.D Student in Criminal Law and Criminology, Maragheh Branch, Islamic Azad University, Maragheh, Iran.

Babak Pourghahramani*

Associate Professor, Department of Criminal Law and Criminology, Maragheh Branch, Islamic Azad University, Maragheh, Iran. (Corresponding author).

Email: b.pourghahramani@yahoo.com

Fatemeh Ahadi

Associate Professor, Department of Criminal Law and Criminology, Maragheh Branch, Islamic Azad University, Maragheh, Iran.

Keywords:

Judicial Procedure,
Cyberspace,
Conflict of
Jurisdiction,
Minimum Contact
Principle,
Purposeful
Direction
,Principle of
Foreseeability,
United States of
America

Abstract

Abstract text The conflict of criminal jurisdiction in cyber crimes is a very fundamental challenge; Because the lack of clear demarcation in this space and ultimately the impossibility of implementing "territorial jurisdiction" as a basic factor in determining jurisdiction, leads to the application of other jurisdictional principles in this field, And when this case is proven in connection with multiple jurisdictions and two or more different courts consider themselves competent in dealing with a crime, we will face a "conflict of criminal jurisdiction" in the cyberspace; which leads to a conflict of jurisdiction in the courts of a country or in the international area. In response to these conflicts, the judicial system of the United States of America has put its approach to the use of traditional legal rules in this field and in line with the use of the criteria of " Minimum Contact Principle", " Purposeful Direction " and " Principle of Foreseeability" to solve this conflict; which has faced major challenges in the operational phase. With the help of the descriptive-analytical method, the present article examines the challenge of the conflict of cyber laws and its solution in the judicial procedure of the United States of America; that the findings of the research show the ineffectiveness of traditional rules in this field; In this regard, the need to change the attitude and apply the special rules of the cyber space and achieve the approach of " Res Extra Commercium " in this space seems inevitable.



This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license:

<http://creativecommons.org/licenses/by/4.0/>

چالش تعارض صلاحیت کیفری در جرایم سایبری و راهکار آن در

رویه قضایی ایالات متحده آمریکا

اسماعیل باغبان

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

بابک پورقهرمانی

دانشیار، گروه آموزشی حقوق جزا و جرم شناسی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران.
نویسنده مسئول) ایران. پست الکترونیک: b.pourghahramani@yahoo.com

فاطمه احدی

دانشیار، گروه آموزشی حقوق جزا و جرم شناسی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران.

تاریخ پذیرش: ۹ اردیبهشت ماه ۱۴۰۲

تاریخ دریافت: ۷ بهمن ماه ۱۴۰۱

چکیده

تعارض صلاحیت کیفری در جرایم سایبری چالشی بسیار اساسی است؛ چراکه نبود مرزبندی مشخص در این فضا و نهایتاً عدم امکان اجرای «صلاحیت سرزمینی» به عنوان عامل اساسی در تعیین صلاحیت، منجر به اعمال سایر اصول صلاحیتی در این زمینه می‌گردد و زمانی که این مورد در ارتباط با چند حوزه قضایی مصداق یابد و دو یا چندین محکمه مختلف خود را در رسیدگی به جرمی صالح بدانند، ما با «تعارض صلاحیت کیفری» در فضای سایبری مواجه خواهیم بود؛ که منجر به تعارض صلاحیت در محاکم داخل یک کشور یا عرصه بین‌المللی می‌گردد. نظام قضایی ایالات متحده آمریکا در واکنش به این تعارض، رویکرد خود را به استفاده از قواعد سنتی حقوقی در این زمینه قرار داده و در راستای استفاده از معیارهای «ارتباط حداقلی»، «بهره‌مندی هدفمند» و «ضابطه پیش‌بینی پذیری» برای حل این تعارض بوده است؛ که در مرحله‌ی عملیاتی با چالش‌هایی اساسی مواجه شده است. مقاله‌ی حاضر با یاری جستن از روش توصیفی-تحلیلی به بررسی چالش تعارض قوانین سایبری و راهکار آن در رویه‌ی قضایی ایالات متحده آمریکا پرداخته؛ که یافته‌های آن نشان از عدم کارایی قواعد سنتی در این زمینه دارد؛ در همین راستا ضرورت تغییر نگرش و اعمال قواعد خاص فضای سایبر و نیل به رویکرد «منطقه بدون اعمال حاکمیت ملی» در این فضا اجتناب‌ناپذیر به نظر می‌رسد.

واژگان کلیدی: رویه قضایی، فضای سایبر، تعارض صلاحیت، ارتباط حداقلی، بهره‌مندی هدفمند، اصل پیش‌بینی پذیری، ایالات متحده آمریکا

مقدمه

متن فضای سایبر به‌عنوان محیطی بسیار حساس به افراد اجازه می‌دهد تا بدون افشای هویت خود و حتی عدم اطلاع از موقعیت مکانی طرف مقابل، تراکنش‌ها را انجام دهند (Farooq, 2004: 408). بی‌تردید یک فرد ممکن است در هر گوشه از دنیا بنشیند و حقوق طرف یا شخص دیگر را زیر پا بگذارد، لذا پارادایم صلاحیت قضایی در حقوق بین‌الملل و قوانین ملی به دلیل ماهیت خاص، استفاده روزافزون و نیاز فضای سایبری که قوانین خاص خود را می‌طلبد (پور قهرمانی، صابر نژاد: ۱۳۹۳: ۲۹)، لازم است تغییر نماید. به دلیل معماری خاص فضای سایبر، هیچ محدودیتی وجود ندارد تا مانع از پراکندگی داده‌های مجرمانه در سراسر گیتی گردد؛ 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 امر آن است که فناوری‌های دیجیتالی کنونی به عامل جرم سایبری اجازه می‌دهد هویتش فاش نشود، چراکه می‌تواند با ارائه داده‌های نادرست یک حساب ایمیل ایجاد کند، از چندین برنامه پیچیده اینترنتی برای تغییر آدرس IP واقعی استفاده نموده 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 می‌نماید (Clough, 2015: 476). در نتیجه، این‌گونه ویژگی‌های جرائم سایبری، دولت‌ها را ناگزیر می‌سازد که برای مقابله با این جرائم با یکدیگر همکاری نمایند. حال اگر در این شرایط جرمی رخ دهد که صلاحیت را در کشورهای مختلف درگیر نماید و در واقع محاکم محل‌های متعددی به خاطر معلوم نبودن دقیق محل ارتکاب جرم، خود را صالح به رسیدگی بدانند موضوع «تعارض صلاحیت کیفری» مطرح می‌گردد که می‌تواند در داخل یک کشور و فضای بین‌المللی مصداق یابد.

دولت نمی‌تواند صلاحیت قضایی را در مورد افراد، رویدادها و چیزهایی که به‌طور فیزیکی در قلمرو کشور دیگری واقع شده‌اند اعمال کند، لذا با توجه به ماهیت فضای سایبر در بسیاری از موارد که طرفین یک تراکنش اینترنتی با ادعاهای همپوشانی و اغلب تناقض در اعمال قانون ملی روبرو می‌شوند، چالشی اساسی به وجود می‌آید. مشکل صلاحیت‌های متعدد و همپوشانی، به این دلیل برجسته‌تر است که دادگاه‌های ملی اصول مساعد را خارج از اصول موجود حقوق بین‌الملل به کار برده‌اند یا اصول جدیدی را برای احراز صلاحیت ایجاد کرده‌اند. اگرچه با توجه به معیارهای مورد بحث تعیین مرجع قضایی صالح به رسیدگی جرایم سایبری به نحوی از انحاء محقق 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 قابل‌رسیدگی 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 به‌طور جدی مورد امعان نظر قرار گیرد (رضوی فرد، موسوی، ۱۳۹۶: ۸۳).

در تحلیل صلاحیت قضایی در فضای سایبر باید به این موضوع پرداخته شود که آیا یک رویداد خاص در فضای مجازی توسط قوانین ایالت یا کشوری که وبسایت در آن قرار دارد کنترل می‌شود یا توسط قوانین ایالت یا کشوری که ارائه‌دهنده خدمات اینترنتی و یا هر دو مورد آن. در ایالات متحده تعدادی از حقوقدان و متخصصان این تئوری را مطرح نموده‌اند که فضای مجازی باید به‌عنوان یک حوزه قضایی یا قلمرو جداگانه تلقی شود؛ اما این دیدگاه در عمل مورد حمایت دادگاه‌ها قرار نگرفته و قانون‌گذاران هم اقبالی به آن نشان نداده است. هدف مقاله‌ی حاضر تحلیل چگونگی ایجاد تعارض در صلاحیت کیفری جرایم سایبری و تدقیق در راهکار رویه‌ی قضایی ایالات متحده آمریکا در این باب است که موضوع از منظر بررسی رویه‌ی کشور مذکور در این باب بسیار بدیع بوده و در ادبیات حقوقی ایران مورد مذاقه قرار نگرفته است. سؤال اساسی پژوهش حاضر نیز تحلیل این مبحث است که قواعد اعمال صلاحیت در فضای سایبر در ایالات متحده آمریکا به چه نحوی است و راهکار آن در خصوص تعارض صلاحیت احتمالی چیست؟ که با یاری جستن از روش توصیفی - تحلیلی در راستای پاسخگویی به آن هستیم.

۱. چالش اعمال صلاحیت در فضای سایبر

یکی از مسائل جدیدی که به موازات تحول و پیشرفت تکنولوژی در زمینه فناوری اطلاعات و ارتباطات به وجود آمده است مسأله چگونگی تعیین مرجع قضایی صالح جهت فضای سایبر، ایجاد دنیای مجازی جدید به نام رسیدگی به جرائم ارتكابی در فضای مذکور است. براساس قواعد سنتی مهم‌ترین ضابطه تعیین صلاحیت مراجع قضایی کیفری، مکان وقوع جرم می‌باشد و در فضای جدید سایبر که یک فضایی مجازی و فارغ از مکان می‌باشد، چنین ضابطه‌ای قابل اجرا نبوده و یا مستلزم تعدیل ویژه می‌باشد. در همین راستا برخی سعی کرده‌اند همان قواعد سنتی ناظر بر صلاحیت کیفری مراجع قضایی را با نگرشی جدید در این فضا اجرا کنند و برخی دیگر با طرح تئوری‌های نو در خصوص صلاحیت، از قبیل «فضای سایبر به‌عنوان یک فضای آزاد بین‌المللی» و یا پیش‌بینی دادگاهی ویژه به نام «دادگاه دیجیتالی یا سایبری» و یا صلاحیت «دادگاه ذی ارتباط منطقی با جرم» را مطرح کرده‌اند (امینی‌نیا، علیزاده، ۱۳۹۷: ۲۱). علی‌رغم وجود اختلافات در خصوص محل وقوع جرم و ضابطه تشخیص آن جهت تعیین دادگاه یا دادسرای صالح، مسئله‌ی مهمی که در این زمینه به‌ویژه در دهه‌های 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 به آن است تفاوت دارد؛ به طوری که این فضا کاملاً غیرملموس و مجازی است و مرز جغرافیایی نمی‌شناسد. این امر مسئله تفاوت صلاحیت مراجع قضایی مختلف در رابطه با آن جرائم در حقوق کیفری را مطرح کرده است (عبدالهی، مرادی، ۱۳۹۴: ۴۰).

درواقع امر با فراگیر شدن اینترنت، افراد و سازمان‌ها صرف‌نظر از مکانشان، به یکدیگر نزدیک‌تر شده‌اند. علی‌رغم مزایای آشکار این فضا که ما را قادر ساخته است رشد سریع اقتصاد جهان را شاهد باشیم، شاهد جنبه‌های تاریک اینترنت و پیامدهای منفی تأثیر اینترنت بر انسان نیز هستیم. در فضای موجود، جریان اطلاعات و ارتباطات محدود به مرزهای جغرافیایی و دولتی نیست و این وضعیت مملو از خطر سلب امنیت برای دولت و جامعه است. ظهور انواع جدید جرائم و ارتكاب جرائم سنتی به روش‌های جدید، نتیجه ورود گسترده فناوری اطلاعات به زندگی ماست. نیاز به مقررات قانونی در فضای مجازی واضح است، باین‌حال، ماهیت فرامرزی، از راه دور و غیر شفاف بودن آن، مشکلات خاصی را ایجاد می‌نماید (Schmitt, 2017: 215). مشکل اصلی در این وضعیت پیدا کردن قوانین صلاحیتی مناسب با رهیافتی پاسخگو در فضای مذکور است. درواقع مشکل مقررات فضای سایبری در این واقعیت نهفته است که صلاحیت دولت‌ها مبتنی بر رویکرد سرزمینی است، درحالی‌که احتمالاً باید در خصوص این فضا، مقررات بین‌المللی یا به‌طور دقیق‌تر، مقررات حقوقی جهانی فضای سایبری باشد. از این گذشته، همه ما علاقه‌مند به قوانین مؤثری هستیم که بتواند روابط حقوقی را که فراتر از قوانین یک کشور است تنظیم کند و به دلیل ویژگی‌های این فضا است که می‌تواند هم‌زمان منافع مختلف چندین کشور را به‌صورت جهانی در برگیرد.

یکی از ویژگی‌های فضای سایبر که آن را از دنیای واقعی متمایز و محاکم را با مشکلات اساسی روبرو نمی‌نماید، ناشناس بودن - ناپیدا بودن - کاربر است که مشکل شناسایی و محرمانگی از آن ناشی می‌شود. به‌عنوان مثال، تلاش برای منطقه بندی فضا بر اساس محدودیت سنی به دلیل اینکه در فضای مجازی، جداسازی بر اساس سن، جنسیت یا معیارهای دیگری که جداسازی آن در دنیای واقعی کاملاً آسان است، بسیار دشوار و پرهزینه است، شکست‌خورده و بنابراین اعمال هنجارهای حقوقی موجود در حل این مشکل بی‌تأثیر است^۱. حریم خصوصی در فضای مجازی نیز با توجه به ویژگی‌های آن با حریم خصوصی در دنیای واقعی متفاوت

¹ See: It's about the case *Reno v. American Civil Liberties Union*, 521US844 (1997).
<https://supreme.justia.com/cases/federal/us/521/844/>

است؛ باین حال، مقررات قانونی مستلزم شفافیت کامل کل اینترنت است که امروزه از نظر فنی مشکل ساز است. اگر فرض کنید هنگام ورود به اینترنت، شناسایی ویدیویی کاربر رخ دهد، مشکل شناسایی با موفقیت حل می‌شود، اما این روش از نظر «حریم خصوصی» خطرناک بوده و بازهم نیاز به شفافیت کامل دارد که اینترنت توانایی فنی این موضوع را ندارد. از سوی دیگر نگرانی‌های قانون‌گذاران در این بخش قابل درک است، زیرا مشخص نیست که آیا کنترل دولتی برای شناسایی موجه یا کافی خواهد بود، یا اینکه ما می‌خواهیم به دولت اجازه دهیم چنین اطلاعات محرمانه‌ای را درباره کاربر دریافت کند. موضوع دیگر در مقررات فضای مجازی، رویکرد به مقررات است، زیرا بدون شک اگر یک کشور فضای مجازی را به شدت تنظیم کند و کشور دیگر به هیچ وجه مقرراتی را تنظیم نکند، در نتیجه کلیت مقررات به شدت بی‌اثر می‌شود. در این راستا، بحث در مورد تصویب قوانین عمومی برای تنظیم فضای مجازی در سطح بین‌المللی ضروری است.

از سوی دیگر اصل سرزمینی به خودی خود مبنای بسیار محدودی برای صلاحیت است. در این صورت، رسیدگی به جنایاتی که عواقبی برای تعداد نامحدودی از کشورهای دیگر دارد، بسیار دشوار خواهد بود. در مورد «پرونده یاهو»^۱ در فرانسه، ملاحظه می‌گردد که دادگاه برای مورد پیگرد قرار دادن جرم نتایج آن در فرانسه را مناط اعتبار قرار داده است؛ اگرچه هیچ عنصر تشکیل دهنده جرم در خاک فرانسه رخ نداده است.^۲ از نظر حقوقی، بدیهی است که چنین رویکردی در اعمال صلاحیت یک دولت در روابط حقوقی در فضای سایبر ناکافی است. از طرفی در مسیر اعمال صلاحیت سرزمینی باید این را مدنظر قرارداد که زیرساخت‌های سایبری دولت‌ها به هم مرتبط هستند، بنابراین اعمال صلاحیت قضایی در یک دولت بر زیرساخت‌های سایبری کشور دیگر تأثیر می‌گذارد. البته، این دلیلی برای محدود کردن حاکمیت یک کشور نیست، چراکه مرزهای سایبری جداگانه وجود ندارد، استقلال سیاسی و حاکمیت ارضی دولت توسط قانون محافظت می‌شود و مفهوم سرزمینی حاکمیت در هنگام تنظیم سایر کشورها مصون از تعرض باقی می‌ماند. اصل موجود حاکمیت ناشی از حقوق بین‌الملل و به‌ویژه از بند ۱ ماده ۲ منشور سازمان ملل متحد، منع مداخله غیرقانونی بین دولت‌ها را پیش‌فرض می‌گیرد. بر اساس اصل حاکمیت سرزمینی، دولت‌ها موظف هستند که اجازه استفاده آگاهانه از قلمرو خود را برای اقداماتی که با حقوق سایر کشورها در تضاد است، ندهند (Corfu Channel case, 1949). نمونه‌ای از مداخله غیرقانونی، انتشار اطلاعات نادرست از طریق اینترنت، تحریک ناآرامی سیاسی توسط یک کشور خارجی به منظور مداخله در انتخابات کشوری دیگر است. به‌عنوان مثال، آلمان بر این باور است که «اقدامات سایبری اگر از نظر مقیاس و تأثیر با اجبار در زمینه‌های غیر سایبری تشابه داشته باشد ممکن است از منظر حقوق بین‌الملل مداخله‌ای ممنوع باشد». علاوه بر این، آلمان این دیدگاه را بیان می‌کند که اگر فعالیت‌های سایبری بخشی از یک درگیری مسلحانه جاری باشد، حقوق بشردوستانه بین‌المللی در مورد فعالیت‌های سایبری در چارچوب یک درگیری مسلحانه اعمال می‌شود (On the Application of International Law in Cyberspace, 2021: 5). بنابراین، بر این عقیده است که حقوق بین‌الملل، منشور ملل متحد و حقوق بشردوستانه بین‌المللی، بدون قید و شرط در زمینه فضای مجازی اعمال می‌شود. نظر مشابهی توسط حقوقدانان روسی وجود دارد که بین صلاحیت قضایی در فضای سایبری و صلاحیت در حقوق بین‌الملل فضایی مشابهی ایجاد کرده‌اند. به نظر آن‌ها، می‌توان تعریف مفهوم قلمرو یک دولت را با گنجاندن فضای دیگری در آن، مثلاً فضای مجازی، گسترش داد (Erentyeva, 2019: 121). در همین حال، به‌منظور اطمینان از ایمنی کار در اینترنت، علی‌رغم بحث‌های داغ برای چندین سال، در فدراسیون روسیه در ماه مه ۲۰۱۹، قانونی به تصویب رسید

¹ The case Yahoo!

² See: The case Yahoo! Inc. against La Ligue Contre Le Racisme et l'Antisemitisme, <https://caselaw.findlaw.com/us-9th-circuit/1144098.html>

که در رسانه‌ها «قانون اینترنت مستقل» نامیده شد.^۱ این قانون مفاهیم جدیدی مانند «نقطه تبادل ترافیک»،^۲ «خطوط ارتباطی فرامرزی»،^۳ سامانه نام دامنه ملی در حال ایجاد و تعهدات اپراتورهای مخابراتی برای استفاده از تجهیزات دولتی در نقاط مبادله ترافیک را معرفی کرد. بدون شک تصویب این قانون نشان‌دهنده رویکرد فدراسیون روسیه در رابطه با ایجاد صلاحیت قضایی در فضای مجازی بر اساس مفهوم اعمال اصل سرزمینی است (Document/View/0001201905010025/<http://publication.pravo.gov.ru>) همچنین اقداماتی از سوی «شورای اروپا»^۴ برای مبارزه با جرائم سایبری انجام شده است که نتیجه آن «کنوانسیون بوداپست»^۵ در سال ۲۰۰۱ است. این کنوانسیون تعدادی معیار را برای ایجاد صلاحیت در جرائم کیفری تعیین می‌کند که هنجارهای کنوانسیون بر اساس اصل سرزمینی است و جرائم ارتكابی در قلمرو یک دولت مطابق صلاحیت آن کشور تلقی می‌شود. این کنوانسیون همچنین اصل تابعیت را به رسمیت می‌شناسد. مطابق با فحوای کنوانسیون، کشورها برای مقابله مؤثرتر با جرائم فرامرزی باید وسایل ارتباطی بین‌المللی در مورد چنین موضوعاتی داشته باشند.

در رویه‌ی قضایی ایالات متحده رویکردهای متفاوت‌تری از این موضوع دیده می‌شود و تمایل بسیاری به اعمال قواعد سنتی در این فضا وجود دارد که البته اولویت اساسی نیز همان صلاحیت سرزمینی می‌باشد، منجر به چالش‌هایی اساسی نیز شده است. یک شکاف اساسی بین مفاهیم صلاحیت شخصی که اساساً ماهیت سرزمینی دارد و اینترنت که تمام محدودیت‌های سرزمینی را نادیده می‌گیرد، وجود دارد (Andrew, 2001: 319). این امر کاربرد دکتترین مبتنی بر قلمرو را پیچیده می‌کند. استدلال شده است که پیچیدگی‌های اینترنت اجازه استفاده از پارادایم‌های حقوقی سنتی را نمی‌دهد و در عوض به یک هیئت حاکمه جداگانه و یک رژیم حقوقی جدید نیاز دارد (Farooq, 2004: 409).

۲. اختلاف نظرات در خصوص حل تعارض قوانین سایبری

در خصوص قواعد اعمالی در صلاحیت سایبری در رویه قضایی ایالات متحده آراء متفاوتی وجود دارد که برخی از آن‌ها در پیدایی قواعدی خاص نقش اساسی ایفا نموده‌اند؛ اما در این بین اختلافات اساسی دیده می‌شود. در همین راستا تحلیل و طرح این نظریه‌ها و خاستگاه آن‌ها در هر پرونده‌ای از اهمیت اساسی برخوردار است که در این قسمت از نوشته‌ی حاضر چگونگی طرح و اعمال این تئوری‌ها در پرونده‌های مختلف مطرح گردیده و در بحث آتی تحلیل گردیده است که هرکدام از این تئوری‌ها با چه چالش‌هایی مواجه است و نهایتاً چه راهکاری قابل طرح می‌باشد.

۱.۲. تئوری «ارتباط حداقلی»

در پرونده «شرکت صنایع فلزی آساهی»^۶ دادگاه اعلام کرد که ممکن است تأثیر این وب‌سایت، در سطح ملی یا حتی بین‌المللی احساس شود، اما این موضوع، بدون در نظر گرفتن موارد دیگر، برای ایجاد صلاحیت به نفع ایالتی که جرم عامداً علیه تبعه‌ی آن انجام شده کافی نیست. بر اساس این حکم، دادگاه همچنین اعلام کرد که اعمال صلاحیت شخصی، حمایت‌های حداقلی دادرسی

¹ See: Federal Law of May 1, 2019 N 90-FZ "On Amendments to the Federal Law" On Communications" and the Federal Law "On Information, Information Technologies and Information Protection", providing for the creation of a national routing system for Internet traffic, tools centralized management, etc. Entered into force on November 1, 2019.

² Traffic exchange point

³ Cross-border communication lines

⁴ Council of Europe

⁵ Budapest Convention

⁶ Asahi Metal Indus. Co. v. Superior Court, 1992

در قوانین ایالات متحده را نقض می‌نماید (Asahi Metal Indus. Co. v. Superior Court, 1992: 102). به منظور برآورده کردن این حمایت‌ها، دادگاه باید دو مورد را مدنظر داشته باشد؛ اولاً، اینکه شرکت غیر مقیم متهم «ارتباط حداقلی»^۱ با کشور رسیدگی‌کننده به جرم را داشته باشد و دوماً اینکه این دادرسی مفهوم سنتی رسیدگی عادلانه را خدشه‌دار نکند.^۲

در موردی دیگر که به‌عنوان «پرونده داو جونز» شناخته می‌شود،^۳ شرکت «داو جونز» مجله «وال استریت و بارونز»^۴ را منتشر کرد. این مجله بر روی «سرور»^۵های نگهداری شده در «نیوجرسی»^۶ ایالات متحده بارگذاری شده بود؛ دربردارنده‌ی مواردی بود که ادعا می‌شد برای متهم «جوزف گاتنیک»^۷، ساکن «ویکتوریا»^۸، توهین‌آمیز است. در این مورد، اساسی‌ترین سؤال مطرح‌شده صلاحیت دادگاه بود؛ که محکمه پس از بررسی اذعان داشت از آنجا که مطالب در «ویکتوریا»^۹ دانلود شده است؛ بنابراین، دادگاه آن محل صالح به رسیدگی است.

مورد دیگر تعارض در اعمال صلاحیت سایبری در ایالات متحده آمریکا در قضیه‌ی «یانگ کیس»^{۱۰} قابل مشاهده است. در این پرونده دادگاه نظری کاملاً مخالف داشته است. در این مورد، دو روزنامه مطالبی را با اظهارنظرهای توهین‌آمیز درباره آقای «یانگ» (سرپرست زندان) منتشر کرده بودند. «دادگاه منطقه‌ای»^{۱۱} اعلام کرد که دادگاه «ویرجینیا»^{۱۲} صلاحیت قضایی دارد، اما شعبه چهارم «دادگاه استیناف» این حکم را لغو کرد و بیان داشت:

«این روزنامه و وبسایت‌های آن منحصراً مخاطبان ویرجینیا را هدف قرار نداده‌اند و صرفاً به این دلیل که هرکسی می‌تواند مقالات را از وبسایت بارگیری کند، صلاحیت قضایی را به دادگاه‌های ویرجینیا نمی‌دهد.» (Schultz, 2008: 804)

این دیدگاه پیش‌تر در قضیه «زیپو منوفکچرینگ علیه زیپو دات کام»^{۱۳} مشاهده می‌شود دادگاه در این مورد صلاحیت خود را بر اساس ماهیت وبسایت یعنی فعال یا غیرفعال بودن آن، اعمال کرده است. (Zippo Manufacturing Co. v. Zippo Dot Com, Inc. 1997: 19).^{۱۴} اما در ادامه فرآیند دادگاه استیناف یافته‌های «پرونده زیپو» را رد کرده و از استانداردهای «جهت هدفمند»^{۱۵} و «اثرات هدفمند»^{۱۶} به جای استانداردهای مبتنی بر ماهیت تعاملی وبسایت استفاده کرده است. در پرونده‌ای دیگر دادگاه به جای اعمال دو اصل مورد اشاره، «اصل ارتباط حداقلی» را اعمال کرده؛ که مجرای آن منوط به ارتباط داشتن متهم با یک حوزه قضایی بر اساس اقامت، رضایت یا ارتکاب اقداماتی در آن، مانند انجام تجارت یا ارتکاب تخلف، است.^{۱۷}

¹ Minimum Contact Principle

² SEE: International Shoe Co. v. Washington, 1945, The text available at: <http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&vol=326&invol=310> (last updated Nov. 17, 2012)

³ Dow Jones and Company Inc. v. Gutnick, 2002

⁴ The Wall Street Journal

⁵ Server

⁶ New Jersey

⁷ Joseph Gutnick

⁸ Victoria

⁹ Young v. New Haven, U.S. Appl 2002

¹⁰ Virginia

¹¹ Zippo Manufacturing Co. v. Zippo Dot Com, Inc.

¹² If a site allows browsers to enter into binding contracts, the court would consider that site as an 'active', and if the Website is only providing certain information to the web browser, the site would be considered 'passive' website.

¹³ Purposeful Direction

¹⁴ Intended Effects'

¹⁵ Burger King Corp. v. Rudzewicz, 1985

البته توضیح این نکته ضروری است که با اعمال همین اصل حتی اگر دادگاه قدرت اعمال صلاحیت را داشته باشد، همچنان باید در مورد معقول بودن اعمال صلاحیت تصمیم‌گیری نماید؛ که «دیوان عالی ایالات متحده آمریکا»^۱ از پنج عامل برای تعیین منطقی بودن ارتباط استفاده کرده است (World-Wide Volkswagen v. Woodson, 1980: 286-297):

۱. بار اثباتی عدم ارتباط بر عهده متهم محفوظ باشد
۲. منفعت دادگاه محل رسیدگی در رسیدگی به اتهام
۳. تسهیل در نائل شدن شاکی به حق مورد تضییع^۲
۴. علاقه سیستم قضایی بین ایالتی به دستیابی به کارآمدترین راه‌حل اختلافات؛
۵. منافع مشترک چندین ایالت در پیشبرد سیاست‌های اجتماعی اساسی.

۲.۲. مبانی حقوق بشری و «حق بر آزادی بیان»

در پرونده «سارل لوئیز علیه ویوفاندرز»^۲، شاکی -یک شرکت فرانسوی- یک نمایش مد در فرانسه ترتیب داده بود. متهم عکس‌هایی از این شوی مد را در وبسایت خود قرار داده بود. شاکی به دلیل استفاده غیرمجاز از مالکیت معنوی و رقابت ناعادلانه به دادگاه فرانسه شکایت نموده و رأی به محکومیت متهم صادر شده بود و نهایتاً متهم اجرای این رأی را از محکمه ایالات متحده خواسته بود (The judgment of appellate court, 2007). «دادگاه منطقه جنوبی نیویورک» ضمن خودداری از اصدار دستور به اجرای رأی بیان داشته بود که: «حکم صادره از دادگاه فرانسوی با اصلاحیه اول و با ماده ۱، بخش ۸ قانون اساسی ایالت نیویورک ناسازگار است (Jonhson, Post, 2012). البته این رأی در دادگاه استیناف نقض شد و برای بررسی بیشتر اعاده گردید، اما تعارض آشکار در این پرونده این بود که دادگاه فرانسه اقدام متهم را نقض حقوق مالکیت حقوق بشر دانسته بود، درحالی که دادگاه ایالات متحده حکم دادگاه فرانسه را برخلاف «سیاست عمومی»^۳ و «متمم اول» قانون اساسی ایالات متحده در نظر گرفته و متهم را با این استدلال که یک مجله خبری است و قرار است رویدادهای عمومی را گزارش کند بر اساس «حق آزادی بیان» مبرا دانسته بود.

یکی دیگر از پرونده‌های مهم صلاحیت قضایی در فضای سایبر پرونده «یاهو» است.^۴ این شرکت به‌عنوان یک ارائه‌دهنده خدمات مستقر در ایالات متحده در بیست کشور ارائه خدمات سایبری دارد. هر سرویس ملی دارای یک کد دوحرفی (URL) است و خدمات ارائه شده در فرانسه تحت عنوان <http://www.yahoo.fr> انجام می‌شود. این شرکت همچنین سایت «حراج یاهو» را ارائه می‌نماید. این سایت به هرکسی اجازه می‌دهد تا کالایی را برای فروش پست کند و در میان کاربران جهانی به حراج گذارد. طبق سیاست‌های این سایت، فروشندگان حراج از ارائه اقلام به خریداران در حوزه‌هایی که فروش چنین اقلامی ناقض قوانین حاکم بر حوزه قضایی است، منع شده‌اند. نمایش «مواد نازی» یا فروش «علائم نازیسم» در فرانسه غیرقانونی است. از آنجاییکه در فرانسه این یک جرم محسوب می‌شود، هیچ ماده یا نشانی حاکی از آن در <http://www.yahoo.fr>، وبسایت ایجاد شده برای فرانسه، وجود نداشت. اما در خصوص این پرونده بحث در مورد نازیسم در چت روم سایت آمریکایی مطرح شده بود و وبسایت آمریکایی همچنین

¹ Supreme Court of the United States

² See also: Spiliada Maritime Corporation v. Cansulex Ltd, 1987

³ Sarl Louis Feraud International v. Viewfinder, Inc. 2007

⁴ Public Policy

⁵ Text is available at- <http://caselaw.findlaw.com/us-9th-circuit/1144098.html> (last updated Nov. 14, 2013)

اطلاعات مربوط به مواد ممنوعه حراج را در اختیار داشت. وبسایت یاهو آمریکا برای اتباع فرانسوی قابل دسترسی بود و فرصت (دسترسی) برای خرید اقلام حراج از جمله لوازم نازی‌ها را داشت.

دو گروه از فعالان مدنی در دادگاه فرانسه شکایت کردند. بر اساس یافته‌های دادگاه فرانسه، نزدیک به ۱۰۰۰ شیء مرتبط با «نازی‌ها» و «رایش سوم»، از جمله «پروتکل من»^۱ اثر «آدولف هیتلر»^۲، «پروتکل بزرگان صهیون»^۳ (گزارش بدنام ضدیهودی که توسط پلیس مخفی تزار در اوایل دهه ۱۹۰۰ تهیه شده بود) در حال انتشار بود. برای فروش در سایت حراج Yahoo.com ارائه شده بود.

در اثنای دادرسی در فرانسه، یاهو صلاحیت دادگاه را مورد اعتراض قرار داد، اما دادگاه این ایراد شکلی را رد کرده و پس از جلسه استماع در ۱۵ مه ۲۰۰۰، دادگاه فرانسه در ۲۲ مه دستور موقت صادر کرد که یاهو را ملزم می‌کرد تمام اقدامات لازم را برای منصرف کردن و غیرممکن کردن هرگونه دسترسی [از قلمرو فرانسه] از طریق Yahoo.com به سرویس حراج مصنوعات نازی و هر سایت یا سرویس دیگری که ممکن است به منزله عذرخواهی برای نازیسم یا اعتراض نازی‌ها تلقی شود، انجام دهد.^۴

یاهو با این دستور مخالفت کرد و از جمله ادعا کرد که «هیچ راه‌حل فنی وجود ندارد که بتواند به‌طور کامل از شرایط حکم دادگاه پیروی کند». دادگاه سه ماه مهلت داد تا به دستور خود عمل کند. یاهو در دادگاه منطقه‌ای ایالات متحده برای اعلام بی‌اعتباری حکم دادگاه فرانسه در ایالات متحده شکایت کرد. دادگاه منطقه اعلام کرد که اجرای دستور فرانسه در ایالات متحده، متمم اول قانون اساسی و اصل آزادی بیان را نقض می‌کند؛ بنابراین، در ایالات متحده غیرقابل اجرا است.

۳. تحلیل علل و تناقض مستتر در اختلاف نظرات

اصلی‌ترین دلیل بروز اختلاف نظرها در خصوص تعارض قوانین سایبری در ایالات متحده آمریکا ریشه در به‌کارگیری معیارهای متفاوت در آن دارد که در مبحث قبلی مورد تذکر واقع شد. به نظر می‌رسد به‌کارگیری ضوابطی خاص در اعمال هریک از این معیارها می‌تواند در کاربردی سازی آن معیار و نهایتاً غلبه بر مشکلات آن مفید فایده باشد.

۱.۳. معیار «ارتباط حداقلی»، «بهره‌مندی هدفمند» و ضابطه‌ی پیش‌بینی پذیری

می‌توان بیان داشت که امروزه یاری جستن از اصل سنتی «ارتباط حداقلی» برای حل تعارض صلاحیت در فضای سایبر با چالش بسیار اساسی روبروست. در نمونه‌هایی از وبسایت‌های غیرفعال که به سمت جامعه جهانی به‌طور کلی هدایت می‌شوند، نمی‌توان انتظار وجه ارتباطی بیش از «دسترسی صرف» با یک کشور خاص را داشت. هدف این نوع وبسایت‌ها ممکن است این باشد که مطالبی را در دسترس برای کل جهان قرار دهند. برای مثال، وبسایت‌های مستهجن عمداً به سمت یک کشور خاص هدایت نمی‌شوند. آن‌ها به‌طور کلی در دسترس جامعه جهانی قرار می‌گیرند. در چنین مواردی، اثبات «ارتباط حداقلی» دشوار است و همچنین اثبات «جهت هدفمند» فقط به سمت یک کشور خاص دشوارتر است. به‌طور مشابه، در نقض حق چاپ آنلاین، مطالب دارای حق چاپ ممکن است برای کل جهان قابل دسترسی باشد. «ارتباط حداقلی» با یک کشور خاص ممکن است ایجاد نشود یا

¹ Adolf Hitler's Mein Kampf

² Adolf Hitler

³ Protocol of the Elders of Zion

⁴ See: http://caselaw.findlaw.com/us-9th-circuit/1144098.html#footnote_ref_1 (last updated Nov. 14, 2013)

ممکن است «عمداً» به سمت آن نباشد؛ بنابراین، اعمال این دکترین در مورد نقض حق چاپ، نویسندگان را درمانده می‌کند. آن‌ها ممکن است نتوانند برقراری «ارتباط حداقلی» یا «جهت هدفمند» را نسبت به یک کشور خاص اثبات کنند.

دکترین «ارتباط حداقلی» و «بهره‌مندی هدفمند» مزایای متعددی دارند؛ اولاً، در مورد عمل احتمالی، یعنی دعوی قضایی، تصور معقولی به متهم می‌دهد و یک معیار پیش‌بینی‌پذیری است که در قلب استاندارد معقولیت قرار دارد. این معیار حکم می‌کند که یک طرف فقط باید در جایی به دادگاه خارجی فرستاده شود که احتمال وقوع چنین احتمالی قابل پیش‌بینی باشد. (Muralidha, S., 2010) ثانیاً، در حداکثر موارد، از تعدد صلاحیت اجتناب می‌کند ولی باز اثبات جهت‌گیری هدفمند به سمت یک دولت خاص دشوار به نظر می‌رسد. در همین راستا برای اعمال دقیق این اصل باید «اصل پیش‌بینی‌پذیری»^۱ را به‌عنوان ضابطه‌ای در نظر گرفت که اعمال آن را تسهیل نماید؛ در همین راستا در پرونده «شرکت جهانی فولکس‌واگن در مقابل وودسون»^۲ دادگاه اعلام کرد که رفتار و ارتباط متهم با دادگاه ایالت مذکور به‌گونه‌ای است که او باید به‌طور منطقی پیش‌بینی می‌کرد که اگر تخلفی انجام دهد در آنجا محاکمه خواهد شد. این اصل را می‌توان بر اساس مفاهیم سنتی بازی جوانمردانه و عدالت اساسی که توسط دادگاه ایالات متحده در قضیه «شرکت کفش بین‌المللی علیه واشنگتن» به رسمیت شناخته شده است، حمایت کرد (International Shoe Co. v. Washington, 1945:310-316). ثالثاً طبق مفهوم سنتی قانون، شخص نمی‌تواند تحت قوانین یک کشور مستقل دیگر مسئول شناخته شود مگر اینکه وارد قلمرو آن شود یا قلمرو حاکمیتی آن در اثر تخلف این فرد متأثر گردد؛ بنابراین، مشکل تعدد صلاحیت و تعقیب کیفری را می‌توان با اعمال اصول فوق به حداقل رساند.

۲.۳. معیارهای حقوق بشری و ضرورت تأسیس مجمعی فراملی

رأی پرونده «سارل لوئیز علیه ویوفاندرز» را می‌توان به دلایل مختلف موردانتقاد قرار داد (The Judgment of appellate court, 2013). به نظر می‌رسد هرچند اولین مفهوم حکم دادگاه منطقه‌ای این است که به قاعده عرفی صلاحیت سرزمینی پایبند باشد ولی در این رأی دادگاه فرض کرده است که قوانین سرزمینی فقط برای قلمرو آن ایالت لازم‌الاجرا است و قانون سایر مناطق در منطقه مذکور قابل اعمال نیست. اگر این رویکرد در سطح جهانی دنبال شود، وب‌سایت‌ها فقط تابع قانون دولتی هستند که جریان اطلاعات از آن نشأت می‌گیرد. این امر جولان مجرمان را آسان می‌کند، زیرا یافتن کشوری با رژیم حقوقی مناسب و انتشار هرگونه محتوایی در آنجا با توجه به سیاست کیفری آن دولت کار سختی نخواهد بود و از سوی دیگر هیچ دلیلی وجود ندارد که منافع جامعه‌ای که در آن اثرات مضر داده‌های جریان آزاد متحمل می‌شود با این فرضیه اشتباه، نادیده بگیریم (Schultz, 2008:802)؛ لذا به نظر می‌رسد قواعد متفاوتی باید در فضای سایبر اعمال گردد و به نظر می‌رسد باید دادگاه حمایت از اتباع فرانسوی را در نظر می‌گرفت.

از سوی دیگر «دادگاه منطقه‌ای جنوب نیویورک» با این ادعا که اجرای حکم توسط دادگاه فرانسوی خلاف «سیاست عمومی» است، این شکایت را رد کرد. سؤال اساسی در مورد «سیاست عمومی» این است که کدام «سیاست عمومی» باید بر فعالیت‌های اینترنتی حاکم باشد؟ آیا این باید سیاست ایالات متحده یا یک کشور خاص یا سیاست جامعه جهانی باشد؟ پاسخ واضح به این سؤال، سیاست جامعه جهانی در کل خواهد بود؛ بنابراین، نیاز به ایجاد یک مجمع فراملی برای تصمیم‌گیری و اجرای «سیاست عمومی» قابل اجرا در اینترنت وجود دارد.

¹ Principle of Foreseeability

² World-Wide Volkswagen Corp. v. Woodson, 1980

مورد دیگری که وجود دارد در خصوص قضیه «سارل لوئیز علیه ویوفاندرز» و «ياهو» تناقض آشکاری است که دیده می‌شود؛ در مورد اول مطالب دارای حق چاپ هم در فرانسه و هم در ایالات متحده محافظت می‌شد؛ بنابراین، دادگاه ایالات متحده ادعای نقض حقوق مالکیت معنوی را در پرتو متمم اول قانون اساسی ایالات متحده محدود کرد، اما در قضیه «ياهو» این عمل در ایالات متحده جرم محسوب نمی‌شد، اما در فرانسه مجازات بود. انتقادات زیادی در خصوص این پرونده مطرح شده است^۱ که یکی از آن‌ها عدم تلاش دادگاه برای بحث درباره مقبولیت اخلاقی تبلیغات نازی‌ها بود (Hadas, 2002:299). یکی دیگر از مشکلات در این پرونده ضرورت صلاحیت فرانسه در این موضوع بود که «پروفسور جک گلداسمیت»^۲ دستیار پیشین دادستان کل آمریکا، پیشنهاد داده بود شایسته بود فرانسه بر ياهو اعمال صلاحیت کند؛ زیرا این شرکت چیزی در وبسایت خود قرار داده که توسط شهروندان فرانسوی قابل دسترسی است و قوانین فرانسه را نقض می‌کند (Kaplan, 2000). گذشته از این، به نظر می‌رسد همان‌طور که «قاضی گومز»^۳ بیان داشته است نیاز به ارزش‌گذاری ارزش‌های اخلاقی وجود دارد و آن‌گونه که ایستگاه‌های تلویزیونی، روزنامه‌ها و مجلات برای به حاشیه راندن دیدگاه‌ها و محصولات که اکثریت قریب به اتفاق آمریکایی‌ها فکر می‌کنند بی‌احترامی یا حتی بالقوه خطرناک هستند، از پذیرش برخی از تبلیغات خودداری می‌کنند؛ شرکت‌های اینترنتی نیز باید همان کار را انجام دهند (Greenberg, 2003:1212).

علی‌رغم استدلال‌های فوق، باید بیان داشت که مشکل تعارض قوانین و تعارض صلاحیت در این مورد، لزوم استفاده از استانداردها یا قواعد یکسان برای فضای مجازی را به جامعه جهانی یادآوری می‌نماید، لذا موضوع مطروحه در پرونده فرانسه باید از هر دو زاویه موردبررسی قرار گیرد:

۱. از منظر حاکمیت، دولت نمی‌تواند به‌طور مؤثر از حق حاکمیت خود برای وضع و اجرای قوانین استفاده کند، اگرچه وبسایت در قلمرو آن قابل دسترسی است. علاوه بر این، فرانسه از آنجایی که این عمل در ایالات متحده مجازات ندارد و استرداد متهم توسط ایالات متحده برخلاف اصل «مجرمیت دوگانه»^۴ خواهد بود، نمی‌تواند درخواست استرداد را داشته باشد.

۲. از منظر حقوق بشری نیز اگر هر کشوری مانند فرانسه شروع به اعمال محدودیت برای گفتار و بیان در اینترنت کند، فضای مجازی موضوع محدودیت‌های عظیمی خواهد بود و عملاً ممکن است حتی امکان استفاده از این مؤثرترین وسیله ارتباطی، وجود نداشته باشد و کاربران در هراس دائمی از پیگرد قانونی در هر کشوری باشند.

به نظر می‌رسد دادگاه ایالات متحده باید با پاسخ به تعهدات بین‌المللی علیه فعالیت‌های نژادپرستانه، اصل همدلی را اعمال می‌کرد. از قضا در سیر تاریخی دادگاه نظامی به رهبری آمریکا موسوم به «دادگاه نورنبرگ»^۵ در خصوص اقدامات نازی‌ها، متهمین را به دلایل نقض جنایت علیه بشریت و سایر جنایات مجازات کردند و در همین محکمه بر این اصل پافشاری کرده‌اند که صلاحیت در این جرایم باید جهانی باشد.^۶ و همین رویکرد نشان‌دهنده‌ی اعمال استانداردهای دوگانه از سوی ایالات متحده آمریکا است.

¹ See: <http://caselaw.findlaw.com/us-9th-circuit/1144098.html> (last updated Nov. 14, 2013)

² Professor Jack Landman Goldsmith

³ Judge Michael Gomez

⁴ Double Criminality

⁵ Nuremberg trials

⁶ See: <http://www.history.ucsb.edu/faculty/marcuse/classes/33d/projects/nurembg/NurembergCrimes.htm> (last updated Nov. 16, 2013)

نتیجه گیری

عطف توجه به رویه‌ی قضایی ایالات متحده در مورد حل تعارض صلاحیت در جرایم سایبری، می‌توان بیان داشت که معضلات قضایی و تعارض قانون سایبری را نمی‌توان با به‌کارگیری «اصول ثابت‌شده» و «ابزارهای قانونی سنتی» که برای مشکلات مشابه در فضای واقعی توسعه داده شده‌اند، به‌اندازه کافی حل نمود. در پرونده «یاهو» موضوع فقط در دادگاه آمریکا قابل مجازات بود. منطق ارائه‌شده در این قضیه صلاحیت سرزمینی سنتی بود ولی در عالم واقع، علیرغم اینکه فرد خارج از قلمرو است، ممکن است مسئولیت عمل ارتكابی در فضای سایبری را بر عهده بگیرد. آیا این بدان معناست که قبل از انجام فعالیت در فضای سایبر، قوانین همه کشورها در نظر گرفته شود؟ حقوق بین‌الملل سنتی شخص را مجبور به رعایت قوانین کشورهای دیگر نمی‌کند مگر اینکه وارد آن سرزمین شود یا حاکمیت آن سرزمین از رفتار وی مستقیماً تحت تأثیر قرار گیرد. در عصر اینترنت، مشاهده این که چه تعداد از کشورها به‌طور مستقیم یا غیرمستقیم تحت تأثیر قرار گرفته‌اند دشوار است. اصول تثبیت‌شده حقوق و حقوق بین‌الملل یا پاسخگوی مشکلات فضای سایبر نیست و یا قدرت حل آن را ندارد. این فضا با فضای فیزیکی تفاوت اساسی دارد. ماهیت، کنترل، گستردگی و تأثیر آن اساساً متفاوت است. اینترنت حوزه قضایی جدید و مجزایی است که در آن قوانین و مقررات دنیای فیزیکی آن‌طور که هست اعمال نمی‌شود. به گفته برخی از نویسندگان، این یک منطقه یکپارچه جهانی-اقتصادی، بدون مرز و غیرقابل تنظیم است. طبق فلسفه حقوق قدیمی، فعالیت‌های یک قلمرو باید توسط قوانین و مقررات یک کشور مستقل اداره شود. فلسفه مذکور را نمی‌توان در فضای سایبر اعمال کرد؛ این فضا باید به‌عنوان یک حوزه قضایی جداگانه به رسمیت شناخته شود زیرا نه دولت مستقل قادر به کنترل آن است و نه مشروعیت قوانین حاکم بر فعالیت‌های آنلاین به‌طور طبیعی در یک کشور واقع شده است.

پیشنهادها

در مقام پیشنهاد باید بیان داشت که:

۱. در مقام پاسخگویی به تعارض صلاحیت کیفری در جرایم سایبری و رویکرد رویه‌ی قضایی ایالات متحده که با چالش‌های اساسی درزمینه‌ی اصرار بر قواعد سنتی صلاحیت سرزمینی روبرو است؛ جهان باید از فلسفه صلاحیت سرزمینی به فلسفه حقوقی جدیدی که به نام فراملیت‌گرایی جهانی معروف است، حرکت کند. حقوق بین‌الملل باید به‌گونه‌ای عمل کند که تعارض را با در نظر گرفتن حقوق و منافع هر یک از طرف‌های متضرر حل کند. برای این منظور فضای سایبری باید به‌عنوان (منطقه بدون اعمال حاکمیت ملی [مشمول آزادی مشترک بهره‌برداری])^۱ اعلام شود. این طرز نگرش حقوقی برای حل معضل تعارض صلاحیت کیفری جرایم سایبری برای نظام حقوقی ایران نیز توصیه می‌گردد.

۲. برای مدیریت قلمرو پیشنهاد شده در بند قبلی، باید یک سازمان فراملی تحت کنترل سازمان ملل متحد وجود داشته باشد. ایجاد چنین سازمانی تحت نظارت سازمان ملل متحد دارای مزایای متعددی است، چراکه از سویی کشورهای قدرتمند از نظر فناوری، قادر به سوءاستفاده خودسرانه بر نخواهند بود و از طرفی دیگر منجر به هماهنگی قواعد و سیستم‌های قضایی در خصوص حل تعارض صلاحیت کیفری می‌گردد.

¹ Res Extra Commercium

منابع

۱. امینی‌نیا، عاطفه، علیزاده، حمیدرضا. (۱۳۹۷). اعمال صلاحیت کیفری (تعارض قوانین) در مورد جرائم ارتكابی در فضای سایبر، فصلنامه پژوهش ملل، دوره ۶، شماره ۳۰.
۲. پور قهرمانی، بابک، صابرنژاد، علی. (۱۳۹۳). حریم خصوصی در فضای سایبر از منظر حقوق بین‌الملل، چاپ اول، تهران: انتشارات مجد.
۳. رضوی فرد، بهزاد، موسوی، سید نعمت‌الله. (۱۳۹۶). محدودیت‌ها و راهبردهای صلاحیت در جرایم سایبری، فصلنامه حقوقی دادگستری، دوره ۸۱، شماره ۹۸.
۴. عبدالهی، اسماعیل، مرادی، سکینه. (۱۳۹۴). صلاحیت کیفری در فضای سایبری، فصلنامه علمی دانش انتظامی بوشهر، دوره ۶، شماره ۲۰.
5. Andrew E. Costa. (2001). 'Personal jurisdiction in cyberspace: Something more is required the electronic stream of commerce', Dynamics of International law Milleniumin,R.K. Dixit
6. Asahi Metal Indus. Co. v. Superior Court, (1992)
7. Burger King Corp. v. Rudzewicz, (1985)
8. Clough, Jonathan. (2015). Principles of Cybercrime, 2nd ed. London: Cambridge University Press
9. Dow Jones and Company Inc. v. Gutnick. (2002)
10. Erentyeva LV. (2019). Principles for Determining Territorial Jurisdiction of the State in Cyberspace. Lex Russica. (7): 119-129. P.121 (In Russ.)<https://doi.org/10.17803/1729-5920.2019.152.7.119-129>
11. Farooq, Ahmad. (2004). Jurisdictional Issues in Cyberspace, Dynamics of International law Milleniumin, R. K. Dixit
12. Federal Law "On Amendments to the Federal Law" On Communications" and the Federal Law "On Information, Information Technologies and Information Protection", (2019),providing for the creation of a national routing system for Internet traffic, tools centralized management, etc. Entered into force on November 1, 2019.
13. Federal Law of May 1, 2019 N 90-FZ "On Amendments to the Federal Law" On Communications" and the Federal Law "On Information, Information Technologies and Information Protection". (2019). providing for the creation of a national routing system for Internet traffic, tools centralized management, etc. Entered into force on November 1
14. Greenberg, Marc H. (2003). A Return to Lilliput:The Licra v. Yahoo! Case and the Regulation of Online Content in the World Market, BerkeleyTechnology Law Journal,Vol;18,No.4
15. Hadas, Rinat. (2002). International Internet Jurisdiction: Whose Law is Right? Yahoo! Inc. v. La Ligue Contre le Racisme et L'Antisemitisme, Florida Journal of International Law,No.15
16. International Court of Justice (ICJ), Corfu Channel case United Kingdom of Great Britain and Northern Ireland v. Albania. (1949). Judgment of 9 April. <https://www.icj-cij.org/en/case/1/judgments>
17. International Shoe Co. v. Washington, (1945)
18. International Shoe Co. v. Washington, 326 U.S. 310, 316 [66 S.Ct. 154, 158, 90 L.Ed. 95] (1945). The text available at- <http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&vol=326&invol=310> (last updated Nov. 17, 2012)
19. Johnson, David R. and Post, David G. (2012), Law and Borders: The Rise of Law in Cyberspace, Stanford Law Review, No, 12, at: http://www.cli.org/X0025_LBFIN.html.
20. Kaplan, Carls. (2000). French Nazi Memorabilia Case Presents Jurisdiction Dilemma, Cyber Law Journal, August 11, At:<http://partners.nytimes.com/library/tech/00/08/cyber/cyberlaw/11law.html> (last updated Dec. 24, 2013)
21. Muralidha, S. (2010). Jurisdictional Issues in Cyberspace, The Indian Journal of Law and Technology,Volume 6, at:<http://www1.nls.ac.in/ojs-2.2.3/index.php/IJLT/article/viewFile/76/61> (lastupdated Nov. 14, 2013)
22. On the Application of International Law in Cyberspace, (2021), the Federal Government of Germany. Position Paper – March, <https://www.auswaertiges-amt.de/blob/2446304/2ae17233b62966a4b7f16d50ca3c6802/on-the-application-of-international-law-in-cyberspace-data.pdf>
23. Rahmatilla Aryani Putri, Huala Adolf, Jafar Sidik. (2021). Law Enforcement of Cyber Crime Jurisdiction in Transnasional Law, Advances in Social Science, Education and Humanities Research, volume 658
24. Reno v. American Civil Liberties Union, 521US844 (1997). <https://supreme.justia.com/cases/federal/us/521/844/>

25. Schmitt, M. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2 nd ed).Cambridge: Cambridge University Press. Glossary
26. Schultz, Thomas. (2008). Carving up the Internet: Jurisdiction, Legal Order and the Private/Public International Law Interface, The European Journal of International Law, Vol. 19 no.4
27. Spiliada Maritime Corporation v. Cansulex Ltd. (1987) 1 AC460
28. The case Yahoo! Inc. against La Ligue Contre Le Racisme et l'Antisemitisme, <https://caselaw.findlaw.com/us-9th-circuit/1144098.html>
29. The judgment of appellate court. (2007). available, at:http://www.leagle.com/decision/2007963489F3d474_1962 (last updated Nov. 14, 2013)
30. Theudgment of appellate court, (2013), available at http://www.leagle.com/decision/2007963489F3d474_1962 (last updated Nov. 14, 2013)
31. World-Wide Volkswagen v. Woodson, (1980)
32. Young v. New Haven,U.S. Appl, (2002)
33. Zippo Manufacturing Co. v. Zippo Dot Com, Inc., (1997)
34. <http://caselaw.findlaw.com/us-9th-circuit/1144098.html> (last updated Nov. 14, 2013)
35. <http://publication.pravo.gov.ru/Document/View/0001201905010025>
36. <http://www.history.ucsb.edu/faculty/marcuse/classes/33d/projects/nurembg/NuremburgCrimes.htm> (last updated Nov. 16, 2013)
37. <https://supreme.justia.com/cases/federal/us/521/844>