مقاله

مجلهٔ

پژوهشهای حقوقی

علمی ـ ترویجی

شماره ۳۱

هزار و سیصد و نود و شش ـ نیمسال اول (دوفصلنامه)

- **تعلیق اجرای قواعد بین‌المللی حقوق بشر در وضعیت‌های عمومی فوق‌العاده** ۷
  دکتر سید قاسم زمانی ـ مرضیه اسفندیاری
- **کاهش فقر؛ دستورالعملی برای توسعهٔ اجتماعی در نظام بین‌المللی حقوق بشر** ٤۷
  دکتر رضا اسلامی ـ مهشید آجلی لاهیجی
- **حمایت از حقوق بشر در فضای سایبر** ۷۹
  دکتر سید یاسر ضیایی
- **تحلیل نظام قانونی ایران در حوزه سرمایه‌گذاری صنعت نفت** ۱۰۷
  دکتر حمید باقرزاده ـ دکتر راحله سید مرتضی حسینی
- **اعتراض ثالث اجرایی در قانون اجرای احکام مدنی** ۱۲۳
  دکتر رسول پروین ـ امین پاهکیده ـ الهه اعتمادی
- **ضوابط حاکم بر ارجاع پرونده‌های قضایی از منظر استقلال قضایی: با مطالعه تطبیقی در حقوق ایران و اسناد بین‌المللی** ۱٤٥
  امید رستمی غازانی
- **نقش شاکی خصوصی و دادستان در جرایم علیه میراث تاریخی و فرهنگی** ۱٦۹
  دکتر کیومرث کلانتری ـ حسن خدابخشی پالندی ـ امیر عرفانی‌فر
- **حمایت حقوقی از آثار تاریخی و فرهنگی در برابر آلودگی‌های زیست‌محیطی** ۲۰۳
  امین ولی‌زاده ـ صابر نجومی
- **حفاظت از تالاب‌ها در حقوق بین‌الملل، در پرتو کنوانسیون رامسر** ۲۳۱
  مهرداد محمدی ـ وحیده نجفی
- **دور باطل تصویب عوارض در شوراها و ابطال در هیئت عمومی دیوان عدالت اداری: کاوشی در نظارت قضایی بر توسعه شهری مغایر با حق مالکیت مردم (۱۳۹٤-۱۳۸۸)** ۲٥۱
  دکتر وحید آگاه ـ محمدنبی بوربوری
- **قانون دعوای جمعی: الگویی برای کشورهای نظام سیویل‌لا** ۲۸۷
  نویسنده: پروفسور آنتونیو جیدی ـ مترجم: دکتر مجید پوراستاد

شهر دانش

مؤسسه مطالعات و پژوهشهای حقوقی

http://jlr.sdil.ac.ir/article_49838.html

حمایت از حقوق بشر در فضای سایبر

دکتر سید یاسر ضیایی*

چکیده:

اینترنت تیغ دولبه‌ای است که از یک سو موجب ترویج حقوق بشر شده است و از سوی دیگر عرصه‌ای شده است برای نقض حقوق بشر. نقض حقوق بشر در فضای سایبر جلوه‌های ویژه‌ای به خود گرفته است و لازم است برای جلوگیری از نقض و جبران آن مکانیسم مناسبی یافت شود. برای انتساب نقض‌های حقوق بشر به دولت نظریات گوناگونی مطرح می‌شود که می‌توان به نظریات اقتدار دولتی، ماهیت عمل و تعقیب فوری اشاره نمود. در فضای سایبر احتمال نقض حقوقی چون آزادی بیان، آزادی اجتماع، آزادی دسترسی به اطلاعات، حق تعیین سرنوشت، حق مالکیت، حق بر حریم خصوصی و غیره وجود دارد. سازمان‌های حقوق بشری مجازی و سایت‌های ثبت شکایت اینترنتی از جمله ساز و کارهای حمایت از حقوق بشر در فضای سایبر هستند که از آن به «خودگردانی اینترنتی» یاد می‌گردد. همچنین کشورهای بالادستی اینترنتی می‌توانند در «تضمین حقوق بشر از سوی ثالث» نقش مهمی در حمایت از حقوق بشر در فضای سایبر داشته باشند.

کلیدواژه‌ها:

فضای سایبر، حمایت از حقوق بشر، تضمین به حمایت از حقوق بشر، انتساب عمل متخلفانه به دولت، حقوق بشر، حقوق بین‌الملل.

مجلهٔ پژوهشهای حقوقی (علمی - ترویجی)، شمارهٔ ۳۱، نیمسال اول ۱۳۹۶
صفحهٔ ۷۹-۱۰۵، تاریخ وصول: ۱۳۹۴/۰۴/۲۰، تاریخ پذیرش: ۱۳۹۴/۰۶/۱۶

* استادیار گروه حقوق بین‌الملل دانشگاه قم Email: yaserziaee@gmail.com

مقدمه

«سایبر» در لغت به معنی «حکمران» است و در اصطلاح به فضای مجازی میان سخت‌افزارهایی می‌گویند که حاوی اطلاعات‌اند. این فضا توسط سرویس‌های نرم‌افزاری مختلفی اطلاعات را به اشتراک می‌گذارد: شبکه جهان‌گستر (world wide web)، Gopher و ftp از این جمله‌اند.[1] برای تفکیک این فضا از فضای موجود میان ابزارهای تکنولوژیک پیشین مانند تلفن، ماهواره، تلگراف، بی‌سیم و رادیو باید عنصر رایانه را به تعریف فضای سایبر افزود. به این ترتیب فضای مذکور باید از طریق سرورهایی تأمین شود که در نقاط مختلف جهان به این کار اختصاص داده شده‌اند. تاریخ ایجاد آنها به تلاش آمریکا برای تمرکززدایی در حوزه اینترنت برمی‌گردد. وزارت بازرگانی، تدبیر امور اینترنت آمریکا را به دانشگاه کالیفرنیا واگذار کرد. دانشگاه مذکور «سازمان اینترنتی انتصاب اسمی و کدهای رقمی»[2] (آیکان) را ایجاد نمود. این سازمان به هر سایتی یک IP مخصوص اعطاء می‌کند. سیزده سرور پیش‌گفته توسط آیکان خلق شدند.[3]

از سوی دیگر حقوق بشر امری پویا و انتزاعی است. این حقوق از آزادی‌های اساسی افراد در هر کجا که باشند حمایت به عمل می‌آورد؛ چه در خلال یک جنگ تمام‌عیار باشند چه در آرامش کامل و پشت کامپیوتر شخصی خود. رابطه میان حقوق بشر و فضای سایبر دوسویه است. بدین معنی که در وهله اول متغیر حقوق بشر بر متغیر اینترنت تأثیرگذار است. به عبارت دیگر اجرای حقوق بشر به نحو احسن، ارمغان ترویج اینترنت را به عنوان یکی از ابزارهای نوین تحقق این حقوق به دنبال دارد؛ چنانچه حق توسعه، حق آزادی بیان و حق آزادی تشکیل اجتماع از جمله از طریق فضای سایبر قابل تحقق است. به دنبال این استدلال می‌توان اعتراض نمود که چرا باید ۷۷٪ جمعیت جهان فقط ۵٪ از خطوط تلفنی را دارا باشند؟ و یا چرا در حالی که میانگین استفاده از اینترنت در جهان یک نفر از هر ۳۸ نفر است در قاره آفریقا (بجز آفریقای جنوبی) یک نفر از هر ۵۰۰۰ نفر است؟[4]

1. Errol P. Mendes, Democracy, "Human Rights and the New Information Technologies in the 21st Century-The Law and Justice of Proportionality and Consensual *Alliances*," National Journal of Constitutional Law 10 (1999), 371.

2. Internet Corporation for Assigned News and Numbers (ICANN)

3. Noel Cox, "The Regulation of Cyberspace and the Loss of National *Sovereignty*," *Information and Communications Technology Law* 11 (2002).

4. Wayne Sharpe, "Rebel Internet: Human Rights and the New Technology," in *Human Rights and the Internet*, ed. Steven Hick, Edward F. Halpin and Eric Hosakins (New York: Macmillan Press, 2000), 45.

در وهله دوم راهیابی فضای سایبر به خانه‌های مردم، تلفن‌های همراه مردم، کافی‌نت‌ها و حتی ادارات دولتی موجب تأثیرگذاری بر حقوق بشر می‌شود. این تأثیر یا در قالب حمایت از حقوق بشر است یا در قالب نقض حقوق بشر. حمایت از حقوق بشر می‌تواند از طریق آموزش، اطلاع‌رسانی، ایجاد وب‌سایت‌های حقوق بشری، جمع‌آوری اعانه، ارسال پست‌های الکترونیکی و غیره محقق شود. به طور مثال «فن رمزنویسی هم به انتشار بی‌نام و نشان اطلاعات نظیر گزارش‌های حقوق بشر توسط برخی کشورها کمک می‌کند و هم مانع تغییر و تحریف اسناد گروه‌های حقوق بشر پس از انتشار می‌شود».[۵] به همین قدرت نیز فضای سایبر می‌تواند موجب نقض حقوق بشر شود. به عبارت ساده‌تر اجرای حقوق بشر نیاز به اینترنت دارد و استفاده از اینترنت نیاز به مکانیسم‌هایی برای حمایت از حقوق بشر.

۱- نقض‌های ارتکابی در فضای سایبر

برای بررسی مکانیسم‌های ممکن برای حمایت از حقوق بشر در فضای سایبر ابتدا لازم است بررسی شود که چه نقض‌هایی در محیط سایبر قابل ارتکاب‌اند و مرتکبین آنها چه کسانی هستند. فضای سایبر فضایی است که در آن سه دسته با یکدیگر در ارتباط‌اند: افراد، دولت ملی و دولت خارجی. هرکدام از اینها می‌تواند علیه دیگری حقوق ناظر بر آنها را نقض کند. در فضای سایبر افراد می‌توانند علیه افراد دیگر جرایمی چون کلاهبرداری، سرقت، تخریب را مرتکب شوند؛ افراد می‌توانند علیه دولت ملی جرایمی چون تروریسم، سابوتاژ[۶]، سرقت اموال دولتی، قاچاق، اشاعه اکاذیب، افشای اسناد سری، پولشویی الکترونیکی و براندازی را مرتکب شوند؛ دولت ملی می‌تواند علیه افراد جرایمی چون استراق سمع، پروکسی غیرقانونی، مصادره سرمایه الکترونیکی، افشای اسرار و نقض حریم خصوصی را مرتکب شود؛ این دولت می‌تواند علیه دولتی دیگر جرایمی چون جنگ اطلاعاتی، جاسوسی، سابوتاژ و تروریسم سایبری را مرتکب شود؛ دولت بیگانه می‌تواند علیه افراد نیز مرتکب جرایمی چون پروکسی سایت از سوی سرور مستقر در کشور میزبان، افشای اسرار و حتی نقض حق تعیین سرنوشت فرهنگی

---

۵. محمدحسین بردبار، *درآمدی بر حقوق ارتباط جمعی: مطبوعات، ماهواره و اینترنت* (تهران: نشر ققنوس، ۱۳۸۱)، ۸۴.

۶. سابوتاژ در فضای سایبر عبارت است از تخریب اموال و دارایی مادی و معنوی یک شرکت تجاری (دولتی و غیردولتی). به طور مثال یک برنامه‌نویس رایانه‌ای در نیوجرسی آمریکا با کارگذاری یک بمب رایانه‌ای موجب تخریب نرم‌افزارهای رایانه‌های یک شرکت شد که ۱۰ میلیون دلار خسارت وارد نمود.
See: "Sabotage", encyclopedia, last accessed May 17, 2017, http://www.encyclopedia.com/doc/1G2-3401803675.html.

شود.[۷] اما باید توجه داشت در حقوق بشر رابطه فرد و دولت مطرح است و از این رو نقض‌های سایبری افراد علیه افراد یا دولت علیه دولت در این نوشتار مطرح نیست. با این حال ماهیت ویژه فضای سایبر این امکان را تسهیل کرده است که دولت‌ها در پوشش شرکت‌های ارائه‌دهنده خدمات اینترنتی دست به نقض حقوق بشر بزنند.

۲- مکانیسم‌های حمایت از حقوق بشر در فضای سایبر

ساز و کارهای حمایت از حقوق بشر در فضای سایبر را می‌توان از یک منظر و به طور عام دو دسته دانست: ساز و کارهای ناظر بر حمایت از نقض حقوق بشر در فضای سایبر (حمایت) و ساز و کارهای ناظر بر پیشگیری از نقض حقوق بشر در فضای سایبر (تضمین به حمایت).

۲-۱- مکانیسم‌های تضمین به حمایت از حقوق بشر در فضای سایبر

در خصوص پیشگیری از نقض حقوق بشر[۸] تلاش‌های زیادی در سطح ملی و بین‌المللی صورت گرفته است. در سطح ملی از جمله بخش امنیت ملی آمریکا به تأسیس «بخش محافظت و مدیریت بحران سایبری» دست زده است و در مالزی «مرکز ملی واکنش سریع و امنیت فناوری اطلاعات»، در اتریش «کمیسیون حمایت از داده‌ها»، در فرانسه «کمیسیون ملی داده‌پردازی فایل‌های داده و آزادی‌های فردی» و در آلمان «کمیسیون حمایت از داده‌ها» تشکیل شده است[۹]. وضع قوانین داخلی متضمن کپی‌رایت محصولات کامپیوتری نیز در این زمره است. عدم وجود قانون کپی‌رایت و ثبت نرم‌افزارهای رایانه‌ای از موارد نقض تضمین حقوق بشر توسط دولت است. در سطح بین‌المللی نیز سازمان همکاری و توسعه اقتصادی رهنمودهایی را برای تضمین حمایت از حریم خصوصی افراد ارائه داده است که طبق آن کشورها در جمع‌آوری داده‌های شخصی محدودیت دارند و باید محافظت‌های امنیتی متعارف برای حفاظت از آنها را تدبیر کنند.[۱۰] برخلاف این رهنمودها که غیرالزامی‌اند، «کنوانسیون شورای اروپا در خصوص تضمین حمایت از حقوق افراد در رابطه با پردازش

7. Kim-Kwang Raymond Choo, "Organized Crime Groups in Cyberspace: a *Typology*," *Trends in Organized Crime* 11 (2008): 270.

8. Ensure to Protect

۹. اولریش زیبر، *جرایم رایانه‌ای*، ترجمه محمدعلی نوری و دیگران (تهران: نشر گنج دانش، ۱۳۸۴)، ۱۲۰.

10. "Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data", The Organization for Economic Co-Operation and Development, last accessed May 17, 2017, http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

خودکار داده‌های شخصی» قواعدی الزام‌آور برای حمایت از داده‌های شخصی ارائه می‌دهد[۱۱]. اصل اساسی در این کنوانسیون اصل «حمایت متقابل» است که طبق آن دولت عضو اتحادیه نمی‌تواند مانع از جریان داده‌ها به کشوری شود که حمایت متقابل ارائه می‌دهد و بالعکس در صورت عدم حمایت دولت باید از جریان داده جلوگیری کند[۱۲]. یکی از کارهایی که دولت‌ها در تضمین حمایت از حقوق بشر باید انجام دهند الزام شرکت‌های واسط به کنترل داده‌های غیرقانونی و میتینگ‌های غیرمجاز و انتشاراتی است که موجب نقض حقوق بشر می‌شوند.

بهترین سندی که تاکنون برای تضمین به حمایت از نقض حقوق بشر در فضای سایبر امضاء شده است «کنوانسیون جرایم سایبری» مصوب شورای اروپا مورخ ۲۰۰۱ در بوداپست است که در آن کشورهای عضو را ملزم به جرم‌انگاری داخلی در خصوص بسیاری از جرایم سایبری نموده است. این جرایم عبارتند از دسترسی غیرقانونی (ماده ۲)، قطع غیرقانونی (ماده ۳)، مداخله در اطلاعات (ماده ۴)، مداخله در سیستم (ماده ۵)، سوءاستفاده از وسایل (ماده ۶)، جعل رایانه‌ای (ماده ۷)، کلاهبرداری رایانه‌ای (ماده ۸)، هرزه‌نگاری کودکان (ماده ۹) و نقض کپی‌رایت (ماده ۱۰)[۱۳].

ب. مکانیسم‌های حمایت از حقوق بشر در فضای سایبر

ساز و کارهای «حمایت» از حقوق بشر در فضای سایبر را می‌توان از دو منظر مطرح نمود: ساز و کارهای موجود در فضای سایبر برای نقض‌های حقوق بشر به طور کلی، اعم از نقض‌های صورت‌گرفته در فضای واقعی و مجازی و دوم ساز و کارهای موجود به طور کلی، اعم از ساز و کارهای موجود در فضای واقعی و فضای مجازی برای نقض‌های صورت‌گرفته در فضای سایبر.

اول. ساز و کارهای فضای سایبر برای حمایت از حقوق بشر

می‌توان گفت اولین و بهترین ابزار حمایت از حقوق بشر احاله موضوع به افکار عمومی است که تجلی اجلّ این افکار عمومی در محیط سایبر محقق شده است. در واقع با به اشتراک گذاردن و مطلع کردن عموم از نقض‌های ارتکابی توسط دولت‌ها می‌توان به مهم‌ترین ابزار حمایت از حقوق بشر تأسی جست که این امر از طریق اینترنت به وضوح قابل تحقق است.

11. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, January 28, 1981.
12. Ibid, Art. 29.
13. Convention on Cybercrime, Budapest, European Treaty Series - No. 185, 23.11.2001.

مثال‌های زیادی از تأثیر این روند موجود است: با افشای خبر کودتای نافرجام در زیمبابوه توسط دو روزنامه‌نگار، این دو نفر دستگیر می‌شوند که با انتشار این خبر در اینترنت و متعاقباً فشارهای افکار عمومی سرانجام به آزادی آنها منجر می‌شود.[۱۴]

در کنار انتشار اخبار از طریق اینترنت باید به امکانات برخی سایت‌ها برای حمایت از حقوق بشر نیز اشاره نمود. این سایت‌ها با امکان دریافت اخبار از شهروندان از طریق پست‌های الکترونیکی دست به اقدام علیه متخلفان می‌زنند. بهترین مثال این مورد سایت مرکز شکایت جرم اینترنتی (ic3) است که جرایم اینترنتی شامل نقض حقوق بشر در اینترنت را از این طریق پی‌گیری می‌کند.[۱۵] البته باید توجه داشت کشور آمریکا به عنوان مقر دو سرور ریشه‌ای اینترنت نمی‌تواند به حکم مرجعی پلیسی یا قضایی به طور کلی اینترنت را در یک کشور قطع نماید[۱۶] بلکه می‌تواند طبق قواعد حقوق بشری سایت متخلف را از دسترس خارج

---

۱۴. با ظهور آزادی در شرق اروپا مردم تحت ستم دولت برای بیان اعتراضشان از ویروس‌های رایانه‌ای استفاده می‌کردند مانند ویروس یانکی دودل (Yankee Doodle) که به طور اتوماتیک آهنگی یانکی را پخش می‌کرد. دیوید جِی. آیکاو، کارل‌ای سیگر، ویلیام‌آر وان استروچ، *راهکارهای پیشگیری و مقابله با جرایم رایانه‌ای*، ترجمه اکبر استرکی و دیگران (تهران: نشر دانشگاه علوم انتظامی، ۱۳۸۳)، چاپ ۱، ۹۵.

با جرأت می‌توان بیان داشت که اثربخشی گزارش کمیته‌های حقوق بشری نیز منوط به انتشار آن در رسانه‌های عمومی‌ای چون اینترنت است به طور مثال کمیسیون حقوق بشر سازمان ملل متحد در سال ۱۹۹۸ قطعنامه‌ای در تقبیح اقدام اندونزی در اشغال تیمور شرقی صادر کرد که بدون انتشار آن در اینترنت قابل دسترسی به ساکنین تیمور شرقی نبود.

Sharon Scharfe, "Human Rights and the Internet in Asia: Promoting the Case of East Timor," in *Human Rights and the Internet*, ed. Steven Hick, Edward F. Halpin and Eric Hosakins (New York: Macmillan Press, 2000), 129.

۱۵. مرکز شکایت جرایم اینترنتی (ic3) با همکاری دفتر بازرسی دولت فدرال (FBI)، مرکز ملی جرایم یقه‌سفید (NW3) و دفتر معاضدت قضایی (BJA) در آمریکا ایجاد شده است. هدف این مرکز ایجاد تسهیلاتی برای کاربران اینترنتی است تا به راحتی بتوانند مقامات را در جریان نقض‌های جنایی و بشری قرار دهند. برای طرح شکایت در این مرکز لازم نیست شاکی خود متضرر نیز باشد و تمام اطلاعات اعلام‌شده به این مرکز مخفی خواهند ماند. برای ثبت شکایت باید به این سایت رجوع نمود:

See: "Filing a Complaint with the IC3", Federal Bureau of Investigation Internet Crime Complaint Center (IC3), last accessed May 17, 2017, http://www.ic3.gov.

۱۶. علت این امر تعهد کشورها به انتقال تکنولوژی به کشورهای در حال توسعه است که در برخی اسناد قید شده است. این حق در بند ۲ ماده ۶۶ موافقتنامه تریپس و در متن پیش‌نویس کارگروه WTO برای تجارت و انتقال تکنولوژی مصوب ۲۰۰۱ که در سال ۲۰۰۵ تبدیل به کدهای رفتاری انتقال تکنولوژی گردید، پیش‌بینی شده است.

Thomas Alured Faunce, Hitoshi Nasu, "Normative Foundations of Technology Transfer and Transnational Benefit Principles in the UNESCO Universal Declaration on Bioethics and Human *Rights*," *Journal of Medicine and Philosophy* Vol 34 No. 3 (2009): 296-321. http://ssrn.com/abstract=1402388

سازد و این نوعی «تضمین به حمایت از حقوق بشر از سوی ثالث» است که مفهومی جدید در حقوق بشر اینترنتی است.[۱۷]

علاوه بر این بسیاری از سازمان‌های حقوق بشری مجازی تأسیس شده‌اند که به اسناد و اخبار مهمی دسترسی دارند. در موارد نقض حقوق بشر و در راستای حمایت می‌توان از این سازمان‌های مجازی برای تأسیس حقوقی «دوست دادگاه»[۱۸] کمک گرفت. دو سازمان معروف در این زمینه یکی «سازمان دِرکاس»[۱۹] مربوط به امور پناهندگان و گمشدگان اجباری و دیگری «سازمان مرز الکترونیکی»[۲۰] در خصوص دفاع از آزادی‌های اجتماعی کاربران است.[۲۱] لازم به ذکر است سیاست‌های راهبردی برخی کشورها اقتضاء می‌کند دسترسی به سایت‌های مربوط به دموکراسی و حقوق بشر را محدود سازند. به طور مثال کشور چین سایت دیدبان حقوق بشر و سایت صدای دموکراسی هنک‌کنگ را مسدود کرده است.[۲۲]

۱۷. همان‌طور که گفته شد در صورتی کشور مورد نظر می‌تواند اینترنت را در یک کشور قطع کند که عضو کنوانسیون شورای اروپا باشد و عدم تضمین به حمایت از حقوق بشر را در کشور دیگر احراز نماید.

۱۸. نهاد دوست دادگاه (Amicus curie) شکلی از مداخله در دادرسی است که نه به عنوان ثالث و نه به عنوان کارشناس در دادگاه شرکت می‌کند بلکه تنها به این دلیل است که منافع جمعیت مورد حمایت (و نه منافع خود سازمان) در خطر است. محمدحسین رمضانی قوام‌آبادی، «حضور سازمان‌های غیردولتی در پیشگاه مراجع قضایی بین‌المللی»، *فصلنامه حقوق* دوره ۳۸ شماره ۲ (۱۳۸۷)، ۱۵۷.

19. NIZKOR, last accessed May 17, 2017, www.derechos.org.

20. www.eff.org

21. Michael Katz-Lacabe, Margarita Lacabe, "Doing Human Rights Online: the Derechos Cyberbirth," in *Human Rights and the Internet*, de. Steven Hick, Edward F. Halpin and Eric Hosakins (New York: Macmillan Press, 2000), 65.

22. Nikola A. Koritz, "The Yahoo Case And Free Speech, Privacy And Corporate Responsibility in The People's Republic Of China", *ExpressO* (2008): 9, last accessed May 17, 2017, http://works.bepress.com/nikola_koritz/1/

علاوه بر این در اینترنت مراجعی برای رسیدگی مستقیم به تخلفات وجود دارد کـه از آن به جلوه‌های «خودگردانی در فضای سایبر»[۲۳] یاد می‌شود. سـه مـورد از ایـن مکانیسـم‌هـای درون‌اینترنتی عبارتند از: مکانیسم .a.c.e.a.n که به حذف اسپم‌های اینترنتی و تعقیب و اقدام علیه صادرکنندگان آن می‌پردازد، مرجع حل اختلاف نام مشترک دامنه‌ها (UDRP) و کمیته ویژه بین‌المللی (IAHC) که اولی زیر نظر سازمان اینترنتی انتصاب اسمی و کـدهای رقمـی (ICANN) و دومی زیر نظر اتحادیه بین‌المللی مخابرات و وایپو به حل اختلافات مربوط بـه ثبت دامنه‌های جهانی و تجاری در اینترنت می‌پردازد[۲۴] و مکانیسم موجود در آمریکـا آنلایـن (America Online) که خدمت‌رسانی به کاربران متخلف خود را متوقف می‌سازد.[۲۵]

دوم. ساز و کارهای حمایت از حقوق بشر در فضای سایبر

ساز و کارهای موجود برای حمایت از حقوق بشر در فضـای سـایبر دو دسـته اسـت: ملـی و بین‌المللی. در سطح ملی برخی کشورها ساز و کاری را برای حمایت از حقوق بشـر در نظـام داخلی خود پیش‌بینی کرده‌اند مانند سند استراتژی امنیت فضای سـایبر آمریکـا کـه از جملـه شرکت‌های ارائه‌کننده خدمات اینترنتی را برای اقداماتشان در فضای سایبر پاسخگو می‌دانـد. قانون ۱۹۹۴ چین نیز در خصوص حفاظت از سیستم‌های اطلاعاتی رایانه‌ای بیان می‌دارد که هیچ فرد یا سازمانی نمی‌تواند از سیستم‌های اطلاعاتی رایانه برای اموری اسـتفاده کنـد کـه منافع جمعی یا ملی شهروندان را به مخاطره اندازد.[۲۶] همچنین ممکن است دادگاه‌هایی چون

23. Cyberspace Self-government.

۲۴. برای مشاهده گزارش یکی از اختلافات مطروح در UDRP نک:

"Julia Fiona Roberts v Russell Boyd Case No. D2000-0210 , May 29, 2000, WIPO Arbitration and Mediation Center", WIPO Arbitration and Mediation Center, accessed November 6, 2007, http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0210.html. See also Jacqueline D. Lipton, "Who Owns 'Hillary.Com?' Political Speech and the First Amendment in Cyberspace, Political Speech in *Cyberspace*," *Case Legal Studies Research Paper* 07-16 (2008): 1-53.

از زمان آغاز خدمات این مرکز داوری در دسامبر سال ۱۹۹۹ میلادی در حدود بیش از ۲۰۰۰ موضوع از بیش از ۱۵۰ کشور جهان به این مرکز مراجعه شده است که این امر نشان‌دهنده استقبال فراوان جامعه اینترنتـی جهـان از این سرویس است. به طور متوسط روزانه چهار تقاضای جدید در این مرکز ثبت می‌شود.

WIPO, WIPO Intellectual Property Handbook, Geneva, 2001, 235.

25. Henry H. Perritt, JR. "Cyberspace Self-Government: Town Hall Democracy or Rediscovered *Royalism?*," *Berkeley Technology Law Journal* 12 (1999): 438-451.

۲۶. ابراهیم حسن‌بیگی، *حقوق و امنیت در فضای سایبر* (تهران: نشر مؤسسه فرهنگی مطالعات و تحقیقات ابرار معاصر تهران، ۱۳۸۴)، چاپ ۱، ۲۵۹.

عدالت اداری، شورای ناظر بر قانون اساسی و غیره در سطح ملی وجود داشته باشد [۲۷] که به تخلفات دولت و شرکت‌های وابسته در نقض حقوق بشر رسیدگی کنند. اما موضوع این نوشتار مکانیسم‌های موجود بین‌المللی برای حمایت از حقوق بشر در فضای سایبر است. همان‌طور که بیان شد نقض‌های حقوق بشری در فضای سایبر در اعمال ارتکابی از سوی دولت علیه شهروندان خود یا شهروندان کشوری دیگر معنا می‌یابد که با توجه به اینکه سرویس‌دهی اینترنت در اکثر کشورهای جهان به بخش خصوصی واگذار شده است انتساب این اعمال به دولت مورد تردید قرار گرفته‌اند. لذا پیش از ذکر موارد امکان‌پذیر نقض حقوق بشر درفضای سایبر باید به دکترین‌های انتساب عمل نقض در فضای سایبر به دولت اشاره شود.

۳- انتساب عمل نقض به دولت در فضای سایبر

پیش از بررسی انتساب یک عمل متخلفانه به یک دولت باید ببینیم علیه چه دولتی امکان طرح مسؤولیت وجود دارد. انتساب عمل متخلفانه به دولت در فضای سایبر به دو علت از ویژگی خاصی برخوردار است. اول اینکه دنیای مجازی در دنیایی خارج از دنیای مرسوم و متعارف واقعی به زیست خود ادامه می‌دهد و پیوستگی اطلاعات در این دنیا به نحوی است که اثر عمل یک دولت در گوشه‌ای از دنیا قابل رؤیت و اثربخش در بسیاری از نقاط دیگر دنیا خواهد بود. به طور مثال کشوری که سرور ریشه‌ای در سرزمین وی مستقر است می‌تواند با قطع آن به قطع اینترنت در بخش وسیعی از جهان دامن زند و یا دولتی با پراکندن اخبار و جملات تحریک‌آمیز به نسل‌کشی یا تبعیض نژادی در فضای مجازی، تمام کاربران دنیای فیزیکی را تحت تأثیر قرار دهد.[۲۸] دوم اینکه اثر عمل نقض در دنیای مجازی قابل رؤیت در دنیای خارج است اما ریشه این عمل نقض و عامل آن در شبکه عنکبوتی اینترنت به سختی قابل ردیابی است.

---

۲۷. به طور مثال نویسنده‌ای تأسیس دادگاه آمریکایی برای فضای سایبر را پیشنهاد کرده و مزایا و معایب آن را بررسی کرده است، ن.ک:

Henry H. Perritt. JR., "Jurisdiction in *Cyberspace*," *Villanova Law Review* 41(1) (1996): 100.

۲۸. پروتکل الحاقی به کنوانسیون جرایم سایبری اینگونه اقدامات را ممنوع اعلام کرده‌اند:

See "Additional Protocol to the Convention on Cybercrime, Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed through Computer Systems, 28.I.2003", Council of Europe, accessed, last accessed May 17, 2017, http://conventions.coe.int/Treaty/EN/Treaties/html/189.htm.

آنچه برای مراجع ذی‌ربط باید مهم باشد بررسی عامل نقض اصلی است. چرا که در فضای سایبر نمی‌توان به اماره سرزمین (که در قضیه کورفو در دیوان بین‌المللی دادگستری مطرح شد) یا تابعیت قربانی برای انتساب عمل نقض به دولت تأسی جست بلکه باید دانست نقض در فضای سایبر به علت ماهیت ویژه آن در دنیایی خلق می‌شود که در آن ترتّب تکنولوژیکی مطرح است. بدین معنی که کشورهای بالادست و صاحب فناوری برتر امکان تسلط و حکمرانی بر کشورهای پایین‌دست را دارند. به طور مثال کشوری که سرور ریشه‌ای در آن مستقر است می‌تواند با اختلال در آن بر حقوق ابنای بشر در سراسر دنیا تأثیر گذارد بدون آنکه دولت سرزمین قربانی، اقدام متخلفانه‌ای انجام داده باشد و بالعکس با قطع اینترنت از سوی کشور متبوع قربانی این شائبه مطرح می‌شود که این اقدام از سرزمین بالادست صورت گرفته باشد! مسئله وقتی پیچیده‌تر می‌شود که بدانیم در این میان شرکت‌های خصوصی واسطی وجود دارند که به ارائه خدمات اینترنتی مشغول‌اند. لذا میزان کنترل بر این شرکت‌ها توسط دولت برای مسؤول دانستن آن دولت بسیار مهم است.

۳-۱- انتساب عمل شرکت‌های خصوصی ارائه‌کننده خدمات اینترنتی به دولت در حقوق بین‌الملل

انتساب عمل بازیگران غیردولتی از جمله شرکت‌های خصوصی به دولت در سه حالت اتفاق می‌افتد: زمانی که دولت کنترل مؤثر بر نهاد مذکور داشته باشد (ماده ۸ طرح مسؤولیت بین‌المللی دولت‌ها)، زمانی که نهاد مذکور طبق حقوق داخلی یک کشور اعمال اقتدار عمومی می‌کند (ماده ۵ طرح مسؤولیت بین‌المللی دولت‌ها) و زمانی که نهاد مذکور در غیاب دولت مذکور و در موارد ضرورت اعمال اقتدار عمومی می‌کند (ماده ۹ طرح مسؤولیت بین‌المللی دولت‌ها). دیوان بین‌المللی دادگستری در قضیه بارسلونا تراکشن متذکر می‌شود که حقوق بین‌الملل تمایز میان شخصیت شرکت‌ها در حقوق داخلی از شخصیت دولت را پذیرفته مگر در مواردی که «پوشش شرکتی»[۲۹] صرفاً وسیله یا ابزاری برای تقلب یا فرار از مسؤولیت باشد.[۳۰] کمیسیون حقوق بین‌الملل در تفسیر ماده ۹ طرح مسؤولیت بین‌المللی دولت‌ها با اشاره به این نکته اضافه می‌کند «اینکه شرکتی ابتدائاً خواه به موجب یک قانون خاص یا به هر طریق دیگر توسط دولت تأسیس شده است دلیل کافی برای انتساب رفتارهای بعدی او به دولت تلقی نمی‌شود. چنین شرکت‌ها یا مؤسساتی اگرچه تحت مالکیت دولت بوده و

29. Corporate Veil
30. Barcelona Traction, I.C.J. Reports, 1970, 39, Para. 56-58.

بدین‌ترتیب تحت کنترل دولتی قرار دارند، اما شخصیت حقوقی مستقلی از دولت دارند و علی‌الظاهر رفتار آنها به دولت قابل انتساب نیست مگر آنکه به اعمال برخی اقتدارات دولتی در مفهوم ماده ۵ (اقتدار دولتی) اقدام کرده باشند».[۳۱] کمیسیون در تفسیر ماده ۵ طرح مسؤولیت دولت‌ها می‌گوید «محدوده دقیق «اقتدار دولتی» برای انتساب رفتار یک نهاد به دولت در این ماده مشخص نشده است. تا حدودی این مسئله که چه نهادی «دولتی» تلقی می‌شود به ویژگی یک جامعه، تاریخ و سنن آن برمی‌گردد. علاوه بر محتوای اختیارات، شیوه اعطای آنها، هدف از اعمال آنها و میزان پاسخگویی آن مؤسسه در برابر دولت از بابت اعمال آن اختیارات، واجد اهمیت بسیاری است».[۳۲] اما باید توجه داشت که برخی امور که در فضای واقعی در حیطه اختیارات عمومی تلقی می‌شوند در فضای سایبر تغییر ماهیت می‌دهند. به طور مثال آزادی مطبوعات در فضای واقعی امری است که هرگونه تخلف در آن قابل انتساب به دولت است اما آزادی مطبوعات الکترونیکی در فضای سایبر امری است که هم ایجاد آن هم مسدودسازی آن کاملاً در دست دولت نیست و افراد خصوصی می‌توانند در آن دخالت داشته باشند.

یکی از معیارهای قابل طرح برای انتساب یک اقدام متخلفانه در فضای سایبر به دولت، «ماهیت تخلف» صورت‌گرفته است. چنانچه ماهیت حملات سایبری به گرجستان در پی جنگ روسیه و گرجستان به نوعی بود که مطالعات دانشگاه دفاع ملی سوئد تحقق آن را بدون حمایت دولت روسیه غیر قابل تصور اعلام نمود.[۳۳] این اقدامات شامل دسترسی به شماره کارت‌های اعتباری و جعل پاسپورت بوده است خصوصاً آنکه روسیه در تعقیب مجرمان منفعلانه عمل نمود. این اقدامات هرچند اعمال اقتدار عمومی نیستند اما بدون کمک دولت هم امکان‌پذیر نبودند.[۳۴] معیارهای دیگری مانند هدفمند بودن و سازماندهی بودن تخلفات را

31. International Law Commission, Commentaries on the Draft Articles on Responsibility of States for Internationally Wrongful Acts, 2001, Article 8, Para. 6.

32. Ibid, Article 5, Para. 6.

33. Swedish Defense University with Preliminary Conclusions on 'Cyberattack against Georgia'. August 2008.

۳۴. برخی اوقات امارات حاکی از آن است که اقدام صورت‌گرفته منتسب به دولتی مشخص است مثلاً حملات رایانه‌ای به سایت‌های اداری جمهوری خودمختار تبت با توجه به سابقه طولانی دشمنی دولت مرکزی چین با جدایی‌طلبان تبت می‌توان ادعا نمود که این حملات منتسب به چین است اما دیدبان جنگ اطلاعاتی (IWM) که زیر نظر دانشگاه تورنتو فعالیت می‌کند احتمال داده است که این حملات برای بدنام کردن دولت چین از سوی دولت ثالثی صورت پذیرفته باشد. به این اقدامات در فضای سایبر استفاده از پرچم مصلحتی در فضای سایبر گفته می‌شود.

برای انتساب یک عمل متخلفانه در فضای سایبر به دولت مطرح کرده‌اند اما در تمام حالاتی که انتساب در معنای حقوق موضوعه احراز نشود از عبارت «هماهنگی» (coordination) استفاده می‌شود و نه کنترل (control).[۳۵]

در خصوص کنترل دولت بر شرکت‌های ارائه‌کننده خدمات اینترنتی باید توجه داشت که کمیسیون حقوق بین‌الملل در تفسیر ماده ۸ خاطرنشان می‌سازد که سه واژه دستور، هدایت و کنترل در هر قضیه باید با توجه به حقایق همان قضیه تفسیر شود.[۳۶] علی‌رغم رویکرد کلی کمیسیون حقوق بین‌الملل به دکترین نیکاراگوئه (کنترل مؤثر)، گفته شده است که به علت ماهیت خاص فضای سایبر و از جمله امکان نقض در لفاف دنیای مجازی، دکترین نیکاراگوئه مورد سوءاستفاده قرار خواهد گرفت و دکترین تادیچ (کنترل عمومی) مناسب‌تر خواهد بود.[۳۷] همچنین باید میان دو نقش شرکت‌های ارائه‌کننده خدمات اینترنتی قائل به تفکیک شد. زمانی این شرکت‌ها در نقش ناشر اطلاعات ظاهر می‌شوند و زمانی نقش توزیع‌کننده این اطلاعات را دارند. در واقع وقتی اطلاعات توزیع می‌شوند مانند مبادلات الکترونیکی و یا کالا این شرکت‌ها مسؤولیت کمی دارند چرا که متصدی سیستم نه اجازه بررسی اطلاعات را دارد و نه امکان آن را.[۳۸] زمانی که شرکت، توزیع‌کننده اطلاعات است به طور اولی نباید مسؤولیت دولت میزبان چنین شرکتی را مطرح نمود.[۳۹]

اما زمانی که نقض ارتکابی توسط یک دولت در بالادست صورت می‌پذیرد (دولتی که میزبان سرور ریشه‌ای است) دولت قربانی برای یافتن مسؤول نهایی چاره‌ای ندارد جز آنکه به دولت پایین‌دست‌تر از کشور میزبان سرور ریشه‌ای که انتساب به آن مسلم است رجوع نماید، سپس با رجوع به کشور میزبان شرکتی که تأمین‌کننده IP است به شرکت بعدی که پشتیبان شرکت قبلی است رجوع می‌کند. این روش (hop back) ادامه پیدا خواهد کرد تا شرکت یا

"Projecting Borders into Cyberspace", Security Focus, last modified April 28, 2009, http://www.securityfocus.com/columnists/500.

35. "Eneken Tikk et al., Cyber Attacks against Georgia: Legal Lessons Identified", Cooperative Cyber Defence Center of Excellence, NATO Unclassified, Version 1.0, 2008, 14. Last accessed May 17, 2017, http://www.ismlab.usf.edu/isec/files/Georgia-Cyber-Attack-NATO-Aug-2008.pdf.

36. International Law Commission, Ibid, Article 8, Para. 7.

37. Scott J. Shackelford, Scott J. Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International *Law*," *Berkeley Journal of International Law* 27 (2008): 234.

۳۸. حسن‌بیگی، پیشین، ۳۸.

۳۹. بعضاً شرکت‌های واسط و ارائه‌کننده خدمات اینترنتی در نقض حقوق بشر با دولت همدستی می‌کنند مانند همکاری یک شرکت اینترنتی در انگلستان با پلیس انگلستان در نقض کنوانسیون اروپایی. هیک استون، *حقوق بشر و اینترنت*، ترجمه و تحقیق سید قاسم زمانی و مهناز بهراملو (تهران: نشر خرسندی، ۱۳۸۶)، چاپ ۱، ۱۹۷.

کشوری که مسؤول نهایی است مشخص شود. اما این روش به علت زمان‌بر بودن و همچنین به علت نیاز به همکاری کشورهای دیگر موجب تأمین حقوق نقض‌شده نمی‌شود برای همین نویسندگانی به اعمال اصل تعقیب فوری (hot pursuit) در فضای سایبر اشاره کرده‌اند. در واقع فضای سایبر به عنوان چهارمین فضا پس از دریای آزاد، فضای ماورای جو و سرزمین‌های مشمول معاهده شینگن به عنوان فضایی تلقی می‌شود که دولت قربانی یا متعهد به تضمین حقوق بشر می‌تواند بدون کسب اجازه از کشورهای بالادست، از حوزه صلاحیتی کشورهای دیگر عبور نموده و دست به تعقیب فوری بزند و علیه شرکت یا کشور متخلف مثلاً دست به اقدام متقابل بزند.[۴۰]

در برخی موارد که نقض حقوق بشر از سوی بازیگران غیردولتی و به طور مستمر تحقق پذیرد آیا می‌توان مسؤولیت دولت میزبان شرکتی که توزیع‌کننده این تخلفات است را مطرح نمود؟ به نظر می‌رسد با تأسی به اصل تلاش معقول (due diligence) برای جلوگیری از نقض حقوق بشر چنانچه دولتی از این امر اطلاع پیدا نمود که اطلاعات مخرب به حال حقوق بشر در حال عبور از شرکت‌ها یا سرورهای موجود در کشورش است موظف به جلوگیری از آن است. در این موارد مسؤولیت غیرمستقیم دولت قابل طرح است.[۴۱]

تعریف مأمورین دولتی در فضای سایبر نیز تغییر یافته است. در حالی که در حقوق مسؤولیت بین‌المللی، زمانی عملی را منتسب به دولت می‌دانستیم که مأمور دولتی در زمان مأموریت یا با امکانات مأموریت دست به اقدام متخلفانه می‌زد امروزه این امکان وجود دارد که مأموران دولتی از طریق رایانه‌های خانگی خود با استفاده از رمز عبور دست به نقض حقوق بشر بزنند.[۴۲] آیا می‌توان گفت مفهوم مأمور دولتی در فضای سایبر دچار تحول مفهومی شده است؟

۳-۲- انتساب عمل شرکت‌های خصوصی ارائه‌کننده خدمات اینترنتی به دولت در حقوق آمریکا و اروپا

در حقوق آمریکا اصلی وجود دارد که طبق آن، مدیر برای اعمال زیردستانش مسؤولیت دارد. به این «مسؤولیت نیابتی» می‌گویند. در مفهومی وسیع‌تر، طرف ثالثی که «حق، اهلیت یا

40. Graham H. Todd, "Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric *Definition*," *Air Force Law Review* 64 (2009): 65-103.

41. Eneken Tikk et al., op. cit., 23.

۴۲. در خصوص تغییر مفهوم خودی و غیرخودی در فضای سایبر نک: زهرا خداقلی، *جرایم کامپیوتری* (تهران: نشر آریان، ۱۳۸۳)، ۴۱.

وظیفه نظارت» بر فعالیت‌های مختلف را داشته است اما از انجام آن طفره رفته یا غفلت کرده است با شرایطی مسؤول اعمال متخلف تلقی می‌شود.[۴۳] دیوان عالی آمریکا اخیراً در پرونده شرکت استودیوی فیلمبرداری مترو ـ گلدن‌مایر علیه گراک استر بیان داشت که چنانچه نقض کپی‌رایت با آگاهی توزیع‌کننده از نقض گسترده صورت گرفته باشد، توزیع‌کنندگان نرم‌افزار نیز مسؤول خواهند بود با این حال اضافه نمود که مسؤولیت مدیر سیستمی که دیگران تحت نظارت او حقوق آمریکا را نقض کرده‌اند بیشتر از مسؤولیت ارائه‌دهنده اینترنت است.[۴۴] این رویه باری را بر دوش بخش‌های خصوصی که کنترل عمومی بر اینترنت دارند می‌گذارد که بر سازه‌های تحت مدیریتشان نظارت پلیسی داشته باشند تا از تخلفات مهم و بالقوه جلوگیری کنند.[۴۵] همچنین چنانچه دادگاه در پرونده هندریکسون علیه شرکت ای‌بِی (eBay) مطرح کرد، شرکت‌ها در قبال ارائه خدمات اینترنتی که از تخلف و تخطی کاربران بی‌اطلاع است، مسؤولیت ثانوی ندارند.[۴۶]

بنابراین مشاهده می‌شود که آمریکا به عنوان میزبان دو سرور ریشه‌ای اینترنت با احاله مسؤولیت شرکت‌های ارائه‌کننده خدمات اینترنتی به خود آنها، از خود سلب مسؤولیت بین‌المللی کرده است.[۴۷] لذا بررسی وضعیت حقوقی این شرکت‌ها در هر کشوری بررسی اوضاع و احوال خاص آن کشور را می‌طلبد.

کنوانسیون جرایم سایبری مصوب شورای اروپا نیز در ماده ۱۲ کشورهای عضو را ملزم به تصویب قوانینی برای طرح مسؤولیت اشخاص حقوقی از جمله شرکت‌ها می‌کند. این ماده در صورتی که شرکت زیر نظر مستقیم یک شخص حقیقی عمل نکرده باشد در کلیت خود مسؤول نقض‌های ارتکابی در فضای سایبر تلقی می‌شود که این مسؤولیت می‌تواند کیفری، مدنی یا اداری باشد. لذا در حقوق کشورهای اروپایی نیز همچون حقوق آمریکا با احاله مسؤولیت ارتکاب جرم یا نقض حقوق بشر در فضای سایبر به شرکت‌های ارائه‌کننده خدمات اینترنتی از دولت سلب مسؤولیت شده است.

---

43. Meyer v. Holley, 537 U.S. 280 (2003).

44. Metro-Goldwyn-Mayer Studios, Inc., v. Grokster, Ltd., 545 U.S. 913 (2005).

۴۵. دادگاه آمریکا در پرونده مرکز دموکراسی و تکنولوژی علیه پاپرت بیان داشت که شرکت‌ها (خصوصاً ارائه‌دهندگان خدمات اینترنتی) در این رسالت نباید راه افراط پیش بگیرند و حتی وب‌سایت‌های بدون تقصیر را تعطیل کنند.

Ctr. for Democracy & Tech. v. Pappert, 337 F. Supp. 2d 606 (E.D. Pa. 2004).

46. Hendrickson v. eBay, Inc., 165 F. Supp. 2d 1082 (C.D. Cal. 2001).

۴۷. نک: پاراگراف ۵ تفسیر ماده ۶ طرح مسؤولیت بین‌المللی دولت‌ها

۴- موارد نقض حقوق بشر در فضای سایبر

پس از اثبات امکان انتساب یک عمل به دولت لازم است به نقض‌های حقوق بشری قابل ارتکاب در فضای سایبر اشاره شود.

۴-۱- آزادی بیان:[۴۸] آزادی بیان از اصول اولیه حقوق بشر است که در اعلامیه جهانی حقوق بشر و میثاق حقوق مدنی و سیاسی و بسیاری از قوانین اساسی دنیا تصریح شده است. آزادی بیان بدین معنی است که افراد یک جامعه حق دارند نظر، عقیده، مذهب و افکار سیاسی خود را صرف‌نظر از تفاوت‌های نژادی، قومی و مذهبی با دیگران به اشتراک گذارند. محیط سایبر محیطی است که داده‌ها به صورت صفر و یک به سرعت در حال تبادل هستند و بیش از پیش در حال کمرنگ کردن مرزهای فیزیکی حاکمیت‌ها هستند. طبیعی است که حکومت‌ها گاه ابزار موجد این فضا یعنی رایانه را تهدیدی برای خود انگارند. از جمله اقدامات دولت در موارد احساس خطر، فیلتر کردن یک وب‌سایت و یا قطع کلی اینترنت یا پایین آوردن ظرفیت اینترنت است که دسترسی به اطلاعات را مشکل می‌سازد.[۴۹]

شاید تصور شود حقوق مربوط به آزادی بیان در رسانه‌های پیشین و سنتی قابل قیاس و به کارگیری کامل در این فضا نیست چرا که این رسانه جدید حداقل سه تفاوت عمده با رسانه‌های سنتی دارد: اول امکان مبادله همزمان اطلاعات (interactive) در حالی که رسانه‌های قبلی یک‌طرفه بودند، دوم امکان ارسال حجم انبوه اطلاعات در واحد زمان و سوم عدم امکان کنترل مؤثر تکنیکی و حقوقی در شرایط حاضر.[۵۰] اما با این حال مکانیسم‌هایی برای حمایت از نقض آزادی بیان در فضای سایبر قابل تأسی هستند. از جمله ضمیمه دوم اتحادیه بین‌المللی مخابرات (ITU) در تعریف مداخله زیان‌بخش ماده ۴۵ اساسنامه اتحادیه بیان می‌دارد «مداخله‌ای که خدمات هدایت رادیویی یا دیگر خدمات ایمنی را به خطر اندازد یا خدمات ارتباطی رادیویی که طبق قوانین رادیویی عمل می‌کند را متلاشی کند، مسدود سازد یا در آن اختلال مستمر ایجاد نماید». این «خدمات ارتباطی» شامل حق آزادی بیان نیز

48. Freedom of Expression

۴۹. هرچند گفته می‌شود ماهیت اینترنت به گونه‌ای است که عمل سانسور را به واقع غیرممکن می‌سازد زیرا در صورت جلوگیری از عبور پیامی از یک کانال پیام می‌تواند از کانال دیگری عبور نماید. استون، پیشین، ۴۲. اما این امکان تنها در خصوص فیلتر امکان‌پذیر است و نه در خصوص قطع یا کاهش ظرفیت اینترنت.

۵۰. همچنین ادعا شده که چون اتصال یک پیام در شبکه‌های رایانه‌ای به علت حرکت الکترون‌ها در داخل سیستم محقق می‌شوند و نه ناشی از حرکت جوهر بر روی کاغذ بنابراین حق آزادی بیان بر آن شامل نمی‌شود. آیکاو، سیگر، وان استروچ، پیشین، ۲۶.

می‌شود و کشورها نباید در جریان آزاد اطلاعات اختلال ایجاد نمایند. لکن حق مذکور در اساسنامه ITU متعلق به دولت‌هاست و نه افراد. از این رو دولت‌ها مسؤولیت مضاعف دارند که در صورت قطع ارتباطات از سوی دولت بالادستی برای حمایت از حقوق شهروندانش به این مقرره استناد جویند. علاوه بر این میثاق مدنی و سیاسی و کنوانسیون‌های اروپایی، آمریکایی و آفریقایی حقوق بشر هم متضمن این حق هستند که در صورت احراز شرایط، قابل توسل توسط افراد است. لازم به ذکر است دادگاه اروپایی حقوق بشر، کمیسیون آمریکایی حقوق بشر، کمیسیون آفریقایی حقوق بشر و مردم، دادگاه آفریقا و تا حدودی دیوان بین‌المللی اروپایی حق رجوع مستقیم برای طرح شکایت را به سازمان‌های غیردولتی در مواردی که قربانی مستقیم نقض حقوق قرار گرفته باشند، اعطاء کرده‌اند.[۵۱]

در اصل بیست و چهارم قانون اساسی ایران از آزادی نشریات و مطبوعات سخن رفته اما اشاره‌ای به آزادی فناوری اطلاعات نشده است اما باید دانست موارد ذکرشده مصادیقی هستند برای تحقق آزادی بیان.[۵۲] بنابراین مثلاً در صورت نقض غیرقانونی آزادی فناوری اطلاعات از سوی دولت افراد می‌توانند به دیوان عدالت اداری رجوع کرده و خواستار اعلام عدم تطابق حکم دولتی با قانون اساسی شوند. باید توجه داشت آزادی بیان در عرصه فضای سایبر دارای محدودیت‌هایی است مانند حریم خصوصی دیگران، حمایت از اسرار تجاری و منافع ملی. مورد اخیر شامل امنیت ملی، سیاست‌های اقتصادی دولت، احتمال وقوع جرم و حفاظت از محیط زیست می‌شود.[۵۳] ماده ۱۹ اساسنامه اتحادیه مخابرات نیز اصل عدم مداخله در خدمات رادیویی را در مورد تنظیم فعالیت‌های امنیتی، قابل نقض می‌داند.[۵۴] در کل در خصوص آزادی بیان در فضای سایبر می‌توان گفت این اصل وجود دارد: «هرچه در offline غیرقانونی است در online نیز غیرقانونی است».

۴-۲- آزادی اطلاعات:[۵۵] سازمان توسعه و همکاری اقتصادی در فهرستی که در سال ۱۹۸۶ در خصوص جرایم ارتکابی در فضای سایبر ارائه داد و اتحادیه اروپا در طرح سال ۲۰۰۲ خود به آزادی ارتباطات در فضای سایبر اشاره نمودند.[۵۶] این حق که صریحاً در اسناد حقوق بشری

51. Ann-Karin Lindblom, *Non-Governmental Organizations in International Law* (Cambridge: Cambridge University Press, 2005), 162-164.

۵۲. حسن‌بیگی، پیشین، ۳۷.

۵۳. همان، ۲۳۸.

54. Scott J. Shackelford, Ibid.

55. Freedom of Information

56. Council Framework Decision 2005/222/Jha

نیامده است را می‌توان از ماده ۱۹ اعلامیه جهانی حقوق بشر مصوب ۱۹۴۸ استنباط نمود. این ماده به افراد حق داده به هر وسیله ممکن از دریافت و انتشار اطلاعات آزاد باشند. اعلامیه ژوهانسبورگ این حق را به رسمیت شناخته است و تنها در مواردی که امنیت ملی کشوری ایجاب کند، طبق قانون قابل تحدید است.[۵۷] این حق در فضای سایبر به بهترین نحو از طریق ایجاد دولت الکترونیک محقق می‌شود.

سؤالی که باقی می‌ماند این است که اگر یکی از شرکت‌های تأمین خدمات اینترنتی مانع دسترسی به اینترنت شود افراد برای شکایت می‌توانند به آیکان رجوع کنند؟ در حال حاضر آیکان فقط در رابطه با شکایاتی مانند نام دامنه و ارسال اسپم رسیدگی می‌کند، اما اگر کسی از خود آیکان شکایت داشت به کجا می‌تواند رجوع کند؟ هیچ مرجعی بر آیکان نظارت نمی‌کند و در نهایت همه باید در مقابل آن تسلیم شوند.[۵۸]

۴-۳- حریم خصوصی: اکثر کشورها از حریم خصوصی افراد حمایت به عمل می‌آورند. نقض این حق به دو صورت جمع‌آوری اطلاعات شخصی و یا استراق سمع (wire trapping) صورت می‌گیرد.[۵۹] چهار جرم از هر پنج جرم رایانه‌ای بررسی‌شده به وسیله اف بی آی در سال ۱۹۹۳ شامل دسترسی بدون اجازه رایانه‌ها از طریق اینترنت بوده است.[۶۰] رهنمودهای سازمان همکاری و توسعه اقتصادی، اینترپل و «کنوانسیون اروپایی حمایت از افراد در رابطه با پردازش خودکار داده‌های شخصی» نیز به این حق اشاره دارند.[۶۱] در این خصوص کشورها دو وظیفه «تضمین» و «حمایت» به عهده دارند. وظیفه تضمین به این خاطر است که

---

۵۷. گفتنی است تاکنون بیش از چهل کشور جهان در این زمینه قوانینی تصویب کرده‌اند. حتی بعضی کشورها نظیر انگلستان سعی کرده‌اند با اصلاح قوانین زیربنایی، نظیر قوانین راجع به حمایت از داده‌ها (حریم خصوصی)، زمینه‌های قانونی دسترسی افراد به اطلاعات را هرچه بیشتر فراهم کنند. امیرحسین جلالی فراهانی، «پیشگیری وضعی از جرایم سایبر در پرتو موازین حقوق بشر»، مجله فقه و حقوق ۶ (۱۳۸۴)، ۱۴۹. و یا سوئد و آمریکا قوانینی تصویب کرده‌اند که طبق آن به شهروندان حق می‌دهد به اطلاعات دولتی دسترسی پیدا کنند. حسن‌بیگی، پیشین، ۲۳۸.

۵۸. حسن‌بیگی، پیشین، ۳۵.

۵۹. مانند اقدام دولت بوش پس از ۱۱ سپتامبر ۲۰۰۱ که به شنود غیرقانونی مکالمات تلفنی و ایمیل‌های شهروندان امریکایی دست زد.

JAMES RISEN, and ERIC LICHTBLAUDEC, "Bush Lets U.S. Spy on Callers without Courts, 2005" (Politics, WASHINGTON: The New York Times, 2005), last modified December 16, 2005, http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html?_r=0, See at 17 May 2017.

۶۰. آیکاو، سیگر، وان استروچ، پیشین، ۴۳.

۶۱. حسن‌بیگی، پیشین، ۱۸۳.

پالس‌های الکترومغناطیسی ساطعه از سخت‌افزارهای رایانه‌ای امکان رمزگشایی و افشای اطلاعات خصوصی را می‌دهد که دولت‌ها باید به نصب و آموزش وسایل محافظ اقدام نمایند. در رابطه با وظیفه حمایت نیز باید از اجبار شرکت‌های ارائه‌کننده خدمات مبنی بر تهیه لیست واژگان کلیدی و حساس و جمع‌آوری خودکار اطلاعات دست بردارند[۶۲] و در صورت نقض از سوی افراد یا شرکت‌ها امکان تعقیب حقوقی آنها را در دادگاه‌های خود فراهم آورند. در صورت عدم امکان توسل به دادرسی منصفانه در داخل برای جبران این نقض می‌توان به نهادهای بین‌المللی از باب نقض ماده ۱۴ میثاق بین‌المللی مدنی و سیاسی (تعهد به رسیدگی منصفانه) علیه دولت طرح دعوا نمود هرچند نتوان از باب نقض حریم خصوصی طرح دعوا کرد.[۶۳]

۴-۴- حق مالکیت و کار: بسیاری از افراد و شرکت‌ها اینک فضای سایبر را عرصه مناسبی برای فعالیت‌های تجاری و سرمایه‌گذاری می‌دانند. در آینده نه چندان دور دامنه‌های موجود در فضای سایبر همچون مستغلاتی ارزشمند مبادله خواهند شد. شرکت‌ها در ابتدایی‌ترین شکل خود دست به قرارداد با دولت میزبان برای تأمین سخت‌افزارهای لازم جهت ارائه اینترنت می‌زنند و از این طریق دامنه‌ها و وب‌سایت‌هایی را به مشتریان خود اختصاص می‌دهند. افراد نیز در محیط سایبر دست به خرید و فروش کالا و حتی بنگاه‌های معاملاتی مجازی زده و فراتر از اینها به خرید و فروش سهام در بازارهایی چون فورکس (Forex) می‌پردازند. چنانچه دولتی بدون توجیه قانونی در روند این بازار مجازی اختلال وارد آورد این احتمال مطرح می‌شود که افراد و شرکت‌های متضرر می‌توانند به طرح شکایت از جهت نقض حق مالکیت و کار بپردازند. سؤال اساسی در این زمینه این است که آیا می‌توان پروکسی بدون دلیل موجه یک سایت را مصادره غیرقانونی تلقی نمود؟

مسئله وقتی غامض می‌شود که یک کشور بالادست موجب اختلال در اینترنت کشورهای زیردست شود و از این طریق به سرمایه‌گذاران و مالکین خصوصی در فضای سایبر لطمه وارد آورد. چنانکه این سرمایه یا ملک از دست رفته قابل جبران نباشد به نوعی سلب مالکیت

---

۶۲. طبق این فناوری هنگامی که واژه‌نامه‌ای راه‌اندازی می‌شود، رایانه‌ها رونوشتی از مطالب را به صورت خودکار به کشوری که واژه‌نامه آن مورد بحث است از طریق معینی ارسال می‌کنند. محتویات مکالمات تلفنی، فاکس و پست الکترونیکی بعداً به میز کار مأمورین امنیتی انتقال یافته و مورد مطالعه و ارزیابی قرار می‌گیرند. سید قاسم زمانی و مهناز بهراملو، مترجم، *حقوق بشر و اینترنت* (تهران: نشر خرسندی، ۱۳۸۶)، چاپ ۱، ۴۷.

۶۳. این امکان رجوع من‌باب نقض ماده ۱۴ میثاق مبنی بر دسترسی افراد به دادرسی عادلانه در تمام نقض‌های امکان‌پذیر در حوزه سایبر قابل اعمال است.

مجازی رخ داده است که برای مشروعیت یا نامشروعیت آن باید قائل به تفکیک میان شهروندان و بیگانگان شویم. چنانچه می‌دانیم مصادره اموال بیگانگان تحت شرایط مضیق‌تری نسبت به مصادره اموال شهروندان امکان‌پذیر است. از این رو کاربران و شرکت‌هایی که مالکیت آنها سلب گردیده است چنانچه نسبت به دولت مرتکب تابعیتی بیگانه داشته باشند می‌توانند مطالبه غرامت نمایند. قطعنامه‌های ۱۸۰۳ و ۳۲۸۱ مجمع عمومی از این افراد حمایت می‌کند.[۶۴] کمیته حقوق بشر اقتصادی، اجتماعی و فرهنگی و محاکم منطقه‌ای حقوق بشر نیز پذیرای شکایت آنها خواهند بود. سازمان بین‌المللی کار نیز با فراهم کردن امکان حضور نمایندگان کارگزاران و سازمان‌های غیردولتی مکان مناسبی برای طرح مشکلات کسانی است که کار خود را صرفاً در محیط سایبر متمرکز کرده‌اند و از این اقدامات صدمه می‌بینند. چنانچه خواسته دعوا ارزش سرمایه‌ای داشته باشد ایکسید نیز مرجع مناسبی برای حل اختلافات است.[۶۵] حقوق معنوی در اینترنت نیز از دیگر مشتقات حق بر مالکیت در اینترنت است که توسط مکانیسم داوری در وایپو و گات قابل پی‌گیری خواهد بود.[۶۶]

۴-۵- حق تعیین سرنوشت: حق تعیین سرنوشت که مورد تأکید قطعنامه‌ها و اسناد بسیاری از جمله میثاقین قرار گرفته ابعاد گوناگونی دارد. حق تعیین سرنوشت در بعد سیاسی آن تنها به مردمی تعلق خواهد گرفت که مشمول تعریف مردم بومی (indigenous people) باشند.[۶۷] این حق به خودمختاری سیاسی این مردم اشاره دارد. در سطحی وسیع‌تر این حق به کل مردم ساکن در یک دولت حق داشتن دموکراسی و فقدان استعمار، نژادپرستی و اشغال را

64. General Assembly Resolution, 1803 (XVII), 1996; 3281 (XXIX), 1974.

۶۵. ایکسید در قضیه CSOB علیه جمهوری اسلواکی بیان داشت که برای رسیدگی به یک دعوا باید به کلیت عملیات نگریست و نه صرفاً به یک معامله خاص. اگر کلیت عملیات جنبه سرمایه‌گذاری داشته باشد و هرچند ناشی از یک سرمایه‌گذاری مستقیم نباشد ایکسید صلاحیت رسیدگی خواهد داشت.

"CESKOSLOVENSKA OBCHODNI BANKA, A.S. v. SLOVAK REPUBLIC (ICSID CASE No. ARB/97/4)", icsid.worldbank, last accessed May 17, 2017, http://icsid.worldbank.org/ICSID/FrontServlet?requestType=CasesRH&actionVal=showDoc&docId=DC555&caseId=C160

لذا سرمایه‌گذاری از طریق اینترنت در بازارهای بورس یا زیرساخت‌های اطلاعاتی می‌تواند مصداق سرمایه‌گذاری در فضای سایبر تلقی شود. به طور مثال دستورالعمل ۱۳۲۳۱ دولت بوش در سال ۲۰۰۱ تحت عنوان «حمایت از زیرساخت‌های حیاتی در عصر اطلاعات» بیان می‌دارد که انقلاب فناوری اطلاعات کارکرد تجارت را تغییر داده است. با این حال سرمایه‌گذاری امنیتی در اینترنت و سرمایه‌گذاری سنتی تفاوت‌هایی دارند.

Lawrence A. Gordon, Martin P. Loeb and William Lucyshyn, *Economic Aspects of Controlling Capital Investments in Cyberspace Security for Critical Infrastructure Assets*, available at: http://www.cpppe.umd.edu/rhsmith3/papers/Final_session7_lucyshyn.loeb.gordon.pdf.

66. Henry H. Perritt. JR., Ibid, 106.

67. General Assembly Resolution, 10612, (2007).

می‌دهد. دموکراسی سایبری متضمن فضایی برای کاهش بوروکراسی، امکان فعالیت سازمان‌های غیردولتی، ارتباط آسان با نهادهای دولتی، رأی‌گیری الکترونیکی، پارلمان الکترونیکی، دولت الکترونیکی و غیره است.

بعد دیگر حق تعیین سرنوشت که غیر قابل انکار است، حق تعیین سرنوشت فرهنگی است. این حق به ملت‌ها در کل و به اقلیت‌ها در جزء حق می‌دهد تا بتوانند فرهنگ‌های متمایز خود از جمله زبان و مذهب را حفظ کنند. در کل می‌توان گفت فرهنگ حاکم بر فضای سایبر نمایانگر مصرف‌گرایی، اصول اخلاقی بی‌ثبات و روند آمریکایی شدن فرهنگ است. این روند موجب نگرانی کشورهای غیردموکراتیک، سوسیالیست و دینی شده است. در هر صورت حاکم شدن هر فرهنگی بر فضای سایبر که تجلی جهانی شدن ارتباطات است می‌تواند اعتراض خرده‌فرهنگ‌های دیگر را به دنبال داشته باشد. اما در سطح پایین‌تر از بین بردن فرهنگ اقلیت در اینترنت نیز نادرست است. به طور مثال اقدام گوگل به حذف نام خلیج فارس[۶۸] از موتور جستوجوگرش و یا نپذیرفتن نام ایمیل‌هایی که در آن کلمه جلاله الله (Allah) بود توسط یاهو،[۶۹] بیانگر تبعیض و نقض حق تعیین سرنوشت است. از این رو می‌توان علیه دولت‌هایی که بر شرکت‌های مذکور وظیفه نظارت داشته‌اند در کمیته حقوق بشر مدنی و سیاسی و کمیته اجتماعی، اقتصادی و فرهنگی طرح دعوا نمود.

۴-۶- جنایت علیه بشریت: مسئله این است که اگر کشوری به طرح مسائل نژادپرستی یا نسل‌کشی اقدام نماید و طیف وسیعی از کاربران را به اینگونه اعمال دعوت کند آیا می‌توان آن را مشمول جنایت علیه بشریت و ژنوسید مذکور در کنوانسیون‌های ۱۹۴۸ و ۱۹۶۵ و اساسنامه دیوان بین‌المللی کیفری دانست؟ هرچند امکان تحقق چنین امری دور از ذهن نیست و چه‌بسا مواردی هم قبلاً تحقق یافته[۷۰] اما باید توجه داشت مسؤولیت قابل پیگرد در این نوع از نقض دو مسؤولیت موازی به همراه دارد: یکی مسؤولیت غیرکیفری دولت و دیگری مسؤولیت کیفری افراد. مسؤولیت دولت در نهادهای بشری پیش‌گفته قابل تعقیب

68. See "Iran criticizes Google for nomenclature of the Persian Gulf", Tech, last accessed May 17, 2017, http://tech.firstpost.com/news-analysis/iran-criticizes-google-for-nomenclature-of-the-persian-gulf-27928.html.

69. "Is Yahoo Banning Allah?" Kallahar's Place, last accessed May 17, 2017, http://zoomq.qiniudn.com/ZQScrapBook/ZqSKM/data/20060222184919/index.html.

۷۰. سه رهبر رواندایی به اتهام انتشار و پخش شعارها و تصاویری که فجایع شدیدی را ایجاد کرد و شدت بخشید محکوم به تحریک به نسل‌کشی شدند.

Prosecutor v. Nahimana, Barayagwiza, & Ngeze, Case No. ICTR-99-52-T, Judgment and Sentence (Dec. 3, 2003).

است اما در طرح مسؤولیت فردی در دیوان بین‌المللی کیفری دو مانع وجود دارد: یکی شرایط اضافی برای تحقق جنایت مانند گستردگی و سازمان‌یافتگی و دیگری اینکه طرح دعوا باید از سوی یک دولت و یا دادستان و یا شورای امنیت صورت گیرد و نه فرد قربانی.

در چارچوب دیوان بین‌المللی کیفری در دو مورد مسؤولیت فردی ناشی از فعالیت در اینترنت قابل تصور است: یکی تحریک به نسل‌کشی و دیگری طبق ماده ۷ اساسنامه که طبق آن هرگونه صدمه شدید و گسترده به سلامت جسمی و روحی جرم است. کنوانسیون نسل‌کشی، «نسل‌کشی» را اینگونه تعریف می‌کند: هرگونه شروع به جرم «یا عملی که با هدف نابودسازی تمام یا قسمتی از یک گروه ملی، قومی، نژادی یا دینی ارتکاب یابد»[۷۱]. همچنین ماده ۹ صریحاً تعهدی را بر کشورها برای جلوگیری از نسل‌کشی بار نمی‌کند. این تا زمانی بود که دیوان بین‌المللی دادگستری چنین تعهدی را در رأی اخیر خود درباره نسل‌کشی بوسنی صادر نکرده بود. دولت‌هایی که اقدام به حملاتی سایبری می‌کنند که فجایع مشابهی را ایجاد می‌کند یا از آن حمایت می‌کنند باید برای این جنایت مسؤول قلمداد شوند. باید متذکر شد که تعهد به جلوگیری از تحریک به نسل‌کشی به علت رویه‌های دولتی و قضایی متباین، هنوز امری مغشوش و نامعلوم است.[۷۲]

۴-۷- آزادی اجتماع: هرچند آزادی اجتماع مورد تأیید میثاقین قرار گرفته است اما باید توجه داشته باشیم که قطعنامه ۱۹۹۶/۳۱ اکوسوک در تعریف سازمان‌های بین‌المللی غیردولتی از عنصر وجود «اداره» سخن به میان می‌آورد و از این رو به وجود یک دفتر در عالم واقعی اشاره می‌کند.[۷۳] هرچند برخی کشورها جهت اعطای مجوز به سازمان‌های بین‌المللی غیردولتی این عنصر را لازم نمی‌دانند اما آنچه اهیمت دارد این است که بدانیم جلوگیری یک دولت از تشکیل یک سازمان غیردولتی «مجازی» در راستای رهنمود اکوسوک است چرا که یک سازمان غیردولتی مجازی لزوماً بین‌المللی نیز هست. علت این امر به ماهیت فضای سایبر برمی‌گردد که در آن مرزها تبدیل به الکترون‌های غیر قابل کنترل می‌شوند.

---

۷۱. طبق ماده ۲، نسل‌کشی شامل اعمال زیر می‌شود: (الف) کشتن اعضای یک گروه؛ (ب) ایراد صدمه جدی فیزیکی یا روانی به اعضای یک گروه؛ (ج) تحمیل متعمدانه شرایطی بر یک گروه که منجر به لطمه فیزیکی در تمام یا بخشی از آنها شود؛ (د) اتخاذ تدابیری با هدف جلوگیری از زاد و ولد در گروه مذکور؛ (ه) انتقال اجباری کودکان از یک گروه به گروهی دیگر.

Convention on the Prevention and Punishment of the Crime of Genocide, December, 9 1948, 78 U.N.T.S.

72. Scott J. Shackelford, Ibid.

73. ESC Res.1996/31, July 25, 1996.

۴-۸- حریم جنسی کودکان: یکی از مسائل مبتلابه اینترنت هرزه‌نگاری کودکان و زنان است چنانچه به گفته اینترپل، اینترنت مهم‌ترین عامل در سوءاستفاده جنسی از کودکان و هرزه‌نگاری از آنها به شمار می‌رود.[۷۴] تنها عنوان مجرمانه‌ای که توسط امضاءکنندگان «کنوانسیون اروپایی جرایم سایبر» مصوب ۲۰۰۱ بدون هیچ حق شرطی پذیرفته شد پورنوگرافی کودکان بود. همین‌طور طبق ماده ۳۴ کنوانسیون حقوق کودک طرف‌های معاهده متعهدند کلیه اقدامات مقتضی را برای جلوگیری از تشویق یا وادار نمودن کودکان به شرکت در فعالیت جنسی، خودفروشی یا هرزه‌نگاری به عمل آورند. در فضای سایبر دو نوع مشکل در ارتباط با کودکان وجود دارد: یکی محتویاتی که قانونی‌اند اما برای کودکان مضرند و دیگری محتویاتی که غیرقانونی‌اند و البته مضرند.[۷۵] در هر دو حوزه ابهامات و پیچیدگی‌هایی وجود دارد. در کل دو الگو برای برخورد با اینگونه مسائل طرح شده است. یکی اینکه فضای سایبر را همچون رسانه‌های سنتی بدانیم و از این رو تابع قوانین ملی و دیگر اینکه فضای سایبر را رسانه‌ای برای برقراری ارتباط خصوصی میان افراد و گروه‌ها بدانیم. با این حال هر دو الگو خصیصه جهانی بودن و یکپارچه بودن فضای سایبر را نادیده می‌گیرند.

مشکل اصلی این است که حتی اگر یک کشور به تعریف هرزه‌نگاری در قوانین ملی خود دست زد و حتی آن را در محیط اینترنت به اجرا در آورد ممکن است با تعریف صورت‌گرفته از هرزه‌نگاری در کشوری دیگر مغایر باشد و از این رو به اعتراضات حقوق بشری در آن سرزمین دامن زند.[۷۶] چرا که کنوانسیون حقوق کودک سن رضایت فعالیت جنسی را ۱۸ سال می‌داند در حالی که سن رضایت از ۱۲ سال در کشور فیلیپین تا ۲۲ سال در ماداگاسکار در نوسان است.[۷۷] این مشکل در خصوص فعالیت جنسی بزرگسالان نیز قابل طرح است. چرا که معدودی از حقوق کشورها انتشار اینگونه تصاویر را نیز ممنوع ساخته‌اند. این مشکل به ظاهر حل‌نشدنی (حداقل تا زمان توافق جامعه بین‌المللی در خصوص صلاحیت بر فضای سایبر) بیش از هر چیز بهم پیوستگی منافع و حقوق ملت‌ها و دولت‌ها را در فضای سایبر نشان می‌دهد. مشکلی که در نقض‌های پیشین کمتر مطرح است.

---

74. Fournier Saint Maura Agnes, "Sexual Abuse of Children on the Internet: a New Challenge for INTERPOL" (Paper Prepared for the Expert Meeting on Sexual Abuse of Children, Geneva, UNESCO, January 17-18, 1999).

۷۵. زمانی و بهراملو، پیشین، ۲۳۶.

76. Chris Reed and John Angel, *Computer Law* (US: Oxford University Pres, 2007), 265.

77. https://www.ageofconsent.net/world.

هرچند این اعمال کمتر قابل انتساب به دولت هستند اما دولت‌ها از باب نقض تکلیفشان به تضمین برای حمایت از حقوق کودک مسؤول خواهند بود. علاوه بر دولت‌ها، یونیسف، یونسکو و اینترپل نیز موظف به تضمین حمایت از این حقوق هستند. در مورد محتویاتی که از نظر حقوق داخلی برخی کشورها قانونی‌اند اما در هر صورت مضر به حال کودکان است چالش دیگری برای این دولت‌ها وجود دارد. دولت‌ها در این خصوص در چالش میان حق آزادی بیان و حق حریم جنسی کودکان قرار دارند. این مشکلات ضرورت همکاری بین‌المللی در جلوگیری از ترویج و اشاعه اینگونه فعالیت‌ها در فضای سایبر را دوچندان می‌کند.[۷۸]

نتیجه

همان‌قدر که اینترنت برای ترویج حقوق بشر در اختیار کاربران آن قرار دارد به همان اندازه می‌تواند عرصه‌ای باشد برای نقض حقوق بشر. در حالی که حقوق بشر افراد در فضای واقعی تنها توسط کشورهای میزبان منافع آنها نقض می‌شود، حقوق بشر افراد در فضای سایبر می‌تواند از سوی تمام کشورهای حاضر در این فضا نقض شود. به همین علت قربانیان نقض حقوق بشر در فضای سایبر از یک سو با پیچیدگی انتساب اعمال متخلفانه بین‌المللی رو به رو هستند و از سوی دیگر با ابهام در حقوق بشر خود در فضای سایبر. همان‌طور که مشاهده شد تعارضات بیشتری میان قواعد حقوق بشر در فضای سایبر وجود دارد بی‌آنکه راه‌حلی بین‌المللی برای آن اندیشیده شده باشد. علاوه بر این، اسناد مختص به حقوق بشر در فضای سایبر به قدری اندک یا ناقص هستند که خلأ وجود ساز و کاری مناسب و یکپارچه برای حمایت از حقوق بشر در فضا احساس می‌شود.

مناسب‌ترین ساز و کار حمایت از حقوق بشر ساز و کاری است که اولاً قابل رجوع توسط خود افراد قربانی باشد و ثانیاً قابل دسترسی باشد. بهترین مثال این مکانیسم سایت‌هایی هستند که امکان طرح شکایت در آنها از طریق اینترنت فراهم شده است. برخی از این پایگاه‌های اینترنتی مانند مرکز شکایت جرایم اینترنتی آمریکا ملی هستند هرچند ضمانت‌اجرای بین‌المللی دارند و برخی از این پایگاه‌های اینترنتی مانند مرجع حل اختلاف نام مشترک دامنه‌ها (UDRP)، بین‌المللی هستند. مناسب است نهادهای حقوق بشری مانند شورای حقوق بشر سازمان ملل متحد، کمیته حقوق کودک و زنان، کمیته حقوق سیاسی و مدنی و کمیته حقوق اقتصادی، اجتماعی و فرهنگی با انعقاد موافقتنامه‌هایی با کشورهای

78. Paul Edward Geller, "Conflicts of Laws in Cyberspace: Rethinking International Copyright in a Digitally Networked *World*," *Columbia-VLA Journal of Law and the Arts* 20 (1996): 571.

میزبان سرورهای ریشه‌ای (کشورهای بالادستی اینترنتی) به حمایت از حقوق بشر از طریق خود فضای سایبر دست بزنند. وجود مراکز بین‌المللی اینترنتی خصوصاً از آن جهت که بخشی از شکایات حقوق بشری متوجه دولت‌های بالادستی اینترنتی است، ضرورت خواهد داشت. این اقدام به تحقق مفهوم جدید «تضمین به حمایت از حقوق بشر از سوی ثالث» در فضای سایبر منجر خواهد شد.

فهرست منابع

الف) منابع فارسی

آیکاو، دیوید جِی، کارل‌ای سیگر، ویلیام‌آر وان استروج. *راهکارهای پیشگیری و مقابله با جرایم رایانه‌ای*. چاپ اول. ترجمه اکبر استرکی، محمدصادق روزبهانی و تورج ریحانی و راحله الیاسی. تهران: نشر دانشگاه علوم انتظامی، ۱۳۸۳.

استون، هیک. *حقوق بشر و اینترنت*. چاپ اول. ترجمه و تحقیق سید قاسم زمانی و مهناز بهراملو. تهران: نشر خرسندی، ۱۳۸۶.

بردبار، محمدحسین. *درآمدی بر حقوق ارتباط جمعی: مطبوعات، ماهواره و اینترنت*. تهران: نشر ققنوس، ۱۳۸۱.

حسن‌بیگی، ابراهیم. *حقوق و امنیت در فضای سایبر*. چاپ اول. تهران: نشر مؤسسه فرهنگی مطالعات و تحقیقات ابرار معاصر تهران، ۱۳۸۴.

خداقلی، زهرا. *جرایم کامپیوتری*. تهران: نشر آریان، ۱۳۸۳.

رمضانی قوام‌آبادی، محمدحسین. «حضور سازمان‌های غیردولتی در پیشگاه مراجع قضایی بین‌المللی». فصلنامه حقوق دوره ۳۸ شماره ۲ (۱۳۸۷): ۱۷۲-۱۵۳.

زمانی، سید قاسم، و مهناز بهراملو، مترجم. *حقوق بشر و اینترنت*. چاپ اول. تهران: نشر خرسندی، ۱۳۸۶.

زیبر، اولریش. *جرایم رایانه‌ای*. ترجمه محمدعلی نوری و دیگران. تهران: نشر گنج دانش، ۱۳۸۴.

ب) منابع انگلیسی

A) Books

Katz-Lacabe, Michael, and Margarita Lacabe. "Doing Human Rights Online: the Derechos Cyberbirth." In *Human Rights and the Internet*, edited by Steven Hick, Edward F. Halpin and Eric Hosakins. New York: Macmillan Press, 2000.

Lindblom, Ann-Karin. *Non-Governmental Organizations in International Law*. Cambridge: Cambridge University Press, 2005.

Scharfe, "Sharon. Human Rights and the Internet in Asia: Promoting the Case of East Timor." In *Human Rights and the Internet*, edited by Steven Hick, Edward F. Halpin and Eric Hosakins. New York: Macmillan Press, 2000.

Sharpe, Wayne. "Rebel Internet: Human Rights and the New Technology." In *Human Rights and the Internet*, edited by Steven Hick, Edward F. Halpin and Eric Hosakins. New York: Macmillan Press, 2000.

B) Articles

Alured Faunce, Thomas, Hitoshi Nasu. "Normative Foundations of Technology Transfer and Transnational Benefit Principles in the UNESCO Universal Declaration on Bioethics and Human *Rights*." *Journal of Medicine and Philosophy* (2009): 296-321. http://ssrn.com/abstract=1402388.

Center for Public Policy and Private Enterprise, School of Public Policy. "Gordon, Lawrence A., Martin P. Loeb and William Lucyshyn. Economic Aspects of Controlling

Capital Investments in Cyberspace Security for Critical Infrastructure Assets." Last accessed May 17, 2017. http://www.cppe.umd.edu/publications/economic-aspects-controlling-capital-investments-cyberspace-security-critical.

Council Framework Decision 2005/222/Jha.,

Cox, Noel. "The Regulation of Cyberspace and the Loss of National *Sovereignty*." *Information and Communications Technology Law* 11 (2002): 241-253.

Edward Geller, Paul. "Conflicts of Laws in Cyberspace: Rethinking International Copyright in a Digitally Networked *World*." *Columbia-VLA Journal of Law and the Arts* 20 (1996): 571-603.

Graham H., Todd. "Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric *Definition*." *Air Force Law Review* 64 (2009): 65-102. http://www.au.af.mil/au/awc/awcgate/law/af_law_review_cyber.pdf

http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!CELEXnumdoc&lg=en&numdoc=52002PC0173

Koritz, Nikola A. The Yahoo Case And Free Speech, Privacy And Corporate Responsibility In The People's Republic Of China, 9, http://works.bepress.com/nikola_koritz/1/

Lipton, Jacqueline D. "Who Owns 'Hillary.Com'? Political Speech and the First Amendment in *Cyberspace*, Political Speech in Cyberspace." *Boston College Law Review* 07-16 (2008): 55-123.

Mendes, Errol P. "Democracy, Human Rights and the New Information Technologies in the 21st Century-The Law and Justice of Proportionality and Consensual *Alliances*." *National Journal of Constitutional Law* 10 (1999).

Perritt, JR, Henry H. "Cyberspace Self-Government: Town Hall Democracy or Rediscovered *Royalism*?." *Berkeley Technology Law Journal* 12 (1999): 413-482.

Perritt. JR., Henry H. "Jurisdiction in *Cyberspace*." *Villanova Law Review* 41(1) (1996): 1-128.

Raymond Choo, Kim-Kwang. "Organized Crime Groups in Cyberspace: a Typology." *Trends in Organized Crime* 11(3) (2008): 270-295.

Security Focus. "Projecting Borders into Cyberspace." last modified April 28, 2009. http://www.securityfocus.com/columnists/500.

Shackelford, Scott J. "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law." *Berkeley Journal of International Law* 27 (2008): 192-251.

Swedish Defense University with Preliminary Conclusions on 'Cyberattack against Georgia'. August 2008.

The Organization for Economic Co-Operation and Development. "Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data". last Accessed May 17, 2017. http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

Tikk, Eneken, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Talihärm, Liis Vihul. "Cyber Attacks against Georgia: Legal Lessons *Identified*." *Cooperative Cyber Defence Center of Excellence, NATO Unclassified* Version 1.0 (2008): 14. http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf.

C) Documents

Barcelona Traction, I.C.J. Reports, 1970, p. 39, Para. 56-58.

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, January 28, 1981.

Convention on Cybercrime, Budapest, European Treaty Series - No. 185, 23.11.2001.

Convention on the Prevention and Punishment of the Crime of Genocide, December 9, 1948, 78 U.N.T.S.

Council of Europe. "Additional Protocol to the Convention on Cybercrime, Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed

through Computer Systems, 28.I.2003." last accessed May 17, 2017. http://conventions.coe.int/Treaty/EN/Treaties/html/189.htm.

Encyclopedia. "Sabotage." Last accessed May 17, 2017. http://www.encyclopedia.com/doc/1G2-3401803675.html.

Federal Bureau of Investigation Internet Crime Complaint Center (IC3). "Filing a Complaint with the IC3." Last accessed May 17, 2017. http://www.ic3.gov.

General Assembly Resolution, 1803 (XVII), 1996; 3281 (XXIX), 1974.

http://icsidfiles.worldbank.org/icsid/ICSIDBLOBS/OnlineAwards/c160/dc559_en.pdf.

https://www.ageofconsent.net/world.

Infoblog.us. "Infoblog.us." last accessed May 17, 2017. http://www.infoblog.us/2006/05/wired-publishes-att-nsa-documents.html.

International Law Commission, Commentaries on the Draft Articles on Responsibility of States for Internationally Wrongful Acts, 2001.

Kallahar's Place. "Is Yahoo Banning Allah?." Last accessed May 17, 2017. http://kallahar.com/stories/2005-Yahoo/yahoo.php.

Tech. "Iran criticizes Google for nomenclature of the Persian Gulf." last accessed May 17, 2017. http://tech.firstpost.com/news-analysis/iran-criticizes-google-for-nomenclature-of-the-persian-gulf-27928.html.

WIPO Arbitration and Mediation Center. "Julia Fiona Roberts v Russell Boyd Case No. D2000-0210 , May 29, 2000, WIPO Arbitration and Mediation Center." accessed November 6, 2007. http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0210.html.

Protection of Human Rights Law in Cyberspace

Dr. Seyed Yaser Ziaee
Ph. D. in International Law, Assistant Professor of International Law, Qom University,
Email: yaserziaee@gmail.com

Internet has two contrary aspects: as a mean for promoting human rights and as a mean for violation of human rights. Violations of human rights law in cyberspace have special kinds and it is necessary to find appropriate mechanisms for protection of human rights.
There are some theories for attribution of human rights violations to a State like authority power, nature of act, hot pursuit, et. It's possible some individual and human freedoms be breached in cyberspace like freedom of speech, freedom of access to information, freedom of assembly, right to self-determination, right property, right to privacy, et. There are some mechanisms for protection of human rights in cyberspace like cyber international organizations and cybercrime complaint submission websites, these are called cyber self-government. Also it is possible for Root Server State to guarantee human rights in other States as a third party for protection of human rights.

Keywords: Cyberspace, Protection of Human Rights Law, Ensure to Protection of Human Rights Law, Attribution of Wrongful Acts to States, Human Rights, International Law.

ISSN 1682-9220

Journal of LEGAL RESEARCH

VOL. XVI, No. 1 2017-1

- **Derogation of Human Rights in Situation of Public Emergency**
  Dr. Seyed Ghasem Zamani - Marzieh Esfandiary
- **Poverty Reduction: A Programme for Social Development in International Law**
  Dr. Reza Eslami - Mahshid Ajeli Lahiji
- **Protection of Human Rights Law in Cyberspace**
  Dr. Seyed Yaser Ziaee
- **Analysis of Iranian Legislation in Petroleum Investment**
  Dr. Hamid Bagherzadeh - Dr. Raheleh Seyed Morteza Hosseiny
- **Third Executive Protest in Execution of Civil Judgements Law**
  Dr. Rasol Parvin - Amin Pahkideh - Elahe Etemadi
- **Regular Assignment of Judicial Cases from the Perspective of Judicial Independence: A Comparative Study in Iranian Law and International Documents**
  Omid Rostami Ghazani
- **The Role of Claimant and Prosecutor in Offences against Historical and Cultural Heritage**
  Dr. kyoumars kalantari - Hassan khodabakhshi palandi - Amir Erfanifar
- **Legal Protection of Historical and Cultural Monuments against Environmental Pollution**
  Amin Valizadeh - Saber Nojomi
- **Ramsar Convention on Wetlands from the Perspective of International Environmental Law**
  Mehrdad Mohammadi - Vahideh Najafi
- **Vicious Cycle of Enacting Local Duties in City Councils and Revocation in Court of Administrative Justice Judges Council: Discussion of Judicial Supervision on Urban Development in Contradiction with the Right to Property of People (2009-2016)**
  Dr. Vahid Agah - Mohammad Nabi Boorboori
- **The Class Action Code: A Model for Civil Law Countries**
  Author: Professor Antonio Gidi - Persian Translator: Dr. Majid Pourostad

S. D. I. L.
The S.D. Institute of Law
Research & Study