Journal iranian political sociology
Vol. 5, No.10, dey 2022

https://dx.doi.org/10.30510/psi.2022.298253.2083

Virtual Citizen Rights on the Dark Web

abstract
In the sociology of law, attention is paid to informal and intangible sources of law and it is emphasized that the mere legal theory can not express the role of legal facts in regulating social relations. From a sociological point of view, we examine the presence of virtual citizens. In fact, when you search for information through common browsers such as Google, you only have access to 4% of the information available in cyberspace, so 96% of the information is hidden from everyone and hidden in the web. Iran's filter law is illegal for users to access the environment, because the identity of users, which we refer to as IP address, is not known due to the use of filter breaker and Tor software, and therefore this environment has become a place for crime and crimes. The dangers of this environment to users and identifying its legal dimensions are the means by which a step can be taken to formulate more laws regarding the dark web and prevent people from getting caught in this environment. According to research In this study, we came to the conclusion that due to the global nature of dark web crimes and rising crime and crime statistics in this environment, it is necessary to take more international measures and cooperation to prevent many crimes and crimes that occur in thisenvironment.
key words: Dark Web, Sociology, Virtual Citizen, Law

ماهنامه علمی (مقاله علمی_پژوهشی) جامعه شناسی سیاسی ایران،
سال پنجم،شماره ده، دی۱۴۰۱،صص۲۹۷۹-۲۹۹۱
https://dx.doi.org/10.30510/psi.2022.298253.2083

حقوق شهروند مجازی دروب تاریک

نفیسه نکویی مهر[۱]

مسعود راعی[۲]

فرامرزعطریان[۳]

تاریخ دریافت : ۱۴۰۱/۰۵/۰۱

تاریخ پذیرش: ۱۴۰۱/۰۷/۰۵

چکیده:

همانطورکه می دانید زمانی که شما ازطریق مرورگرهای رایجی مثل گوگل به جستجوی اطلاعاتی می پردازیم تنها به ۴٪اطلاعات موجوددرفضای مجازی دسترسی دارید بنابراین ۹۶٪دیگراطلاعات ازدیدهمگان پنهان است ودرمحیط وب تاریک نهفته است.طبق قانون فیلترایران دسترسی کاربران به محیط غیرقانونی است زیراهویت کاربران که ازآن به عنوان آدرس IPیادمی کنیم به دلیل استفاده ازفیلترشکن ونرم افزارTorمشخص نیست وبه همین دلیل این محیط،تبدیل به مکانی جهت جرم وجنایات شده است.روش تحقیق توصیفی تحلیلی است وهدف ازاین پژوهش توصیف ومعر فی خطرات این محیط به کاربران وشناسایی حقوق شهروندان مجازی در آن است تابدین وسیله بتوان گامی درراستای حمایت ازحقوق شهروندان مجازی در وب تاریک برداشت واز،دردام افتادن افراددراین محیط جلوگیری کرد.باتوجه به تحقیقات صورت گرفته دراین پژوهش به این نتیجه رسیدیم که به دلیل جهانی بودن جرایم وب تاریک وبالارفتن آمارجرم وجنایات دراین محیط لازم است اقدامات وهمکاری های بین المللی بیشتری صورت بگیردتابتوان ازجرم وجنایات زیادی که دراین محیط رخ می دهدجلوگیری وازحقوق شهروندان مجازی حمایت کرد.

کلیدواژگان: وب تاریک,ابعادحقوقی,جرم وجنایات,هویت,نرم افزارTor

---

گروه حقوق،واحدنجف آباد،دانشگاه آزاداسلامی،نجف آباد،ایران.[۱]
دانشجوی دکتری، گروه حقوق،واحدنجف آباد،دانشگاه آزاداسلامی،نجف آباد،ایران.[۲]

گروه حقوق،واحدنجف آباد،دانشگاه آزاداسلامی،نجف آباد،ایران.[۳]

مقدمه

"دارک وب" اصطلاحی است که به مجموعه وب سایت هایی اطلاق می شود که برای همه قابل رویت می باشند، اما آدرس های IPسرورهایی که آن ها را اجرا می کنند، پنهان هستند بنابراین هر کاربر وبی می تواند این وب سایت ها را مشاهده کند .اما فهمیدن این موضوع که چه کسی پشت این سایت ها قرار دارد، کار بسیار دشواری است و شما به کمک موتورهای جستجو نمی توانید این سایت ها را جستجو و پیدا کنید. تقریباً تمامی سایت های موجود در دارک وب با استفاده از ابزار رمزگذاری Tor هویت خود را پنهان می کنند. این ابزار برای پنهان کردن هویت و جعل آدرس سایت مورد استفاده قرار می گیرد. وقتی وبسایتی از طریق Tor اجرا می شود، هویتش پنهان می شود.در حقیقت؛ Tor پنهان ماندن یک وب سایت را چندین برابر می کند. برای مشاهده دارک وبی که از رمزگذاری Tor استفاده کرده؛ کاربر می بایست از Tor استفاده کند. درست مانند IP کاربر نهایی که از میان چندین لایه رمزگذاری شده جهش داده می شود تا در قالب آدرس IP دیگری در شبکه Tor ظاهر شود، وضعیت وبسایت هم به همین گونه است. بنابراین برای دیدن یک وب سایت در اینترنت باز، لایه های متعدد بزرگتر و پنهان تری در مقایسه با عمل پنهان استفاده از Tor، وجود دارند. درکنارخطراتی که دراین محیط وجوددارد،دارک وب کاربردهای قانونی نیز دارد، برای مثال افرادی که در جوامع توتالیته کار می کنند می توانند از آن برای برقراری ارتباط با جهان خارج استفاده نمایندویااینکه فعالان حقوق بشردررژیم های سرکوب گربرای پنهان نگاه داشتن هویت خودمی توانندراین محیط به فعالیت های خودبپردازند. تور اولین نسخه خود را در ۲۰ سپتامبر ۲۰۰۲ عرضه کرد. این نرم‌افزار از سیستم مسیریابی پیازی استفاده می‌کرد، که توسط آزمایشگاه تحقیقاتی نیروی دریایی آمریکا ایجاد شده‌بود. وظیفهٔ اصلی آن ایجاد شبکه‌ای امن برای مکالمات دولتی بود .پس از ایجاد تور، این پروژه توسط خبرنگاران، مخالفین حکومت‌ها، سازمان‌های اطلاعاتی و پلیس مورد استفاده قرار می‌گیرد. پشتیبان‌های این نرم‌افزار نیروی دریایی آمریکا در سال‌های اولیه و سپس ای‌اف‌اف و بنگاه سخن‌پراکنی ایالات متحده در سال‌های کنونی بودند. در عین حال این پروژه از محل کمک‌های افراد نیز درآمد دارد.در سال ۲۰۱۰ این پروژه توسط بنیاد نرم‌افزارهای آزاد به عنوان پروژه آزاد نمونه انتخاب شد دلیل آن کمکی بود که این نرم‌افزار به گروه‌های آزادی‌خواه در کشورهایی مانند ایران و مصر که با سانسور اینترنت دست و پنجه نرم می‌کنند، کرد.به طورکلی جرایمی که دراین محیط رخ می دهدبه دلیل ویژگی جهانی بودن نیازمندتدوین قوانین بین المللی وهمکاری های بین المللی دولت هاست.که دراین مقاله علاوه برآگاه سازی کاربران ازخطرات این محیط به دنبال بیان روش های موثرجلوگیری ازجرم وجنایات وتدوین قوانین جامع در عرصه داخلی وبین المللی هستیم.مبحثی که دراین خصوص مطرح این است که باتوجه بحث حریم شخصی درقوانین بااین محیط چگونه برخوردشودکه منافاتی به حفظ حریم شخصی اشخاص درفضای مجازی نداشته باشد؟باتوجه به بحث دسترسی آزاداشخاص به اطلاعات موجود در اینترنت چه تدابیری اتخاذ شود که علاوه برجلوگیری نفوذافرادبه این محیط ،حق دسترسی آزادبه اطلاعات نقض نشود؟باتوجه به حق حریم خصوصی ودسترسی آزادبه اطلاعات آیاصرفاورودبه این محیط جرم است؟

مرورپیشینه ها:

درخصوص موضوع ابعادحقوقی وب تاریک درعرصه مجلات داخلی میتوان گفت به لحاظ جدیدبودن موضوع تحقیقی درقالب علمی وپژوهشی صورت نگرفته است ولی درعرصه بین المللی،ازمهم ترین مقالات ، میتوان به مواردذیل اشاره کرد:

1-A public policy perspective of the Dark Web(**08 Sep 2016, Accepted 20 Feb 2017, Published online: 13 Mar 2017**):Mishael Chertoff

دراین مقاله آقای میشل چرتف ضمن توصیفی ازمحیط وب تاریک به بررسی نقش دولت هابرای جلوگیری ازجرایم دراین محیط پرداخته است وایشان معتقداست چون بسیاری ازدولت ها مثل آمریکاوفیلیپین ، منابع سرشاری ازاین محیط کسب کرده اند همکاری زیادی درخصوص کاهش جرم وجنایات ازخودنشان نمی دهند.ودرخصوص روش های شناسایی مجرمان دراین محیط مثل دستگیری مدیر سایت جاده ابریشم که درزمینه فروش موادمخدرفعالیت داشت اطلاعاتی رامنتشرنمی کنند.

۲-Vitaris, B. 2015. "Russian Government Sues Firm for Failing to Deanonymize Tor Users." Accessed August 30, 2016.

دراین مقاله آقای ویتاریس ازروسیه به تحلیل نرم افزارTorپرداخته ودراین خصوص بیان داشته که این نرم افزاربه دلیل برخورداری ازلایه های امنیتی بالا باعث پنهان نگه داشتن هویت کاربران در فضای مجازی می شود.

۳- Sui, D., J. Caverlee, and D. Rudesill. 2015. "The Deep Web and the Darknet." Accessed August 30, 2016.

دراین مقاله آقایان رودیسل وکاورلی به توصیف مزایا ومعایب فضای وب تاریک پرداختند وآنها معتقدبودند وب تاریک باوب عمیق متفاوت است ووب تاریک بخشی ازوب عمیق است.آنهااینترنت رابه کوهی یخی تشبیه کردندواعتقادداشته اند که قسمت ازکوه یخی که برروی سطح آب ها قراردارد surface web یعنی همان محیطی که بامرورگرهای رایج قابل مشاهده است نام داردوقسمتی که دراعماق آبها واقع شده همان وب عمیق وبخش نهایی وب تاریک نام دارد.

۱-مفهوم وب تاریک ونرم افزارTOR

دارک وب یا[۲] وب تاریک به شبکه‌ای گفته می‌شود که در دسترس عموم نبوده و بیشتر برای مقاصد غیرقانونی مورد استفاده قرار می‌گیرد. ردیابی فعالیت‌های آن و شناسایی افراد در آن دشوار یا غیرممکن است. در این شبکه اطلاعات جامعی نهفته شده که افراد ناشناس آن‌ها را مدیریت می‌کنند، فروشندگان مواد مخدر، هکرها، تروریست‌ها و افراد سودجو غالباً این دسته از افراد را تشکیل می‌دهند. دارک وب بخش کوچکی از وب پنهان است(Clemmitt,2016:245).

دارک وب سایت‌هایی است که برای عموم قابل مشاهده است اما توسط آی‌پی‌های مخفی سرور اجرا می‌شوند. در این شبکه تمامی اطلاعات به صورت آنلاین و با پسوردهایی محافظت شده‌اند. برای دسترسی به اطلاعات آن باید از چندین پِی‌وال‌ها گذشته و از نرم‌افزارهای به خصوص استفاده کرد. هر کاربری می‌تواند به سادگی از این وب‌سایت‌ها بواسطه سرویس هایی همچون هیدن ویکی دیدن کند. بسیاری از این وب‌سایت‌ها از موتورهای جستجو بهره نمی‌گیرند، از این‌رو جستجو در جستجوگرها برای پیدا کردن آنها تقریباً با شکست مواجه می‌شود(Sui,2015:51). اغلب این وب‌سایت‌ها که آنها را برای مخفی سازی هویتشان از ابزار رمزگذاری تور بهره می‌گیرند و پسوند onion.را دارند. همچنین بیشتر اطلاعات دارک وب در پایگاه داده‌هایی نظیر LexisNexis ذخیره می‌شود(Vitaris,2016:11). بسیاری از نرم افزارها و فیلم هایی که در محیط معمولی وب یافتن و دریافت آن به سختی صورت می پذیرد در دارک وب به سادگی قابل مشاهده و دریافت می باشد. نرم افزارهای کرک شده، فیلم ها و بازی ها با قیمت بسیار کمتر در این وب سایت ها به فروش می رد. حتی **بازی نهنگ آبی** که اخیرا بسیار مورد توجه عموم قرار گرفته از دارک وب به سادگی قابل دریافت می باشد(Swearingen,2014:23).

در حقیقت اگر فضای وب را بخواهیم دسته بندی نماییم، می توان آن را به یک فضای دیپ وب و وب معمولی تقسیم نمود. فضای دیپ وب مجموعه ای از فضایی است که شامل پنل های مدیریت و نویسندگی وبسایت ها می شود. در این فضا فقط کاربرانی توانایی حضور دارند که به نوعی با وبسایت مورد نظر ارتباط داشته باشند(Stevens,2016:16). اما اگر بخواهیم دارک وب را تعریف کنیم، باید بگوییم که این فضا زیر مجموعه ای از دیپ وب می باشد و فقط افرادی قادر به ارتباط با آن هستند که از پل ارتباطی مخصوص آن نظیر **تور بروزر (Tor Browser)** استفاده نمایند.در واقع دارک وب یک محیط اینترنتی امن برای خلافکاران می باشد که از طریق آن می توانند به گسترش شبکه های غیرقانونی خود پرداخته و به نوعی به پول بیشتر دست یابند .**فروشگاه های دارک وب** دقیقا همانند فروشگاه های معمول در وب می باشند و به همان شیوه اداره می شوند، منتها در این فروشگاه ها معمولا مواد مخدر و یا اسلحه های غیر قانونی فروخته می شود(Jardine,2015:87).

شاید با خود بیندیشید که چرا دولت ها نمی توانند از گسترش چنین شبکه هایی جلوگیری نمایند؟ در پاسخ به این سوال باید بگوییم که چون این شبکه ها در محیطی کاملا ایزوله ایجاد می گردند و هیچ نشانه و اثری از گردانندگان آن ها وجود ندارد، برای دولت ها بسیار مشکل است که گردانندگان اصلی این شبکه های غیر قانونی را بیابند. این محیط برای افرادی که با آن آشنایی چندانی ندارند و صرفا از روی کنجکاوی اقدام به گشت و گذار در آن می نمایند، می تواند بسیار خطرناک باشد .همانطور که اشاره شد، این محیط پر است از انسان های قانون شکن و هکرهای پر قدرت که به سادگی می توانند اقدام به بدست آوردن موقعیت و اطلاعات افرادی که با آن ها ارتباط برقرار می کنند ، نمایند. به همین سبب پیشنهاد می گردد که در آن زیاد کاوش

[۲] Dark Web

نکنید. فیلم ها و تصاویر بسیاری از شکنجه افراد، قتل، تجاوز و غیره در این محیط دیده می شود. بدیهی است که اگر گردانندگان این وب سایت ها حس کنند شما قصد خرابکاری و یا کاوش در کار آن ها را دارید، از خود واکنش نشان داده و تهدیداتی را علیه شما انجام دهند(Cox,2016:12).

با این حساب اگر بخواهیم یک تعریف کلی و جامع از محیط دارک وب و دیپ وب داشته باشیم باید بگوییم دیپ وب یک محیط گسترده در بستر اینترنت است که شامل پنل های مدیریتی وب سایت ها و پایگاه های داده آن می باشد که کاربران غیر مجاز دسترسی به آن نداشته و دارک وب که زیر مجموعه ای از دیپ وب می باشد، محیطی است که در آن می توان انواع خلافکاری ها و امور غیر قانونی را دنبال کرد و فقط افرادی که از ابزار خاص ورود به آن استفاده نمایند، قادر به دسترسی به آن می باشند(Ward,2014:10).

یکی از معروفترین وبسایت‌هایDark Web ، وبسایت Silk Road[۴] بود. این سایت، بازاری بزرگ از مواد مخدر بود که امکان خرید این مواد بوسیله‌ی بیت کوین[۵]برای مصرف‌کنندگان را فراهم می‌کرد. پس از خرید و پرداخت هزینه با بیت کوین هم محموله بوسیله‌ی پست به خریدار فرستاده می‌شد(Satterfield,2016:25).

---

[۴] - سیلک رود به انگلیسی (Silk Road) :یک بازار الکترونیکی و تحت وب بود که گردانندگانش آن را با استفاده از فناوری سامانه نرم‌افزاری پنهان تور اجرا می‌کردند. بیشتر کالاهایی که در سیلک‌رود برای فروش گذاشته می‌شد در حوزه قضایی بیشتر کشورها قاچاق محسوب می‌شد.رادیوی عمومی ملی از این وب‌گاه به عنوان» آمازون.کامِ داروهای غیرمجاز» یاد کرد .اکونومیست نیز آن را در مقاله‌ای درباره بیت‌کوین به عنوان «نوعی ئی‌بِی برای مواد مخدر در گوشه‌ای تاریک و پنهان از وب به نام تور «معرفی کرد .فروش سالانه سیلک رود نزدیک به ۲۲ میلیون دلار تخمین زده شده بود .در ۲ اکتبر ۲۰۱۳ این وبسایت توسط اف‌بی‌آی ضبط شد .اف بی آی ۲۶،۰۰۰ بیت کوین را مصادره کرد که هر یک $۱۴۰ ارزش داشتند که مبلغی بالغ بر ۳،۶ میلیون دلار می شد. یک سخنگوی اف بی آی گفت که بیت‌کوین ها را تا پایان رویه قضایی ضبط و سپس نقد خواهد شد .در اکتبر ۲۰۱۳ اف‌بی‌آی حدود ۱۴۴ هزار بیت‌کوین را بر مبلغ روز حدود ۲۸،۵ میلیون دلار مصادره کرد که متعلق به راس اولبریچ بود.خدمات مارشال‌های ایالات متحده آمریکا در ژوئن ۲۰۱۴ حدود ۳۰ هزار بیت‌کوین را در حدود ۱۸ میلیون دلار فروختند .۱۴۴ هزار بیت‌کوین دیگر که ارزشی حدود ۸۷ میلیون دلار در سال ۲۰۱۴ داشت(حدود ۴۰۰ میلیون دلار در سال ۲۰۱۷) روی لپ‌تاپ راس اولبریچ یافت شد که به تدریج فروخته شد.

[۵] - بیت‌کوین به انگلیسی (Bitcoin):یک نوآوری اینترنتی با کارکردهای مشابه» پول بی‌پشتوانه «یا پول حکومتی است. نوآوری بودن بیتکوین به این معناست که خالقان آن توانسته‌اند آنرا در مدت کوتاهی از یک ایده به یک واقعیت اثرگذار بر دنیای اقتصاد و مراکز سیاست پژوهی مبدل کنند. زیرا در چندسال گذشته ارزش بیتکوین در بازارهای جهانی از چند صدم دلار به چندهزار دلار افزایش یافته‌است[۱] اما پول بودن یک جایگاه حقوقی است و پول بودن بیتکوین منوط به پذیرش جایگاه حقوقی آن از سوی دولت‌ها است. تا کنون هیچ دولتی بیتکوین را به عنوان پول به رسمیت نشناخته‌است و دولت‌های ایالات متحده آمریکا، آلمان و چین بر کالا بودن بیتکوین تأکید دارند].[۲] البته از لحاظ فنی و کارکردی این عبارت صحیح است که بیت کوین نوعی پول دیجیتال بر پایه شبکه همتا به همتا، امضای دیجیتال و اثبات دانایی صفر است و به کاربران امکان می‌دهد که بدون هیچ واسطه‌ای، انتقال پول غیرقابل بازگشت انجام دهند .گره‌های شبکه هر معامله را در شبکه اعلام می‌کنند که پس از تأیید در یک سیستم اثبات کار، در یک تاریخچه عمومی به نام زنجیره بلوکی ذخیره می‌شود .

بیت کوین امکان پرداخت‌های بسیار کم هزینه را فراهم می‌کند. شبکه بیت کوین سیستم کنترل کننده متمرکز ندارد و توسط هیچ سازمان، مؤسسه یا نهاد دولتی اداره نمی‌شود. زمان متوسط تأیید هر انتقال بیت‌کوین، تقریباً ده دقیقه است .انتقال پول از یک نقطه به نقطه دیگر در تمام شبکه اطلاع‌رسانی شده و تمام نقاط از آن آگاه خواهند شد .

۲-بررسی ابعاد حقوقی ورود به وب تاریک

پیش ازبررسی وضعیت حقوقی درخصوص ورود به وب تاریک نیاز است که ابتدا بامبحث IP Address(هویت کاربران)درفضای مجازی آشناشوید.همانطورکه هویت کاربران درفضای زمین به واسطه کدملی وکدشناسنامه که آدرسی منحصربه فرداست مشخص می شود هویت کاربران درفضای مجازی توسط Ip Address مشخص می شود.

۲-۱-ارتباط شرکت های ارائه دهنده خدمات اینترنتی با هویت کاربران

آی اس پی (ISP) برگرفته از کلمه «Internet Servise Provider» شرکت خدمات سرویس های اینترنت است. مراکز ارائه دهنده خدمات اینترنت(ISP) ، خدمات متعددی نظیر پست الکترونیکی و دستیابی به اینترنت را در اختیار متقاضیان قرار می دهند. بیشتر این مراکز خدمات اینترنتی، شامل شرکتی است که امکان دستیابی به اینترنت و دیگر سرویس های وب را فراهم می کند. مراکز ارائه دهنده خدمات اینترنت علاوه بر نگهداری و پشتیبانی از یک خط مستقیم به اینترنت، فعالیت های متعدد دیگری نظیر نگهداری و پشتیبانی از سرویس دهندگان وب را نیز انجام می دهند.

برای شناخت این مراکز باید بگویم شما اکنون با خط تلفن به صورت دایل آپ DialUPیا ای دی اس ال، خطوط پر سرعت Adslبه اینترنت متصل شده اید؛ شرکتی که کارت اینترنتی آن را خریداری کرده اید و اکنون به شماره های شبکه آن متصل شده اید یا از خدمات اینترنت پر سرعت آن بهره می برید، در اصل آی اس پی یا مرکز ارائه سرویس های اینترنتی است. فروش پهنای باند و سرویس های اتصال کاربر به اینترنت یکی از خدمات این شرکت هاست. باتوجه به وظایف وخدماتی که برای شر کت های اراده دهنده خدمات اینترنتی بیان کردیم به این نتیجه رسیدیم که:

۱-مسئولیت رعایت قوانین مالکیت معنوی و حق تالیف و تصنیف به عهده ارائه کننده اطلاعات در شبکه می باشد.
۲-امکان و اعمال برقراری پالایه (filter) توسط این شرکت ها وجوددارد‌وضوابط ومصادیق موارد پالایش (filter) توسط شورای عالی اطلاع رسانی تصویب و اعلام می شود.
۳-هر ISP موظف است اطلاعات کلی کاربران وIP های مربوط را ثبت و یک نسخه از آن نیز به وزارت پست و تلگراف و تلفن اعلام نماید.طبق آئین نامه شرکت های ISPاقطعا یکی از پایه های اصلی برای حفظ امنیت کاربران در فضای مجازی، حفظ حریم خصوصی آنها است و قانون جرایم رایانه ای مصوب ۵/۳/۱۳۸۸ مجلس شورای اسلامی، در ۲۰/۳/۱۳۸۸ توسط شورای نگهبان تایید شده و رسمیت یافته است و رعایت آن برای همه ضروری است و تخلف از آن قابل پیگرد قانونی است.
بنابراین مطابق مواد ۲۱ الی ۲۳ قانون جرایم رایانه ای، شرکت ها تنها مکلف به پاسخگویی به ۲ مرجع هستند :کارگروه تعیین مصادیق مجرمانه و مقام قضایی رسیدگی کننده به پرونده.(قید "رسیدگی کننده به پرونده" در مواد مذکور نیز بیانگر آن است که حتما باید قبلا در اثر شکایت، پرونده ای تشکیل شده باشد و تنها مقام قضایی رسیدگی کننده به "همان پرونده" صلاحیت درخواست لازم را دارا خواهد بود)بنابراین پس ازبدست آوردن IPمجرم توسط پلیس تخصصی جرایم سایبری وتشکیل پرونده، مقام قضایی به شرکت های ISPدستورمی دهد باتوجه به آدرس اطلاعات شخصی مجرم راتحویل دهد.

۲-۲- حقوق فیلترینگ

فیلترینگ اینترنت در ایران عبارت است از اعمال سانسور، محدودیت و نظارت ساختاریافته و هدفدار بر دسترسی به محتوای وب‌گاه‌ها و استفاده از خدمات اینترنتی برای کاربران ایرانی. فیلترینگ در ایران بر اساس قوانین مصوب در مجلس شورای اسلامی اعمال می‌گردد و طیف گسترده‌ای از وب‌گاه‌های اینترنتی، از پورنوگرافی گرفته تا سیاسی را در بر می‌گیرد. گرچه مسدود کردن دسترسی به وب‌گاه‌های اینترنتی در ایران جنبه قانونی دارد، اما روند آن، به ویژه برای وب‌گاه‌های سیاسی و اجتماعی، به درستی مشخص نیست و سیاست‌های آن غیرشفاف است.

در خرداد ۱۳۸۰ , سیدعلی خامنه‌ای« ابلاغیه سیاست‌های کلی شبکه‌های اطلاع‌رسانی رایانه‌ای»را صادر کرد. با ابلاغ سیاست‌های کلی شبکه‌های اطلاع‌رسانی رایانه‌ای به محمد خاتمی (رئیس جمهور وقت ایران)، علی‌رغم مخالفت مخابرات و دولت او با قانون‌گذاری پیرامون اینترنت در خارج از مجلس، شورای عالی انقلاب فرهنگی به تصویب قوانین مربوط به اینترنت از جمله فیلترینگ پرداخت. که در مجموعه مصوباتی با عنوان «مقررات و ضوابط شبکه‌های اطلاع‌رسانی و رایانه‌ای» به مسئله فیلترینگ و نظارت بر شرکت‌های تأمین خدمات اینترنتی پرداخته شد. در سال ۸۱ فیلترینگ به صورت جدی مورد توجه قرار گرفت. کمیته‌ای سه نفره شامل: نماینده وزارت اطلاعات، نماینده وزارت فرهنگ و ارشاد اسلامی و نماینده صدا و سیما برای رسیدگی به وضعیت اینترنت تشکیل شد. نماینده دبیرخانه شورای اسلامی و نماینده سازمان تبلیغات اسلامی به عنوان دو عضو دیگر، بعداً به این کمیته پیوستند. این کمیته برای شروع لیست ۱۱۱ هزار سایت ممنوعه را به شرکت‌های تأمین خدمات اینترنتی داد .فیلترینگ با هدف جلوگیری از دسترسی کاربران به وب‌گاه‌های مغایر با قوانین و سیاست‌های جمهوری اسلامی ایران از سوی شرکت مخابرات ایران صورت می‌گیرد؛ تا سال ۸۸ در صورت وارد کردن نشانی یک وب‌گاه فیلتر شده، پیغامی نزدیک به این عنوان ظاهر می‌شد: «مشترک گرامی! دسترسی به این سایت امکان‌پذیر نمی‌باشد». از ابتدای سال ۱۳۸۹ به جای پیغام قبلی صفحه‌ای جایگزین شد که ضمن اعلام فیلتر شدن نشانی مذکور به کاربران توصیه می‌کرد به وب‌گاه‌های دیگری که در آن صفحه معرفی شده‌اند مراجعه کنند .

نهادهای دخیل در فیلترینگ ایران گسترده و ساختاری پیچیده دارند، از جمله نهادهای مهم می‌توان به شورای عالی فضای مجازی، کارگروه تعیین مصادیق محتوای مجرمانه، ارتش سایبری جمهوری اسلامی ایران و پلیس فتا اشاره کرد. در این میان رهبر ایران دارای نقشی مهم در تعیین افراد اصلی تأثیرگذار بر نهادهای فیلترینگ دارد .شورای عالی فضای مجازی بالاترین نهادی است که مسئولیت تعیین سیاست‌های کلی فضای مجازی را در برابر جنگ نرم با کشورهای غربی بر عهده دارد و مستقیماً به دست رهبر جمهوری اسلامی در سال ۲۰۱۲ میلادی تشکیل شده. شورای عالی فضای مجازی تعیین‌کننده محتواهایی از وب است که غیرقانونی تشخیص می‌دهد. این شورا فهرست وب‌گاه‌هایی که باید مسدود شوند را بر پایه ملاک‌هایی چون خلاف هنجارهای جامعه بودن، خلاف شئون اسلامی بودن، تهدیدبودن برای امنیت ملی، و تبلیغ روش‌های دورزدن فیلترینگ تعیین می‌کند .این شورا و کارگروه تعیین مصادیق رابطه نزدیکی دارند و دارای اعضای مشترک نیز هستند. دفتر دادستان کل بر کمیته‌های فیلترینگ نظارت دارد و فهرست فیلترینگ را به شرکت مخابرات ایران و شرکت خدمات ارتباطات داده‌ها و نهادهای مرتبط دیگر ابلاغ

می‌کند. شرکت مخابرات ایران بخشی از فهرست را مستقیماً از راه کنترل شبکه عمومی داده‌ها اعمال می‌کند و مسئولیت بخشی دیگر را به رساننده‌های خدمات اینترنتی می‌سپارد که همگی مجبورند پهنای باند خود را از طریق شرکت مخابرات خریداری کنند.

از سوی دیگر رسانندگان اینترنتی همگی زیر نظر سازمان تنظیم مقررات و ارتباطات رادیویی هستند که از نظر قانونی آن‌ها را موظف می‌کند سیاست‌های تعیین‌شده توسط کارگروه تعیین مصادیق محتوای مجرمانه را اجرا کنند.

مسدود کردن وب‌گاه‌های اینترنتی در ایران با تصمیم کمیته‌ای تحت نظارت شورای عالی انقلاب فرهنگی با حضور نمایندگان صداوسیما، مخابرات و وزارت اطلاعات صورت می‌گیرد و شرکت خدمات ارتباطات داده‌ها مجری تصمیم‌گیری این کمیته‌است . برخی سایت‌ها اینترنتی نیز مستقلاً با دستور قوه قضائیه فیلتر یا دفاتر آنان پلمپ گردید .

باتوجه به مطالبی که توضیح داده شده درحال حاضراتصال به فضای وب تاریک فیلتراست حال سوالی که دراینجا مطرح است این است که آیا استفاده ازفیلترشکن جرم محسوب می شود؟درپاسخ به این سوال بایدگفت بنا بر نظر مقامات قانونی ذیربط، برخی سایت‌های موجود در اینترنت به دلیل عدم رعایت قوانین ، فیلتر و یا پالایش می‌شوند و در این میان برخی کاربران فضای مجازی ، فیلترشکن‌های مختلفی را مورد استفاده قرار داده و به سایت مورد نظر دسترسی پیدا می‌کنند.
اما لازم است بدانید که طبق ماده ۱ قانون جرایم رایانه ای هرکس به طور غیرمجاز به داده‌ها یا سیستم‌های رایانه ای یا مخابراتی که به وسیله تدابیر امنیتی حفاظت شده است، دسترسی یابد، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج تا بیست میلیون ریال ، یا به هر دو مجازات محکوم خواهد شد.همچنین بر اساس ماده ۲۷ قانون جرایم رایانه ای ، در صورت تکرار جرم برای بیش از دو بار ، دادگاه می‌تواند مرتکب را از خدمات الکترونیکی عمومی از قبیل اشتراک اینترنت، اشتراک تلفن همراه، اخذ نام دامنه مرتبه بالای کشوری و بانکداری الکترونیکی برای مدت یک ماه تا پنج سال محروم کند که مدت این محرومیت، بستگی به شدت و درجه جرم ارتکابی دارد.بنابراین صرفاورودبه فضای وب تاریک جرم محسوب می شود.

۳-اقدامات دولت ها درخصوص مبارزه باجرایم وب تاریک

۳-۱-دولت آمریکا

۱-۱-۳- آژانس پروژه‌های پیشرفته دفاعی که از سازمان‌های تابعه وزارت دفاع آمریکاست، در حال کار بر روی یک پروژه مطالعاتی موسوم به Memexاست تا یک موتور جستجوی جدید طراحی کند که الگوها و روابط میان داده های دیجیتال آنلاین را بدست آورده و به منظور تشخیص فعالیت های غیر مجاز و غیر قانونی، به نیروهای مختلف امنیتی کمک کند. در واقع هدف نهایی پروژه‌ی Memexتشکیل دادن یک نقشه‌ی جامع از محتواهای موجود بر روی اینترنت است.

۲-۱-۳- آژانس امنیت ملی آمریکا(NSA)، برنامه (XKeyscore)در دستور کار خود دارد (این برنامه توسط ادوارد اسنودن فاش شده است). بر مبنای این برنامه، هر کاربری که نرم افزار خاص ورود به وب تاریک را از اینترنت دانلود کرده است، به طور خودکار، مورد پیگرد قرار خواهد گرفت و تمامی فعالیت‌های او ثبت خواهد شد.

۳-۱-۳- سرویس‌های اطلاعاتی و امنیتی آمریکا نیز این موضوع را در رأس فعالیت‌های خودقرار داده‌اند. موسسه مطالعات پیشرفته جاسوسی در آمریکا نیز برنامه‌ای با عنوان "حملات سایبری، روش‌های پیش‌بینی، تشخیص، مقابله و دفاع در برابر آن" را توسعه داده است(**Greenberg,2014:23**).

۲-۳-دولت آلمان

دانشگاه آلمانی پورت اسموث با بکارگیری ۴۰ کامپیوتر و نرم افزارهای خزنده این تحقیقات را به پیش برده است که به آنها اجازه بررسی و دسترسی به سایت های بیشماری را در شبکه تور فراهم کرده است. بر اساس این تحقیقات که بوسیله ۴۰ بازدید (۴۰ کامپیوتر) انجام شده نشان می دهد که تمام این کامپیوترها بوسیله نرم افزارهای مخربی که هکرها در بستر سرورهای توری بساط کرده اند آلوده شده اند. در واقع این سرویس و سایت های توری با داشتن ارتباطات بات نت بستر حمله هماهنگ به کاربران این شبکه را فراهم می آورند. با این حال چیزی که در نهایت از این تحقیقات عائد تیم اوون شد این بود که ۸۳ درصد بازدیدها از سایتهای توری، مرتبط با دسته بندی کودک آزاری جنسی بوده است

(**Finklea,2015:31**).

۳-۳-دولت ایران

باتاسیس پلیس تخصصی فتا برای بررسی جرایم سایبری(این پلیس درحال حاضربا روش هایی همچون روش صفرویک به رصددرفضای سایبرمی پردازد وازوقوع جرم پیشگیری میکند.وهمچنین باابزارها ونرم افزارهای تخصصی مجرمان رادرمحیط سایبرشناسایی میکنند).وبه نقل ازسردارهادیان فر:پایس فتا ایران قادربه کشف ۶۵ درصد جرایم سایبری است.

-ایران قانون جرایم رایانه ای را درخصوص جرایم سایبری تاسیس نموده است.

باعضویت درکنوانسیون جرایم سایبری که درسال ۲۰۰۱درمجارستان به تصویب شورای اروپارسیده است همکاری بین المللی خودرابرای دستگیری ومجازات مجرمان افزایش داده است.

-وجودشعب رسیدگی به جرایم رایانه ای دردادسراهای مرکزاستان ها

-عضویت پلیس تخصصی فتا ایران در IGCI [۶](مرکز پیشرفته تحقیق و توسعه برای شناسایی جنایات و جنایتکاران)واقع در سنگاپور

-همکاری با UNODC[۷]واقع دروین (دفترمبارزه با مواد مخدر غیرقانونی و جرایم بین المللی سازمان ملل متحد).

نتیجه گیری

باتوجه به مطالعات صورت گرفته دراین پژوهش به این نتییجه رسیدیم که دوچالش اساسی درخصوص این محیط وجوددارد:نخستین چالش استفاده ازنرم افزارتورودومین چالش جهانی بودن این جرم است.دولت هاباییددرخصوص مبارزه با مجرمان این محیط سعی کنندموثرترین روش راانتخاب کنند،درواقع بایدبه جستجوی سایت های غیر قانونی به جای کاربران غیر بپردازندهمانطورکه میدانید با توجه به صلاحیت قانونی مناسب، هکرهای دولتی می توانند ابزارهای decanonymisingرا بر روی رایانه های کاربرانی که به سایت دسترسی دارند، قرار دهند.وتمام اقدامات این کاربران رارصدکنند و اگر دولت صرفا سایت را قطع کند، دیگری به جای آن پاپ آپ می شود .از سوی دیگر، اگر دولت هاقوانینی درخصوص عضویت درسایت های غیرقانونی وضع کنند بسیارمناسب ترازجلوگیری ازورودبه این محیط است .باتوجه به حق دسترسی آزادبه اطلاعات واینکه این محیط علاوه برمضرات،مزایایی نیزداردوهمچنین قوانین حقوق بشر، صرف ورودبه این محیط نمی تواند جرم محسوب شود.باتوجه به جهانی بودن جرایم این محیط نیازاست همکاری های بین المللی وقوانین بین المللی دراین خصوص صورت گیرد.وتدابیری اتخاذ شود که سطح های امنیتی نرم افزارتورراشناسایی کنند تابتوانند هویت کاربران تورارمشخص کنند وهمچنین قانون IPراتدوین کنند تاهویت همه کاربران متصل به اینترنت قابل تشخیص باشد.

۶- INTERPOL Global Complex for Innovation

۷- united nations office on drugs and crime

منابع

- Clemmitt, M. 2016. “The Dark Web.” Accessed August 30, 2016. http://library.cqpress.com/cqresearcher/document.php?id=cqresrre2016011500.

- Cox, J. 2016. “The FBI’s ‘Unprecedented’ Hacking Campaign Targeted Over a Thousand Computers.” Accessed August 30, 2016. https://motherboard.vice.com/read/the-fbis-unprecedented-hacking-campaign-targeted-over-a-thousand-computers.

- Darknet Markets Are Not beyond the Reach of Law. 2016. Accessed August 30, 2016. https://darkwebnews.com/darknet-markets/darknet-not-beyond-law/.

- Finklea, K. 2015. “Dark Web.” Accessed August 30, 2016. https://www.fas.org/sgp/crs/misc/R44101.pdf.

- Going Dark: The Internet behind the Internet. 2014. Accessed August 30, 2016. http://www.npr.org/sections/alltechconsidered/2014/05/25/315821415/going-dark-the-internet-behind-the-internet.[Google Scholar]

- Greenberg, A. 2014. “Hacker Lexicon: What is the Dark Web.” Accessed August 30, 2016. https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/.[Google Scholar]

- Jardine, Eric. 2015. “The Dark Web Dilemma: Tor, Anonymity and Online Policing.” Accessed December 14, 2016. https://www.cigionline.org/sites/default/files/no.21.pdf.[Google Scholar]

- King, Gary, Jennifer Pan, and Margaret E. Roberts. 2013. “How Censorship in China Allows Government Criticism but Silences Collective Expression.” Accessed December 13, 2016. http://gking.harvard.edu/files/gking/files/censored.pdf.[Google Scholar]

- Owen, Gareth and Nick Savage. 2015. “The Tor Dark Net.” Accessed December 13, 2016. https://www.ourinternet.org/sites/default/files/publications/no20_0.pdf.[Google Scholar]

- Satterfield, J. 2016. “FBI Tactic in National Child Porn Sting under Attack.” Accessed September 6, 2016. http://www.usatoday.com/story/news/nation-now/2016/09/05/fbi-tactic-child-porn-sting-under-attack/89892954/.[Google Scholar]

- Stevens, G. n.d. “The Truth about the Deep Web.” Accessed August 30, 2016. http://kernelmag.dailydot.com/features/report/7477/the-truth-about-the-deep-web/.[Google Scholar]

- Sui, D., J. Caverlee, and D. Rudesill. 2015. “The Deep Web and the Darknet.” Accessed August 30, 2016. https://www.wilsoncenter.org/publication/the-deep-web-and-the-darknet.

[Google Scholar]

- Swearingen, J. 2014. “A Year after Death of Silk Road, Darknet Markets are Booming.” Accessed August 30, 2016. https://finance.yahoo.com/news/death-silk-road-darknet-markets-۱۴۲۵۰۰۷۰۲.□□□□.[□□□□□□ □□□□□□□].

- Tor: Sponsors. n.d. Accessed August 30, 2016. https://www.torproject.org/about/sponsors.html.en.[Google Scholar]

- Vitaris, B. 2015. “Russian Government Sues Firm for Failing to Deanonymize Tor Users.” Accessed August 30, 2016. https://www.deepdotweb.com/2015/11/30/russian-government-sues-firm-failing-deanonymize-tor-users/.[Google Scholar]

- Vitaris, B. 2016. “Russian [Sic] is Collecting Encryption Keys as ‘Anti-terrorism’ Legislation Goes into Effect.” Accessed August 30, 2016. https://www.deepdotweb.com/2016/08/03/russian-collecting-encryption-keys-anti-terrorism-legislation-goes-effect/.[Google Scholar]

- Ward, M. 2014. “Tor’s Most Visited Hidden Sites Host Child Abuse Images.” Accessed August 30, 2016. http://www.bbc.com/news/technology-30637010.[Google Scholar]

- Yellin, T., D. Aratari, and J. Pagliery. n.d. What is Bitcoin? Accessed August 30, 2016. http://money.cnn.com/infographic/technology/what-is-bitcoin/.[Google Scholar]