

A Study of the Place of Deep Web and Dark Web Cyberplaces under the International Law

Alireza Ansari Mahyari

Assistant Professor Department of Law, Najafabad Branch, Islamic Azad
University, Najafabad, Iran (Corresponding Author)

Alimahyari63@gmail.com

Zahra Sadat Hosseini

Department of International Law, Najafabad Branch, Islamic Azad
University, Najafabad, Iran

Zahra.hosseini00@yahoo.com

Ahmad Radman

Department of International Law, Najafabad Branch, Islamic Azad
University, Najafabad, Iran

Ahmadradman1994@gmail.com

Keywords:

Internet,
International Law,
Cybercrimes,
Dark Web, Deep
Web

Abstract

In addition to the clear dimensions available to everyone, the internet and cyberspace also has dark dimensions that constitute a platform for committing cybercrimes. In a general division, the cyberspace is divided into the surface web space and the deep web space, where the dark web space is a part of the deep web space, which can be accessed only by using special software tools. The main discussion of this article covers investigation of web surfaces and their position from the perspective of international law with a view to cybercrimes. Unfortunately, not only the dark web and deep web, but also all the topics of the cyber field and crimes in this field are neglected from the point of view of international law, and there are limited international treaties and documents covering the same which totally do not meet the needs of the international community in the cyber field today. Buying and selling weapons, drugs, slaves, and human body parts are of the main businesses in the dark web, which are done using digital currencies. Today, due to the rapid development of communication technologies and the lack of specific international laws in the field of cyberspace, it is necessary for the International Law Commission to present and develop a plan to regulate and approve laws and treaties in the field of the Internet and create a platform for the cooperation of all governments in this field.

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/>



بررسی جایگاه فضای دیپ وب و دارک وب در حقوق بین الملل

علیرضا انصاری مهیاری

استادیار گروه حقوق، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران (نویسنده مسئول)

alimahyari63@gmail.com

زهرا سادات حسینی

گروه حقوق بین الملل، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران

Zahra.hosseini00@yahoo.com

احمد رادمان

گروه حقوق بین الملل، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران

Ahmadradman1994@gmail.com

تاریخ پذیرش: ۳۱ تیر ۱۴۰۳

تاریخ دریافت: ۲۳ خرداد ۱۴۰۲

چکیده

فضای اینترنت مضاف بر ابعاد روشن و در دسترس برای همگان، دارای ابعادی تاریک نیز بوده که بستری برای انجام جرایم سایبری می‌باشند. فضای اینترنت در یک تقسیم‌بندی کلی به فضای وب‌سطح و دیپ‌وب تقسیم می‌شود که فضای دارک‌وب بخشی از فضای دیپ‌وب بوده که دسترسی به آن تنها با استفاده از ابزارهای نرم‌افزاری مخصوص میسر می‌باشد. موضوع اصلی این مقاله بررسی سطوح وب و جایگاه آنها از منظر حقوق بین‌الملل با نگاهی به جرایم سایبری می‌باشد. متأسفانه نه تنها فضای دارک‌وب و دیپ‌وب، بلکه تمام مباحث حوزه سایبر و جرایم این حوزه از دید حقوق بین‌الملل مغفول مانده و معاهدات و اسناد بین‌المللی محدودی وجود دارد که این موارد نیز پاسخگوی نیازهای امروز جامعه بین‌المللی در حوزه سایبر نیستند. خرید و فروش اسلحه، مواد مخدر، برده و اعضای بدن انسان از تجارتهای اصلی در فضای دارک‌وب بوده که با استفاده از ارزهای دیجیتال انجام می‌شوند. امروزه با توجه به پیشرفت سریع تکنولوژی‌های ارتباطی و عدم وجود قوانین بین‌المللی تخصصی در حوزه فضای سایبری، لازم است تا کمیسیون حقوق بین‌الملل اقدام به ارائه و تدوین طرحی برای تنظیم و تصویب قوانین و معاهداتی در زمینه فضای اینترنت و ایجاد بستری برای همکاری تمامی دولت‌ها در این زمینه نماید.

واژگان کلیدی: اینترنت، حقوق بین‌الملل، جرایم سایبری، دارک‌وب، دیپ‌وب.

خصیصه اصلی فضای سایبری این است که با وجود تمامی فواید و آسان‌سازی دسترسی به اطلاعات و انجام امور، بستری امن برای افراد مجرم باشد (ضیایی و شکیب نژاد، ۱۳۹۶: ۲۲۷). پیشرفت سریع و روزانه تکنولوژی‌های ارتباطی، علیرغم وجود مزایای فراوان، دارای معایبی نیز می‌باشند؛ با نگاهی به وب‌سایت‌های مختلف می‌توان به این نتیجه رسید که صنعت وب روزانه در حال رشد بوده و این موضوع، فرصتی طلایی برای مجرمینی است که در حال فعالیت در فضای اینترنت می‌باشند. وب به صورت کلی به سطوح وب‌سطح و دیپ‌وب تقسیم بندی می‌شود که اکثر افراد در کارهای روزمره خود از وب‌سطح استفاده می‌کنند و برای دسترسی داشتن به فضای دیپ‌وب و دارک‌وب بایستی از روش‌های مخصوصی استفاده نمود که افراد عادی قادر به انجام این کار نمی‌باشند. با توجه به تحولات گسترده در حوزه تکنولوژی و فناوری ارتباطی و اطلاعاتی در چند سال اخیر، با توجه به کارکردهای خوب و مثبت این حوزه، گاهی دیده می‌شود که برخی از اشخاص سودجو با فراگیری مهارت‌های حوزه سایبر درصدد سوءاستفاده کردن از اشخاص کاربر در این فضا و ایجاد مشکلاتی برای آنها می‌باشند. فضای سایبری، فرصتهایی جدید و پیشرفته‌ای را برای قانون‌شکنی در اختیار اشخاص قرار می‌دهد و توانی بالقوه برای ارتکاب جرایم را به روش‌های غیرمرسوم و جدید دارد تا افراد مجرم این حوزه قادر باشند تا در فضای گسترده صفرویک هر فکر و اندیشه‌ای را که در ذهن دارند، عملی کنند که این موضوع به وضوح در فضای دیپ‌وب قابل مشاهده است.

در ارتباط با بحث دیپ‌وب، نرم‌افزار تور از مهمترین ابزارهای نرم‌افزاری در زمینه استفاده از این فضا می‌باشد؛ این نرم‌افزار یک سیستم مرورگر با ارتقای حفظ حریم خصوصی بوده که برای محافظت نمودن از کاربرهای اینترنتی در برابر حملات تجزیه و تحلیل‌های ترافیکی که از جانب یک غول غیرقانونی جهانی در حوزه وب به وجود آمده، به کار می‌رود (باقرپور، ۱۴۰۰: ۲۴). افرادی از این نرم‌افزار استفاده می‌کنند، اکثراً از کشورهای اروپایی، جمهوری خلق چین و ایالات متحده آمریکا هستند (Jardine, 2015: 17).

فضای دارک‌وب بر خلاف باور عموم، گسترده نبوده و یک مجموعه از سایت‌هایی بوده که به صورت عمومی قابل مشاهده نیستند و آدرس (آی.پی) سرورهای اجراکننده آنها با ترفندهای برنامه‌نویسی، پنهان و غیرقابل ردیابی شده‌اند (Sui & Caverlee & Rudesill, 2019: 32).

در بحث حقوق بین‌الملل، با توجه به پیشرفت روزانه تکنولوژی و گسترش فناوری‌های ارتباطی و گسترش دامنه و حوزه ارتکاب جرایم اینترنتی در قلمروهای داخلی کشورها نسبت به حوزه بین‌الملل، متأسفانه منبع و قوانین بین‌المللی بروز و قابل استنادی وجود ندارد (Kratchman & Smith & Smith, 2018: 74). در حوزه حقوق بین‌الملل، در موارد مشابه با مبحث فضای مجازی می‌توان به بحث مبحث حق بر فراموشی و پرونده گوگل اسپانیا و سند اخلاق و حفاظت از داده‌ها مصوب سال ۲۰۱۸ میلادی اتحادیه اروپا و دستور العمل تالین اشاره نمود (محقق هرچقان؛ اردبیلی؛ بیگ زاده؛ مهدوی ثابت، ۱۴۰۱: ۲۷۰).

امروزه جنگ بین ابرقدرتها، از نیروگاه‌های اتمی و سلاح‌های کشتار جمعی و جنگ‌افزارهای نظامی، به کامپیوترها و فضای سایبری منتقل شده است، اکثر کشورهای قدرتمند در حوزه‌های نظامی، در حوزه سایبر و ساخت تکنولوژی‌های مرتبط با این حوزه پیشگام هستند (Bradbury, 2019: 42). با توجه به این موارد، حقوق بین‌الملل و سازمان‌های بین‌المللی در ارتباط با این موضوعات چه رویه‌ای را اتخاذ نموده‌اند؟ در حوزه جرایم سایبری بین‌المللی می‌توان به هک کردن سیستم‌های دولتی یک کشور توسط یک گروه هکری یا یک دولت دیگر در خارج از خاک کشور اول اشاره نمود که این موضوع به کرات در حوزه فضای سایبر قابل مشاهده است. در این زمینه، کشور خسارت‌دیده چه راهکاری و چه مرجعی برای طرح شکایت دارد؟ در این زمینه، کشورها برای تلافی و جبران، اقدام متقابل را اتخاذ می‌نمایند که این موضوع را می‌توان نقض‌کننده حقوق بین‌الملل و نقض صلح بین‌المللی عنوان نمود که لازم است در این زمینه برای رفع نواقص و خلأهای موجود اقدام‌هایی اساسی صورت پذیرد.

۱. بررسی فضای سایبری و جرایم این حوزه

فضای سایبر در علم لغت به معنای فضایی مجازی و غیرواقعی بوده و فعالیت‌های سایبری یا کامپیوتری به زبان بسیار ساده به معنی یک مجموعه از ارتباط‌های میان افراد از طریق رایانه و دستگاه‌های مخابراتی، بدون در نظر داشتن مختصات جغرافیای فرد می‌باشد (صفدری و بابایی

پور، ۱۴۰۱: ۰۳). در تعریفی دیگر، فضای مجازی شبکه جهانی تشکیل شده از زیرساخت‌های فنی و رایانه ای و مخابراتی بوده که در سطح جهانی به هم پیوسته اند (السان، ۱۴۰۱: ۱۷). در زمینه جرایم سایبری می‌توان به دستورالعمل تالین نیز اشاره داشت و می‌توان گفت یک سند مهم در زمینه مبارزه با جرایم سایبری بوده که کمتر مورد توجه واقع شده است. در سال ۲۰۰۹م، مجموعه دستورالعمل تالین، به عنوان یک سند علمی و غیرالزام‌آور در راستای قانونمند ساختن عملیات‌های سایبری، توسط یک گروه متخصص بین‌المللی تهیه و تدوین شده و به دعوت مرکز عالی دفاع سایبری ناتو در شهر تالین استونی تشکیل گردیده؛ گروه اصلی، متشکل از ۲۳ نفر فرد متخصص بوده و کار آنان توسط یک گروه ۱۳ نفره متخصص دیگر بررسی گردید. این امر منتج به منتشر شدن نخستین دستورالعمل تالین گردید، که بر قوانین جنگ متمرکز بود. در دومین دستورالعمل تالین برخلاف سند اول، نه تنها عملیات سایبری با آستانه بالا را پوشش داده شده، بلکه شامل آن گروه از اقدام‌های سایبری که اثر و مقیاس بیشتری داشته و امکان دارد که منتج به نقض توسل به زور شود، یا اقدام‌های سایبری که همراه با یک مخاصمه مسلحانه ایجاد می‌شد و همچنین اقدام‌های با آستانه پایین، مانند عملیات سایبری که امکان داشت موازین حقوق بین‌الملل، مانند اصل بر حاکمیت و عدم مداخله را نقض نمایند، نیز شده است (Allhusen& Alsmadi& Wahbeh& Al-Ramahi& Al-Omari, 2021: 03)

۱.۱. بررسی جرایم سایبری

مجرمین حوزه سایبر از تفاوت‌های موجود در ظرفیت‌های پیشگیری، کشف، تحقیق و تعقیب جرایم این حوزه سوءاستفاده نموده و به سرعت در حال تبدیل شدن به یک دغدغه جهانی می‌باشند (گیوکی و حکاک زاده، ۱۴۰۱: ۱۹). این خصلت فراملی به مجرمان سایبری، چه به صورت فردی یا به عنوان گروه‌های جنایت‌های سازمان‌یافته امکان فرار از اقدامات پیشگیرانه و قانونی را می‌دهد، حتی اگر این اقدامات توسط تواناترین اشخاص، طراحی و اجرا شود (Baiden, 2017: 15).

جرایم سایبری به موازات فرصت‌هایی که از طریق افزایش سریع استفاده از اینترنت برای تجارت الکترونیک و در کشورهای درحال توسعه ایجاد می‌شود، تکامل یافته‌اند. دلیل اصلی رشد جرایم سایبری از اواسط دهه ۲۰۰۰ به گسترش «بات‌نت‌ها» به عنوان ابزارهای انبوه برای سوءاستفاده از رایانه و تقویت این فعالیت‌ها از طریق (کیت‌های ابزار)، (مانند ژئوس) نسبت داده شده است. در این زمینه، سرویس‌هایی مخفی با ضریب امنیتی بالا، ارائه‌دهنده داده‌های سرقت شده هستند و به افراد اجازه می‌دهد تا داده‌های سرقت شده، مانند جزئیات کارت اعتباری را با پرداخت هزینه‌ای مشخص، دانلود کنند. به صورت خلاصه، جرم سایبری به سرعت از یک جرم کوچک که توسط یک مجرم متخصص به صورت انفرادی انجام می‌شود، به جرمی بزرگ و گسترده (سازمان یافته و صنعتی) تبدیل شده است. در حالی که بسیاری از انواع جرایم سایبری به درجه بالایی از سازماندهی و تخصص نیاز دارند، شواهد و مدارک کافی برای تعیین اینکه آیا جرایم سایبری اکنون تحت سلطه گروه‌های جرایم سازمان‌یافته است یا خیر و این گروه‌ها دارای چه ساختاری هستند، در دسترس نیست (Kranhold, 2014: 34)

۲. بررسی فضای دیپ‌وب و دارک‌وب

تفاوت‌های ماهیتی موجود در حوزه فضای سایبری با دنیای حقیقی، نیازمند تغییر در مفهوم‌ها و ارکان بعضی بحث‌ها و اصطلاح‌های حقوقی در این فضا می‌باشد. از جمله این مباحث، بحث جرایم و مجازات‌ها می‌باشد که در زمینه بستر وقوع جرایم می‌توان به فضای دیپ‌وب و مشتقات آن اشاره نمود (بی نا، ۱۳۹۷: ۲۱). اینترنت دارای دو بلوک ساختاری است: «وب‌سطح» و «دیپ‌وب». اکثر افراد از وجود وب‌سایت‌هایی مانند آمازون، ویکی‌پدیا، فیسبوک، یوتیوب و... آگاهی دارند؛ این سایت‌ها در وب‌سطح قرار داشته و توسط موتورهای جستجو مانند گوگل، بینگ، یا هو و... ایندکس شده و در نتایج نشان داده می‌شوند. وب‌سطح به عنوان (وب قابل مشاهده) شناخته می‌شود، اما باید عنوان نمود که وب‌سطح بخشی فشرده از فضای اینترنت بوده که تنها ۴٪ از این فضا را تشکیل داده که تنها برای عموم قابلیت دسترسی دارد (Balhara& Ubba& Sharma& Chawla. 2020: 15)

وب‌سطح حجم اطلاعاتی بسیار زیادی را به صورت قانونی در دسترس افراد قرار می‌دهد. به غیر از وب‌سطح، وب‌سایت‌هایی مخفی وجود داشته که تشکیل‌دهنده ۹۶ درصد از فضای اینترنت بوده و در دسترس عموم مردم نمی‌باشند که در فضای دیپ‌وب قابل مشاهده هستند. از آنجایی که عمل اعتبارسنجی برای دسترسی به داده‌هایی مانند حساب‌های بانکی یک عمل اجباری قانونی بوده، وب‌سایت‌های موجود در فضای دیپ‌وب، تنها شرط محرمانه بودن اطلاعات را برای کاربران فراهم می‌کنند؛ اگر وب‌سایت‌های موجود در دیپ وب ایندکس (فهرست) گردند، هر فردی

قادر است تا با جستجوی یک نام (اعم از نام فرد یا یک سازمان و...) به داده‌ها دسترسی پیدا نموده و اطلاعات شخصی و محرمانه موجود در این فضا برای دیگران نمایش داده شود (Hari Tewari, 2019: 50).

۱۰۲. دیپوب

برداشتی اشتباه در بین عموم افراد وجود دارد که دیپوب و دارکوب فضای یکسان بوده و نامهایی همانند هستند، اما این دو فضا دارای تفاوت‌های بسیاری هستند؛ دیپوب، فضای سایبری ایندکس نشده است و برای تضمین امنیت اطلاعات کاربران، توسط موتورهای جستجوی رایج قابلیت فهرست شدن ندارد، در حالی که دارکوب، بخشی کوچک از فضای دیپوب بوده و همانند دیپوب فهرست نشده و دسترسی به آن به مراتب از دیپوب سخت‌تر می‌باشد (Schäfer& Fuchs& Strohmeier& Engel& Liechti& Lenders, 2019: 14).

دسترسی به فضای دارکوب تنها با استفاده از مرورگری مخصوص امکان پذیر می‌باشد. در فضای دیپوب، در هنگام نمایش تمام سایت‌های موجود که ایندکس نگردیده اند، به افراد اعلام می‌شود که موتورهای جستجوگر، اطلاعات این سایت‌ها را بعد از جستجو کردن به افراد باز نمی‌گردانند (Yang& Liu& Kizza& Mark & Ege, 2017: 63).

فضای دیپوب همچنین شامل بخشی خاص از فضای وب اصلی قانونی شده، همانند وبسایت‌هایی از جمله آمازون، آی. ایم. دی. بی، نتفلیکس می‌باشد، به این دلیل که این وبسایت‌ها به صورت سفارشی برای کاربران طراحی شده و نیازی به فهرست کردن هر آدرس مجازی سایت نیست (Gercke& Vrochidis & Helen 2021: 65). برخی از سایت‌ها، همانند فیس‌بوک، اینستاگرام نیز به عنوان دیپوب عمیق طبقه بندی می‌شوند، به این علت که با استفاده از رابط برنامه کاربردی می‌توان به این سایت‌ها دسترسی پیدا نمود. دیپوب حاوی تمام داده‌هایی است که با کمک موتورهای جستجوی رایج قابل یافتن نمی‌باشند (Park,2020:14).

داده‌های ذخیره‌شده در فضای دیپوب برای موتورهای جستجوی عمومی، مانند گوگل قابل مشاهده نبوده و نمایه‌سازی وبسایت‌ها به دلیل ناهماهنگی داده‌ها و مسائل اسمی پیچیده می‌شود. این وبسایت‌های ناشناس برای دسترسی به داده‌ها نیازمند اعتبار ورود هستند. این وبسایت‌ها دارای زمان بندی بوده و بعد از بازه زمانی مشخص از دسترس خارج می‌شوند (Xiaolei,2015: 45).



تصویر ۱-۱- بخش بندی فضای اینترنت بر اساس درصد مشاهده کاربران:

الف) وب سطح ۴٪: سایت‌های عمومی و موتورهای جستجوگر مانند گوگل، یاهو، بینگ؛ سایت‌های خبرگزاری مانند سی. ان. ان، یورو نیوز؛ شبکه‌های اجتماعی مانند اینستاگرام، فیس‌بوک، واتساپ، توئیتر و...

و فضای دارکوب که شامل فضای برای انجام اعمالی مانند خریدوفروش داروی قاچاق، اعتراضات سیاسی، فروش اسلحه و ادوات نظامی، مهمات، مواد منفجره ممنوعه، پورنوگرافی کودکان، برده‌فروشی، قاچاق اعضای بدن انسان و...

۲-۲-۲- دارکوب

دارکوب محتوای پنهان موجود وب جهانی بوده، تشکیل دهنده بخشی از دیپوب بوده و از فضای اینترنت استفاده می‌کند، اما برای دسترسی داشتن به این فضا، نیاز به یک مرورگر مخصوص، مجوز و وجود تنظیمات رایانه‌ای خاصی می‌باشد. در فضای دیپوب، محرمانه‌بودن اطلاعات و هویت افراد حاضر در این فضا، از اولویت‌های مهم بوده و این موارد توسط موتورهای جستجوی وب برای عموم نشان داده نمی‌شوند (East, 2017: 41).

فضای دارکوب تنها با استفاده از نرم‌افزارهای ناشناس مخصوص نصب شده در مرورگرهایی مانند تور، سابگراف، واترفاکس، آی. تو، پی (پروژه اینترنت نامرئی) و... قابل دسترسی می‌باشند. فضای دارکوب، یک اینترنت رمزگذاری شده بوده و به سرگرمی‌های بزرگ و وحشتناک اجازه می‌دهد تا به صورت مخفیانه ایجاد و شروع به فعالیت نموده و فعالیت خود را در همین فضا ادامه دهند. این فضا، فضای واقعی برای خریداران و فعالان حوزه تجارت‌های غیرقانونی می‌باشد، در همین راستا، مرورگر تور، راهی ساده برای دسترسی به فضای دارکوب بوده و ممکن است برای فعالیت‌های قانونی و همچنین غیرقانونی استفاده شود؛ از جمله استفاده‌های قانونی می‌توان به آزادی‌بیان برای خبرنگاران و اطلاع‌دهندگان، تبادل اطلاعات در سطح جهانی با حفظ حریم خصوصی و استفاده‌های غیرقانونی مانند معامله با مواد مخدر، جزئیات کارت اعتباری سرقت‌شده و شرط‌بندی و فروش برده، پورنوگرافی کودکان، فروش اسلحه و مهمات جنگی و... اشاره نمود (Dalins & Wilson & Marc, 2018: 33).

فضای دارکوب، مجموعه‌ای از خدمات پنهان شده از دید موتورهای جستجو و کاربران عادی بوده و توسط مجرمان سایبری برای ارائه انواع خدمات و کالاهای غیرقانونی استفاده می‌شود. فعالیت‌های مجرمانه سایبری در فضای دارکوب را می‌توان یکی از مشکلات حیاتی جوامع در سراسر جهان عنوان نمود؛ تکنیک‌های وب‌کاوی، همانند تجزیه و تحلیل محتوا و تجزیه و تحلیل ساختار می‌تواند برای شناسایی و اجتناب از تهدیدات تروریستی در سراسر جهان، امری مفید باشد (Alnabulsi, Islam, ۲۰۱۸: ۴۵).

امروزه از تحلیل شبکه‌های اجتماعی برای بررسی انواع پدیده‌ها و فرآیندهای اقتصادی و سازمانی استفاده می‌شود. تجزیه و تحلیل شبکه‌های اجتماعی به صورت موثر برای مقابله با پولشویی، سرقت‌هویت، کلاهبرداری آنلاین، حملات سایبری و به‌ویژه، روش‌های ارائه‌شده در این شبکه‌ها در بررسی بسیاری از عملیات غیرقانونی با اوراق بهادار و سرمایه‌گذاری‌های افراد در این زمینه‌ها، برای جلوگیری از شورش و غیره مورد استفاده واقع می‌شوند (Biddle & England & Peinado & Willman, 2017: 19).

۲-۲-۱- شیوه کار دارکوب

وبسایت‌های دارکوب بر روی مرورگر تور، با دامنه (دات آنیون) نمایش داده می‌شوند. تمرکز مرورگر تور بر روی ارائه دسترسی محدود به دارکوب با حفظ اطلاعات می‌باشد. هر وبسایت یا آدرس وب نشان‌دهنده یک نقطه شروع در دارکوب است. این نقطه شروع، اتصال را برای رسیدن به سروری که وبسایت واقعاً در آن ذخیره شده، تنظیم می‌نماید. این گره‌ها، ورودی یا دسترسی به شبکه را فراهم نموده و به صورتی پیوند داده شده‌اند تا از هویت فردی که از وبسایت در فضای دارکوب استفاده می‌کند، محافظت نماید. به علت وجود سیستم رمزگذاری چندلایه، هویتها و مکانها پنهان شده و قابل ردیابی نیستند. داده‌های ارسال شده را می‌توان توسط گره بعدی موجود در شبکه که به مقصد منتهی می‌شود، رمزگشایی نمود. این روش، روشی ایمن بوده و محرمانه‌بودن اطلاعات افراد و هویت آنها را حفظ می‌کند. این سیستم پیچیده، بازسازی مسیر گره‌ها و رمزگشایی لایه به لایه اطلاعات را غیرممکن نموده و از آنجایی که ناشناس‌بودن در فضای دارکوب بسیار اهمیت دارد، وبسایت‌ها نمی‌توانند آی.پی و موقعیت مکانی کاربر را ردیابی نموده و کاربران نیز به علت محافظت از داده‌ها در این فضا، اطلاعاتی در مورد گردانندگان وبسایت‌ها و موقعیت مکانی آنها به دست آورند (Woodley, 2015: 14).

برقراری ارتباطات میان کاربران دارکوب به صورت بسیار محرمانه و با استفاده از ابزارهای رمزگذاری انجام می‌شود و به کاربران این اجازه را می‌دهد تا به صورت محرمانه و بدون افشای هویت خود، وبلاگ‌نویسی نموده، با همدیگر صحبت کنند و فایل‌های مدنظر خود را به اشتراک بگذارند. تمام اتصالات در فضای دیپوب کدگذاری شده و ایمن بوده و دسترسی به شبکه‌ها را نمی‌توان مسدود کرد که این امر، اتصالات و

رمزگذاری شبکه را در فضای دارکوب به صورت ناشناس نشان می‌دهد و این ناشناس بودن به میزان بسیار زیاد سبب می‌شود تا دارکوب، بستری امن برای گشت‌وگذار کاربران اینترنتی و مجرمان شود (Liggett & Lee & Roddy & Wallin, 2020: 95).

۲,۲,۲. خصوصیات دارکوب

داده‌های ارسال شده توسط برنامه‌های کاربردی مبتنی بر وب در بخش وب‌سطح، در برابر نقض‌های امنیتی و سایر حملات بسیار آسیب‌پذیر هستند. از سویی دیگر، دارکوب ویژگی‌های قابل توجهی، مانند حفظ حریم خصوصی کاربران در هنگام دسترسی یا استفاده از اینترنت، حفظ ناشناس بودن و ارائه محرمانه بودن، تبادل اطلاعات با سانسور اینترنتی، خرید کالاها محدود، آزادی بیان و غیره را ارائه می‌دهد. برخی از مزایای دارکوب عبارتند از:

- ناشناس بودن کاربران: محرمانه بودن هویت کاربران را برای آنها فراهم نموده و گشت‌وگذار در وبسایت‌های دارکوب به همین دلیل در یک بستر امن صورت می‌گیرد، گشت‌وگذار در دارکوب، امکان دسترسی به سایت‌هایی را فراهم می‌کند که ایندکس نشده‌اند و پس از جستجو، هیچگونه تاریخچه‌ای در مرورگر به جا نمی‌گذارند؛ این ناشناس بودن سطح امنیتی بالایی را در فضای دارکوب فراهم می‌کند، زیرا هویت و مکان کاربران پنهان بوده و به دلیل سیستم رمزگذاری چند لایه، قابل ردیابی نمی‌باشد؛

- خرید کالای محدود: خرید برخی از کالاها در دارکوب قابل توجه است؛ به عنوان مثال، برخی از داروها، مانند قرص‌های خواب و قرص‌های مسکن که در اروپا قانونی هستند، ممکن است در بسیاری از کشورهای آسیایی و خاورمیانه غیرقانونی باشند؛

- وجود آزادی بیان بدون هیچ محدودیتی: این موضوع نتیجه مستقیم، ناشناس ماندن و عدم افشای هویت افراد در فضای دارکوب می‌باشد؛ دارکوب این امتیاز را برای ابراز آزادانه نظر در مورد هر موضوعی، بدون هیچ ترسی فراهم نموده و افراد می‌توانند نظراتشان را در مورد هر موضوعی بدون تردید و ترس از تهدیدات جانی و امنیتی بیان کنند (Griffith & Xu & Ratti, 2017: 29).

۳,۲,۲. مرورگر تور، مسیر دسترسی به دیپ‌وب و دارکوب

دارکوب شامل وبسایت‌هایی است که در قسمت پنهان یا سایت‌های فهرست نشده اینترنت وجود دارند؛ این فضا در شبکه ای خاص وجود دارد که در وب‌سطح قابل مشاهده نیست. کاربران تنها با استفاده از مرورگر تور که نقطه اصلی در دسترسی به فضای دیپ‌وب است، قادر به مشاهده و دسترسی فضای دارکوب هستند. مرورگر تور عمدتاً برای بسیاری از اهداف خاص توسعه یافته است؛ این مرورگر نخستین بار توسط آزمایشگاه تحقیقات دریایی ایالات متحده آمریکا در قرن بیست و یکم توسعه یافت و هدف از توسعه آن، فراهم کردن طبقه‌بندی و محرمانه ماندن اطلاعات نیروهای مسلح ایالات متحده آمریکا که درگیر عملیات‌های نظامی در خارج از خاک آمریکا بودند، می‌باشد (Biswas & Fidalgo & Evanovich, 2017: 63).

مرورگر تور بر اساس مدل تکنیک (مسیریابی پیازی) عمل می‌کند که در آن اطلاعات کاربر ابتدا رمزگذاری شده و سپس از طریق رله‌های مختلفی که در شبکه تور وجود دارد، منتقل می‌شود. مسیریابی با استفاده از مرورگر تور (مسیریابی پیازی یا لایه لایه) برای تأمین امنیت کاربر و پنهان کردن هویت کاربر استفاده می‌شود. با یک پرش از نقطه اتصالات از رایانه کاربر به نقطه هدف از طریق زنجیره رله‌ای واسطه عمل می‌کند (Yadava & Bhushanb & Saxena, 2020: 15). این موارد در سرتاسر جهان قابل مشاهده و کاملاً توسط داوطلبانی اجرا می‌شوند که به همین دلیل آماده‌اند تا برخی از ظرفیت‌های انتقال داده را کنار بگذارند. هنگامی که نگرانی اصلی در دسترسی به فضای دارکوب، ناشناس بودن و سرعت شبکه مرورگر تور باشد، رله‌های بیشتری قابل استفاده هستند، زیرا هر رله، حجم بسیار زیادی از انتقال داده را برای ارائه دارد. اگر تعداد رله‌ها بیشتر باشد، ردیابی کاربر سخت‌تر می‌شود؛ یک لایه رمزگذاری شده در هر رله بعدی، رمزگشایی شده و باقی‌داده‌ها به هر رله ارسال می‌شود تا زمانی که به سرور مورد نظر خود برسد. برای سرور هدف، رله خروج به عنوان منبع داده نشان داده می‌شود، در نهایت، این داده‌های رمزگذاری شده، مجدداً رمزگذاری می‌شوند تا فقط رله ورودی بتواند آن را رمزگشایی نماید. هر رله دارای داده‌هایی می‌باشد که باید بدانند از کجا داده‌ها را دریافت کرده و به کجا داده‌ها را منتقل می‌کند (Mane & Khot, 2020: 25).

۴,۲. دارکوب و دیپوب از منظر حقوق بین الملل

در ارتباط با فضای دارکوب و فضای دیپوب در حقوق بین الملل می توان به موضوع هک شدن سیستم های دولتی اشاره نمود که این عمل غیرقانونی برای سرقت داده های دولتی در جنگ های پنهان و خاموش میان دولت ها مرسوم می باشد. هکراهی که برای دولت روسیه کار می کردند به رایانه های کمیته ملی دموکرات نفوذ کردند و ایمیل های مربوط به انتخابات ریاست جمهوری ۲۰۱۶ را سرقت کردند. هکراهی که در دولت چین ردیابی شده بودند، به رایانه های دولت ایالات متحده نفوذ کردند و پرونده های پرسنلی بیش از ۲۲ میلیون کارمند را کپی کردند. هکراهی کره شمالی در واکنش به فیلمی که رهبری کره شمالی را مسخره می کرد، وارد رایانه های شرکت سونی در ایالات متحده شدند. گزارش ها حاکی از آن است که ایالات متحده و اسرائیل، کامپیوترهای دولتی ایران را هک کردند تا سانتریفیوژهای خود را در یک نیروگاه هسته ای ایران غیرفعال کنند؛ اما تمام هک های دولتی به منظور جاسوسی یا انتقام نیست، در برخی از موارد، دولت ها به عنوان بخشی از تحقیقات جنایی قانونی، رایانه ها را هک می کنند. در دهه های اخیر، همکاری های بین المللی در تحقیق و اجرای قوانین کیفری به یک امر عادی تبدیل شده است. شبکه پیچیده ای از معاهدات جهانی، منطقه ای و دوجانبه در حال حاضر وجود دارد که به طیف گسترده ای از جرایم مانند جرایم سایبری، فساد، جرایم سازمان یافته فراملی، مواد مخدر و تروریسم پرداخته است. علاوه بر این موارد، شبکه ای از معاهدات عمدتاً دوجانبه بر استرداد و کمک های حقوقی متقابل برای جرائم قابل مجازات در هر دو حوزه قضایی متمرکز است؛ کشورها همچنین از طریق سازمان های بین المللی، خواه اینترپل، شورای اروپا، یا کمیسیون پیشگیری از جرم و عدالت سازمان ملل متحد، یا از طریق اجلاس های وزیران موقت در مورد پیشگیری از جرم، همکاری های گسترده ای دارند سفارت خانه ها در سرتاسر جهان از افرادی تشکیل شده اند که متهم به تحقیق در مورد جنایات فراملی بوده که اغلب به آنها وابسته قانونی می گویند. تماس های تلفنی فراملی، فکس ها، ایمیل ها و جستجوهای اینترنتی توسط مقامات مجری قانون در همه جا وجود دارد. آنها دیگر محدود به یادداشت های دیپلماتیکی که گاهی اوقات از یک سفارت خانه به یک وزارت خارجه یک کشور که ممکن است در دهه های گذشته وجود داشته باشد، نیستند. به صورت خلاصه، دولت ها دیگر به این موضوع که رفتار مجرمانه در قلمرو یک دولت مورد توجه دولت های دیگر است، واکنشی نشان نداده و به آسانی به دنبال همکاری عمل گرایانه بر مبنای متقابل برای مقابله با تهدیدات فراملی هستند. با توجه به ماهیت بدون مرز اینترنت، همکاری بین دولت ها بخش مهمی از تحقیقات جرایم رایانه ای را تشکیل می دهد (بنوشی، ۱۴۰۰: ۱۲۰).

۵,۲. ضرورت توجه به فضای دارکوب و دیپوب در حقوق بین الملل

مهم بودن و ضروری بودن توجه به فضای دارکوب از منظر حقوق داخلی و حقوق بین الملل، نیازمند توجه نمودن به مفهوم های وب سطح و وب عمیق (دیپوب) می باشد که تفکیک نمودن این دو فضا، ضرورت توجه به دیپوب را هویدا می کند. وصف ذاتی دیپوب که آن را مهم و متمایز می نماید، قرار گرفتن در حجاب گمنامی به لطف وجود امکانات سامانه های ناشناس کننده می باشد. این قسمت از وب جهانی توسط موتورهای جستجو، فهرست نشده و فقط به تقاضای مستقیم فرد یا افراد با وارد نمودن نشانی صفحه ها، توسط افراد پدیدآور یا کاربرهای تعریف شده، قابلیت دسترسی دارند. همچنین با بهره مندی از امکانات سامانه های ناشناس کننده، طرف های ارتباط، عمداً رد پای اینترنتی، هویت، موقعیت مکانی و محتویاتشان را از دید شاهدین بیرونی مخفی نمایند (Goldberg, 2017: 09). بر همین اساس، میزان و ابعاد گمنامی در دیپوب با وب سطح قابل قیاس نبوده و در بحث وب سطح، گرچه ممکن است اشخاص بخشی از هویت خود را به صورت هایی مانند استفاده نمودن از یک اسم مستعار مخفی کنند، سطحی از گمنامی که در آن و هویت کامل فرد و موقعیت مکانی و دیگر موارد مهم قابل شناسایی در وب سطح نیست (Raghavan & Garcia-Molina, 2011: 55).

اولین و قطعی ترین علت در توجیه نمودن ضروری بودن توجه و واکنش حقوق بین الملل به فضاهای دارکوب و دیپوب، یک واکنش فراسرزمینی مناسب می باشد. هیچ کشوری نمی تواند ادعای داشتن کنترل بر فضای وب را مطرح کند. فضای وب، یک مهم در موضوع حقوق بین الملل شناخته شده و تنظیم گری و قانون گذاری در حوزه های متعدد فضای وب، مانند دیپوب به تنهایی توسط هیچ دولتی میسر نخواهد بود. برخی از دولت ها به عللی از قبیل عدم وجود آگاهی، دانش فنی و نیروی انسانی متخصص، قادر به واکنش حقوقی کافی و مناسب به فضای دیپوب نیستند. این موضوع سبب افزایش یافتن استفاده های زبان بار و نادرست از این فضا در قلمرو دولت ها و ورود آسیب به

شهروندان می‌گردد. همچنین با توجه به ویژگی‌های فراسرزمینی، فضای دیپوب تبدیل به بهشتی برای مجرمان بین‌المللی و خطری خاموش و عظیم برای امنیت جهانی می‌شود که پنهان نمودن رد اثرات جرم در آن، امری ساده و فرآیندهای اجرایی لازم برای مقابله کردن با این اعمال، امری دشوار است. بر همین اساس، اثرات انفعال برخی از دولت‌ها، در عمل متوجه تمامی دولت‌ها و جامعه جهانی خواهد بود. اقدامات حقوقی بین‌المللی از یک جهت، کاستی‌های فنی و انسانی این دسته از دولت‌ها برای تقابل و کنترل فضای دیپوب را پوشش داده و از جهتی دیگر، از تبدیل خطرات ناشی از انفعال برخی از دولت‌ها به یک معضل با نتایج و اثرات بین‌المللی، ممانعت بعمل می‌آورد (Chertoff, 2017: 33).

برخی از اعمال زیان‌باری که تحت پوشش گمنامی فراهم شده، توسط فضای دیپوب واقع می‌گردد، نه تنها تهدیدی برای جوامع و دول مختلف می‌باشد، بلکه در ابعادی گسترده‌تر می‌تواند یک تهدید علیه صلح و امنیت بین‌المللی نیز به‌شمار آید. به عنوان نمونه، یکی از فعالیت‌های رایج در فضای دیپوب که عمدتاً در قالب رمزبازارها (بازارهای مجازی) صورت می‌پذیرد، خرید و فروش تسلیحات غیرمجاز می‌باشد. این شکل از معاملات، چارچوب‌های کنونی حقوق بین‌الملل را در زمینه کنترل تسلیحات را تهدید می‌کند. از جهتی دیگر، یکی از نگرانی‌های جدی در ارتباط با فضای دیپوب، استفاده گروه‌های تروریستی از ویژگی‌ها و امکانات ناشناس‌ساز این محیط برای مقاصد، مانند انجام تبلیغات، تدارک اطلاعات، تأمین مالی، جذب عضو، دستیافتن به تسلیحات و به تبع آن تسهیل نمودن حملات سایبری می‌باشد. از آنجایی که فناوری‌هایی مانند فضای دیپوب، سبب تسهیل فعالیت‌های گروه‌های تروریستی می‌شود، توجه حقوقی در ابعاد بین‌المللی به این موضوع برای کنترل نمودن خطرهای ناشی از این شکل از سوءاستفاده نمودن از فضای دیپوب یک امر ضروری است، چنان‌که در گزارش سال ۲۰۱۷م ارائه شده دبیرکل سازمان ملل در زمینه تهدیدات گروه تروریستی داعش برای امنیت و صلح بین‌المللی به شورای امنیت، تأکید شده تا بر اساس اعلان دولت‌های عضو، ارتباطات داخلی و پروسه جذب عضو، به سمت و سوی استفاده از روش‌های پنهان در حال حرکت می‌باشد که از جمله آن‌ها می‌توان به افزایش استفاده از فضای دیپوب و کدگذاری اشاره نمود. بر همین اساس، استفاده گروه‌های تروریستی از فضای دیپوب در راستای گسترش فعالیت‌های تروریستی، خود به تهدیدی جدی و مهم برای صلح و امنیت بین‌المللی بدل شده است (Denker, 2019: 120).

اكتفانمودن به عملکرد حاکمیت محور کشورها در حوزه فضای دیپوب، می‌تواند منتج به بروز یکسری ناهنجاری‌های بین‌المللی و نقض شدن چارچوب‌های اساسی و بنیادین مستقر و موجود در حقوق بین‌الملل شده و مسئولیت بین‌المللی آنها را در پی داشته است؛ برای مثال، می‌توان به گرایش برخی از دولت‌ها به استفاده از روش‌های تعقیب شبکه ای برای تقابل با جرم‌های ارتكابی در فضای دیپوب اشاره نمود. با توجه به معلوم نبودن هویت و موقعیت مکانی افراد کاربر در فضای دیپوب، این خطر وجود دارد که رایانه و شخص موضوع عملیات اجرایی این دسته از دولت‌ها، در قلمرو صلاحیتی دولتی دیگر باشد و در نتیجه، با اجرای این عملیات، صلاحیت اجرایی و قانونی یک دولت در قلمرو صلاحیتی یک دولت دیگر اعمال می‌گردد که بر طبق چارچوب‌های حقوق بین‌الملل حاضر، این اقدامها، اعمال نمودن صلاحیت فراسرزمینی به‌شمار آمده و مورد قبول و مشروع نیست. از جهتی دیگر، دولت‌هایی که با مجرمانه محسوب نمودن اصل استفاده از فضای دارکوب و فضای دیپوب، تلاش در ممنوع و محدود نمودن دسترسی افراد کاربر به این فضاها داشته و همچنین در راه نقض هنجارهای قبول شده فضای دیپوب، در حال حرکت هستند. واکنش این گروه از دولت‌ها که فضای دیپوب را به صورت اجمالی، تهدیدی علیه امنیت ملی خود محسوب می‌کنند، عمدتاً فراتر از حد ضرورت و تناسب بوده و می‌تواند منتج به تضییع شدن حقوق بشری آنلاین افراد کاربر گردد. این عوامل سبب شده تا فضای دیپوب توجه حقوق بین‌الملل را به خود جلب کند، به صورتی که کمیسیون اتحادیه اروپا در زمینه مهاجرت عنوان نموده که فضای دارکوب در حال تبدیل شدن به یک پناهگاه برای جرایم سازمان یافته می‌باشد و این موضوع، تهدیدی برای جامعه و اقتصاد اروپا محسوب شده و تنها در مقیاسی جهانی می‌توان با آن مقابله نمود (Kavallieros & Myttas & Kermitis & Lissaris, E. Giataganas, & Darra, 2021: 03).

۶.۲. جایگاه کنونی فضای دارکوب در حقوق بین‌الملل

افراد کاربر فضای دارکوب برای جلوگیری نمودن از نظارت و دخالت گسترده دولت‌ها و بازیگران خصوصی این عرصه، به وصف گمنام بودن این فناوری و حمایت‌هایی که از آن در پناه حقوق بشر امکان دارد، امید بسته‌اند (Faizan & Khan, 2019: 41).

بر همین اساس، کارکردهای مثبت فضای دارکوب عمدتاً مورد حمایت حقوق بین‌الملل بشر واقع شده است. البته در اسناد و رویه‌های حقوق بین‌الملل، کماکان ادله کافی برای قبول یک حق مستقل با نام حق بر گمنامی وجود ندارد؛ اما این موضوع به معنای عدم امکان حمایت از گمنامی در

نظام بین الملل حقوق بشر نیست (غفوری، ۱۳۹۹: ۲۵). ممنوع بودن گمنامی فراهم شده در فضای دارکوب، با حق بر آزادی عقیده و بیان و حق بر حریم خصوصی دارای تطابق نبوده و با این وجود، از یک جهت، از کارکردهای منفی فضای دارکوب را نمی توان غافل شد و از جهتی دیگر، هر دو حق بر حریم خصوصی و حق بر آزادی عقیده و بیان حقوقی مطلق نبوده و بر طبق مصالح اجتماعی می توانند محدود شوند؛ از این رو، حق بر گمنامی، حقی مطلق نبوده و بر اساس ملاحظات مشروعی که در چارچوب نظام بین المللی حقوق بشر قبول گردیده اند، قابلیت محدود شدن دارند. راهکار عاقلانه برای تدوین نمودن قواعد بین المللی در حوزه فضای دیپوب، اولویت دادن به اصل بر آزادی استفاده از فضای دیپوب برای حمایت نمودن از کارکردهای مثبت و در نقطه مقابل، تحدید و تعدیل نمودن آن بر طبق واقعیت های موجود و ملاحظات مشروع پذیرفته شده در حقوق بین الملل در زمینه کنترل نمودن کارکردهای منفی این فضا می باشد. اکنون می توان ادعا نمود که فضای دیپوب، به عنوان یک موضوع دارای اهمیت و وصف بین المللی، در ابعاد بین المللی با واکنش حقوقی خاص و مناسب و فراگیر، همراه نبوده است (Ertan & Floyd & Pernik, 2019: 16).

فضای دیپوب، بخشی مهم و ناپیدا از فضای وب و جدیدتر و نشناخته تر از آن می باشد؛ اکنون در حالی سخن از واکنش های حقوقی در ابعاد بین المللی بیان می شود که با گذشته ۳۰ سال از رواج فراگیر اینترنت، کماکان عدم وجود یک نظام حقوقی جامع و منسجم در ابعاد بین المللی برای فضای اینترنت، احساس می گردد. تلاش هایی که تاکنون برای نظام مند نمودن فضای اینترنت در ابعاد بین المللی انجام شده است، موفقیت چندانی در ایجاد کردن یک نظم حقوقی جامع که پاسخگوی ویژگی های ذاتی فضای وب و چالش های بین المللی آن باشد، نداشته اند. بخشی قابل توجه از انفعال حقوق بین الملل در مقابل فضای دیپوب، ریشه در علت ناکامی ایجاد یک چارچوب حقوقی بین المللی برای فضای اینترنت به صورت کلی دارد. دلیل اصلی در واکنش ناکافی بوده نظام حقوق بین الملل نسبت به فضای وب و سختی محقق شدن اجماع بین المللی، شکافی گسترده در مواضع و دیدگاه های دولت ها در زمینه مسائل چالشی حوزه فضای وب، مانند حق بر حریم خصوصی، حق بر آزادی بیان، حق بر گردش آزاد اطلاعات و... می باشد. به عنوان نمونه، اکثر کشورهای اروپایی در مواجهه با محتوای زیان بار در فضای آنلاین، بر حذف شدن آن ها تأکید دارند، در حالی که کشور ایالات متحده آمریکا، بر اساس اصلاحیه نخست قانون اساسی خود، حق بر آزادی بیان را نسبت به حفاظت از جامعه و افراد شهروند در مقابل محتوای زیان بار، یک اولویت محسوب نموده است. همچنین در مورد تقابل احتمالی حق بر آزادی بیان و حق بر حریم خصوصی اتحادیه اروپا، حریم خصوصی شهروندان را واجد اولویت و کشور ایالات متحده آمریکا، حق بر آزادی بیان را مقدم محسوب نموده است. برخی دیگر از دولت های قدرتمند، مانند جمهوری خلق چین و روسیه نیز در تقابل با فضای دیپوب بیش از هر چیز دیگر، بر موضوع امنیت ملی توجه نموده و موضع خود را در مقابل این قبیل تحولات را بر مبنای این ملاحظه تنظیم می نمایند. نبود یک واکنش حقوقی مناسب و خاص، به فضای دیپوب در ابعاد بین المللی، اثراتی مانند امنیت و مصونیت افراد کاربر هنجارشکن، محروم شدن افراد کاربر قانونمند از حقوق مشروع خود در برخی از دولت ها و قرار گرفتن دولت ها در معرض مسئولیت بین المللی را در پی دارد. یکسان سازی مقررات ملی و تدوین نمودن سندهای دوجانبه و چندجانبه در زمینه همکاری های اجرایی و قضایی در زمینه جرایمی که در فضای دیپوب صورت می گیرد، می تواند سبب کاستیهایی در راهکارهای صرفاً ملی و نواقصات ناشی از نبود قواعد بین المللی در این حوزه را در کوتاه مدت تا حد زیادی جبران نماید (Breckheimer, 2010: ۱۴۹).

نتیجه گیری

فضای اینترنت را می‌توان به‌طور کلی به سه بخش تقسیم نمود: وب‌سطح، دیپ‌وب و دارک‌وب که از میان آنها، بخش دوم، ناشناس بودن را به کاربران و میزبانان خود ارائه می‌دهد. دیپ‌وب یک شبکه رمزگذاری شده است که در نتایج جستجوی موتورهای جستجوگر، مانند گوگل، یاهو، بینگ و... شناسایی نمی‌گردد. کاربران بایستی از مرورگر تور برای دسترسی به فضای دیپ‌وب و بازدید سایت‌های موجود در این فضا استفاده کنند. میزان ۹۶٪ فضای وب به علت پنهان بودن جزء فضای دیپ‌وب محسوب می‌شود، فضای اینترنت همانند یک کوه یخ می‌باشد که مردم فقط می‌توانند بخشی کوچک از قسمت بالای کوه را مشاهده کنند، در حالی که بخش اعظم این کوه در زیر دریا پنهان شده است. روش‌های پایه تئوری گراف و داده‌کاوی که به تحلیل شبکه‌های اجتماعی می‌پردازد، می‌تواند به صورت جامع برای درک و یادگیری فضای دیپ‌وب و شناسایی تهدیدات سایبری مورد استفاده قرار گیرد. از آنجایی که فضای اینترنت به سرعت در حال تکامل بوده و محدود کردن دسترسی به فضای دیپ‌وب تقریباً امری غیرممکن می‌باشد، نیاز به توسعه مکانیزم و ابزارهای استاندارد برای نظارت بر این فضا احساس می‌شود. فضای دیپ‌وب، به دلیل وجود ویژگی‌هایی، مانند ناشناس بودن، در تمایز بین کاربران مخرب و معتبر ناتوان بوده و مقامات اجرایی بایستی با اجرای تکنیک‌هایی که از حریم خصوصی کاربران و همچنین دستگیری مجرمان مراقبت می‌کند، با این چالش مقابله کنند؛ این کار را می‌توان با بررسی سایت‌های کلاهبردار به جای کاربران متقلب به صورت موثر انجام داد. گشت‌وگذار در وبسایت‌های موجود در فضای دارک‌وب، عملی اشتباه یا غیرقانونی محسوب نمی‌گردد، اما درگیر شدن در فعالیت‌های غیرقانونی موجود در فضای دارک‌وب، عملی اشتباه است. مقابله و برخورد با جرایم موجود در فضای دارک‌وب و فضای دیپ‌وب، به علت ناشناس بودن گردانندگان سایت‌های موجود در این فضا، امری محال و سخت بوده که در حقوق بین‌الملل با توجه به گسترده بودن دامنه این جرایم، وجود همکاری‌های بین‌المللی در این زمینه احساس می‌شود. در حقوق بین‌الملل، مقابله با جرایم موجود در فضای دارک‌وب و فضای دیپ‌وب، که در یک نقطه از دنیا متمرکز نبوده و در هر کشور، انجام این جرایم مقدور است، نیازمند قوانینی جامع و همچنین یک سازمان تخصصی در این زمینه می‌باشد تا با وجود یک استقلال قضایی بین‌المللی به مقابله با این جرایم سازمان‌یافته بپردازد. متأسفانه در این زمینه، کشورها به صورت سلیقه‌ای عمل نموده و در عمل، بسیاری از کشورها در مقابله با جرایم موجود در فضای دیپ‌وب ناتوان هستند، به این علت که ردیابی مجرمین، کاری بسیار سخت بوده و در فرضی که مجرمین ردیابی شده و در قلمرو حاکمیتی یک کشور دیگر باشند، در اکثر موارد، کشورها برای دستگیری و استرداد مجرمین با همدیگر همکاری نمی‌کنند که این موضوع سبب شده تا فضای دیپ‌وب، بستری امن برای مجرمین شود.

منابع

۱. السان، مصطفی و دوان یامچی، امین. (۱۳۸۳)، «ماهیت رایانه‌ای و جنبه‌های حقوقی امضای دیجیتالی»، مجله دیدگاه‌های حقوقی شماره‌های ۳۰ و ۳۱، ۲۴-۷۷.
۲. صادقی، محسن و ناصر، مهدی. (۱۳۹۹)، خطرات حقوقی امضای الکترونیکی و الزامات قانونی در پیشگیری از آنها: مطالعه تطبیقی در حقوق ایران و آمریکا، نشریه‌ی پژوهش نامه بازرگانی شماره ۹۶، ۱۸۹-۲۲۴.
۳. صادقی، محسن و ناصر، مهدی. (۱۳۹۸). «اعتبارسنجی و چالش‌های حقوقی به کارگیری قراردادهای هوشمند: با مطالعه تطبیقی نظام حقوقی ایران و آمریکا»، فصلنامه پژوهش حقوق خصوصی، سال هفتم شماره ۲۷، ۲۲۵-۲۸۸.
۴. صادقی‌نشاط، امیر. (۱۳۹۳)، «اعتبارسنجی اسناد الکترونیک»، فصلنامه پژوهش حقوق خصوصی، سال سوم، شماره هشتم، ۷۲-۱۰۰.
۵. صفایی، سید حسین. (۱۳۸۶)، دوره مقدماتی حقوق مدنی، جلد دوم: قواعد عمومی قراردادها، ج ۲، چاپ پنجم، تهران: نشر میزان.
6. Agrawal, Ravikan. (24 May 2018). "Digital Signature for Blockchain Context", (Last visit: September 2, 2022), <https://ravikantagrawal.medium.com>.
7. Arcari, Jared. (2019). "Decoding Smart contracts: Technology, Legitimacy, & Legislative Uniformity", *Fordham Journal of Corporate and Financial Law*, Vol. 24, No. 2, 364-396.
8. Blythe, Estephen. (2005). "Digital Signature Law of the United Nations, European Union, United Kingdom & United States: Promotion of Growth in E-Commerce With Enhanced Security", *Richmond Journal of Law and Technology*, Vol. 11, No. 2, 1-20.
9. Cannarsa, Michel (1 December 2018). "Interpretation of Contracts and Smart Contracts: Smart Interpretation or Interpretation of Smart Contracts?". *European Review of Private Law*. 26 (6): 773–785. doi:10.54648/ERPL2018054. S2CID 188017977.
10. Cohn, Alan, West, Travi & Parker, Chelsa. (2017). "Smart After All: Blockchain, Smart Contracts, Parametric Insurance, and Smart Energy Grids", *GEO. Law Tech. Review*, Vol. 1, 273-303.
11. "Cómo se usa". (2018). Uruguay.
12. Drummer, Daniel; Neumann, Dirk (5 August 2020). "Is code law? Current legal and technical adoption issues and remedies for blockchain-enabled smart contracts". *Journal of Information Technology*. 35 (4): 337–360. doi:10.1177/0268396220924669. ISSN 0268-3962.
13. E. Stern, Jonathan. (2001). "The Electronic Signatures in Global and National Commerce Act", *Berkeley Tech. Law Journal*, Vol. 16, 391- 395.
14. "Electronic Communications and Transactions Act [No. 25 of 2002]". *Government Gazette*. 446 (23708). (2 August 2002). Republic of South Africa.
15. "Electronic Transaction Law". *Communication and Information Technology Commission*. Saudia Arabia.
16. "Elektronik İmza Kanunu [Electronic Signature Act]". (2004-01-23). *Mevzuat Bilgi Sistemi (in Turkish)*. Resmi Gazete.
17. *Federal Electronic Signatures in Global and National Commerce Act*. (2000), United States.
18. Filatova, Nataliia (1 September 2020). "Smart contracts from the contract law perspective: outlining new regulative strategies". *International Journal of Law and Information Technology*. 28 (3): 217–242. doi:10.1093/ijlit/eaad015. ISSN 0967-0769.
19. Fischer, Susanna Fredrick. (2001). "Saving Rosencrantz & Guildenstern in a Virtual World a Comparative Look at Recent Global Electronic Signature Legislation", *B. VJ.SCI. & Tech Law*, Vol. 7, 229-233.
20. Fries, Martin; P. Paal, Boris (2019). "Smart Contracts" *Mohr Siebeck*. ISBN 978-3-16-156911-1. JSTOR j.ctvn96h9r.
21. Fulmer, Nathan. (2019). "Exploring the Legal Issues of the Blockchains Applications", *Akron Law Review*, Vol. 52, No. 1, Article5, 162-191.
22. *Guidance Note Regarding the Relation Between the Uniform Electronic Transaction Act and Federal Esign Act, Blockchain Technology and "Smart Contracts"*.
23. J.Smeding, Thomas. (1999). "Electronic Contracts & Digital Signatures: An Over View of Law & Legislation", *PLI.PAT*, Vol. 564, No. 125.
24. JA, Ashiq. (2016). "Recommendations for Providing Digital Signature Services".
25. Jaikaran, Chris. (2018). "Blockchain: Background and Policy Issues", *Congressional Research Service Analyst in Cybersecurity Policy*, R45116, 1-11.

26. Katz, Jonathan; Lindell, Yehuda. (2007). "Chapter 12: Digital Signature Schemes". Introduction to Modern Cryptography.
27. "Law 15-04". (February 1, 2015). Official Journal. Algeria.
28. "Ley-19799 Sobre Documentos Electronicos, Firma Electronica Y Servicios de Certification de Dicha Firma". (2002). Ley Chile – Biblioteca del Congreso Nacional.
29. O'Shield, Roggie. (2017). "Smart Contracts: Legal Agreements for The Blockchain", 21 N.C. Banking Inst, 177-194.
30. Reed, Chris & John, Angel. (2007). "Computer Law 6th Edition", Oxford University, 232-233.
31. Rohr, J. G. (2019). "Smart Contracts and Traditional Contract Law, or: The Law of the Vending Machine", Cleveland State Law Review, Vol. 67, No. 1, 71-92.
32. Röscheisen, Martin; Baldonado, Michelle; Chang, Kevin; Gravano, Luis; Ketchpel, Steven; Paepcke, Andreas (1998). "The Stanford InfoBus and its service layers: Augmenting the internet with higher-level information management protocols". Digital Libraries in Computer Science: The MeDoc Approach. Lecture Notes in Computer Science. Vol. 1392. Springer. pp. 213–230. doi:10.1007/bfb0052526. ISBN 978-3-540-64493-4.
33. Savelyev, Alexander (14 December 2016). "Contract Law 2.0: "Smart" Contracts As the Beginning of the End of Classic Contract Law". Social Science Research Network. SSRN 2885241.
34. Secure Electronic Signature Regulations SOR/2005-30". (10 March 2011) Justice Laws Website.
35. Szabo, Nick (1997). "View of Formalizing and Securing Relationships on Public Networks | First Monday". First Monday. doi:10.5210/fm.v2i9.548. S2CID 33773111.
36. T.svikhart, Riley. (2017). "Blockchain's Big Hurdle", Stanford Law Review, Volume 70, 100-111.
37. Tapscott, Don; Tapscott, Alex (May 2016). "The Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money", Business, and the World. Portfolio/Penguin. pp. 72-83, 101, 127. ISBN 978-0670069972.
38. The Information Technology Act". (2000). Department of Telecommunications, Ministry of Communication, Government of India. The Gazette of India Extraordinary.
39. Turner, Dawn. (2016). "Major Standards and Compliance of Digital Signatures – A World-Wide Consideration".
40. "Uniform Electronic Transaction Act". (1999). United States.
41. "US E-Sign Act of 2000". (2000). United States.