فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال سوم | شماره دوم | تابستان ۱۴۰۲
ویگا مجله: https://cyberlaw.maragheh.iau.ir:
ISSN: 2821-126X

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.

فصلنامه علمی
مطالعات حقوقی فضای مجازی
صفحات مقاله ۴۱ الی ۵۳

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@yahooIcom
احمد رادمان
گروه حقوق بین الملل، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران
Ahmadradman1994@gmail.com

تاریخ دریافت : ۲۳ خرداد ۱۴۰۲ تاریخ پذیرش: ۳۱ تیر ۱۴۰۳

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، موادمخدر، برده و اعضای بدن انسان از تجارتهای اصلی در فضای دارک‌وب بوده که با استفاده از ارزهای دیجیتالی انجام می‌شوند. امروزه با توجه به پیشرفت سریع تکنولوژی‌های ارتباطی و عدم وجود قوانین بین‌المللی تخصصی در حوزه فضای‌سایبری، 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، جرایم‌سایبری، دارک‌وب، دیپ‌وب.

مقدمه

خصیصه اصلی فضای‌سایبری 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 تکنولوژی‌های‌ارتباطی، علیرغم وجود مزایای فراوان، دارای معایبی نیز می‌باشند؛ با نگاهی به وب‌سایت‌های مختلف می‌توان به این نتیجه رسید که صنعت‌وب 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 تکنولوژِی 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 سوءاستفاده‌کردن از اشخاص کاربر در این فضا و ایجاد مشکلاتی برای آنها می‌باشند. فضای‌سایبری، 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 حریم‌خصوصی بوده که برای محافظت نمودن از کاربرهای اینترنتی در برابر حملات تجزیه‌وتحلیل‌های ترافیکی که از جانب یک غول غیرقانونی جهانی در حوزه وب به وجود آمده، به‌کارمی‌رود (باقرپور،۱۴۰۰: ۲۴). افرادی از این نرم‌افزار استفاده می‌کنند، اکثراً از کشورهای‌اروپایی، جمهوری‌خلق‌چین و ایالات‌متحده‌آمریکا 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 غیرقابل‌ردیابی 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,2008: 74 18) در حوزه حقوق بین‌الملل، در موارد مشابه با مبحث فضای‌مجازی می توان به بحث مبحث حق‌برفراموشی و پرونده گوگل‌اسپانیا و سند اخلاق و حفاظت از داده ها 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 کشتارجمعی و جنگ‌افزارهای‌نظامی، به کامپیوترها و فضای‌سایبری منتقل‌شده 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 نموده اند؟ در حوزه جرایم‌سایبری 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، کشورخسارت‌دیده 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 می توان 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 فضای‌سایبری و جرایم این حوزه

فضای‌سایبر در علم لغت به معنای فضایی‌مجازی و غیرواقعی بوده و فعالیت‌های‌سایبری یا کامپیوتری به زبان بسیار ساده به معنی یک مجموعه از ارتباط‌های میان افراد از طریق رایانه و دستگاه‌های مخابراتی، بدون درنظرداشتن مختصات جغرافیای فرد می‌باشد (صفدری و بابایی

پور، ۱۴۰۱: ۰۳). در تعریفی دیگر، فضای‌مجازی 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 جرایم‌سایبری می‌توان به دستورالعمل تالین نیز اشاره داشت و می‌توان گفت یک سند مهم در زمینه مبارزه با جرایم‌سایبری 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 عملیات‌های‌سایبری، 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 از۲۳ نفر فرد متخصص بوده و کار آنان توسط یک گروه ۱۳ نفره متخصص دیگر بررسی گردید. این امر منتج به منتشرشدن نخستین دستورالعمل تالین گردید، که بر قوانین جنگ متمرکز بود. در دومین دستورالعمل تالین برخلاف سند اول، نه تنها عملیات‌سایبری با آستانه بالا را پوشش داده شده، بلکه شامل آن گروه از اقدام‌های‌سایبری که اثر و مقیاس بیشتری داشته و امکان دارد که منتج به نقض توسل به زور شود، یا اقدام‌های‌سایبری 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 مجرمان‌سایبری، 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).

جرایم‌سایبری به موازات فرصت‌هایی که از طریق افزایش سریع استفاده از اینترنت برای تجارت‌الکترونیک و در کشورهای‌درحال‌توسعه ایجاد می‌شود، تکامل یافته‌اند. دلیل اصلی رشد جرایم‌سایبری از اواسط دهه ۲۰۰۰ به گسترش «بات‌نت‌ها» به عنوان ابزارهای انبوه برای سوءاستفاده از رایانه و تقویت این فعالیت‌ها از طریق (کیت‌های ابزار)، (مانند زئوس) 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 سرقت‌شده، مانند جزئیات کارت‌اعتباری را با پرداخت هزینه‌ای مشخص، دانلود کنند. به صورت خلاصه، جرم‌سایبری 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 جرایم‌سایبری به درجه بالایی از سازماندهی و تخصص نیاز دارند، شواهد و مدارک کافی برای تعیین اینکه آیا جرایم‌سایبری اکنون تحت سلطه گروه‌های جرایم‌سازمان‌یافته 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 فضای‌سایبری با دنیای حقیقی، نیازمند تغییر در مفهوم‌ها و ارکان بعضی مبحث‌ها و اصطلاح‌های حقوقی در این فضا می‌باشد. از جمله این مباحث، بحث جرایم و مجازات‌ها می‌باشد که در زمینه بستر وقوع جرایم می‌توان به فضای‌دیپ‌وب 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 قرارداشته و توسط موتورهای جستجو مانند گوگل، بینگ، یاهو 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 به‌صورت 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 فضای‌دیپ‌وب قابل مشاهده هستند. از آنجایی که عمل اعتبارسنجی برای دسترسی به داده‌هایی مانند حساب‌های بانکی یک عمل اجباری قانونی بوده، وب‌سایت‌های موجود در فضای‌دیپ‌وب، 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).

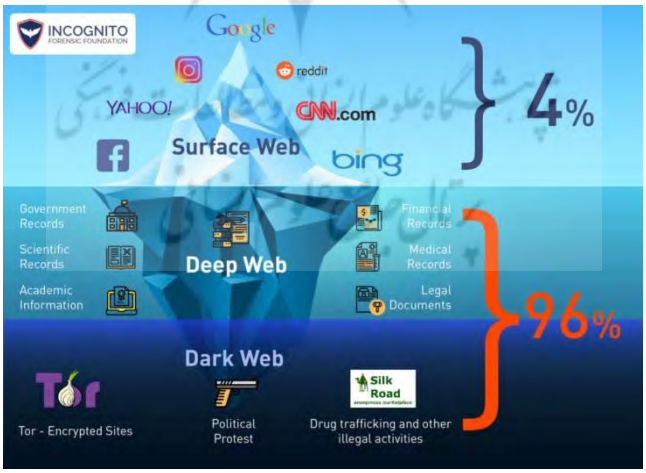
۲و۱. دیپ‌وب

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 وب‌اصلی قانونی شده، همانند وب‌سایت‌هایی از جمله آمازون ، آی. اِم. دی. بی، نتفلیکس می‌باشد، به این دلیل که این وب‌سایت‌ها به صورت سفارشی برای کاربران طراحی شده و نیازی به فهرست‌کردن 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 زمان‌بندی بوده و بعد از بازه زمانی مشخص از دسترس خارج می‌شوند (Xiaolei,2015: 45).



تصویر ۱-۱- بخش‌بندی فضای اینترنت بر اساس درصد مشاهده کاربران:

الف) وب‌سطح ۴٪: سایت‌های عمومی و موتورهای جستجوگر مانند گوگل، یاهو، بینگ؛ سایت‌های خبرگزاری مانند سی. اِن.اِن، یورو نیوز؛ شبکه‌های اجتماعی مانند اینستاگرام، فیس‌بوک،واتساپ، توییتر و... .

و فضای دارک‌وب که شامل فضای برای انجام اعمالی مانند خریدوفروش داروی قاچاق، اعتراضات‌سیاسی، فروش‌اسلحه و ادوات نظامی، مهمات، مواد منفجره ممنوعه، پورنوگرافی‌کودکان، برده‌فروشی، قاچاق‌اعضای‌بدن‌انسان و...

۲-۲-دارک‌وب

دارک‌وب محتوای پنهان موجود وب‌جهانی بوده، تشکیل دهنده بخشی از دیپ‌وب بوده و از فضای‌اینترنت استفاده می‌کند، اما برای دسترسی‌داشتن به این فضا، نیاز به یک مرورگر مخصوص، مجوز و وجود تنظیمات رایانه‌ای خاصی می‌باشد. در فضای‌دیپ‌وب، محرمانه‌بودن اطلاعات و هویت افراد حاضر در این فضا، از اولویت‌های مهم بوده و این موارد توسط موتورهای جستجوی‌وب 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. فضای‌دارک‌وب، یک اینترنت‌رمزگذاری‌شده 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 می باشد، 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 حریم‌خصوصی و استفاده‌های غیرقانونی مانند معامله با موادمخدر، جزئیات‌کارت‌اعتباری سرقت‌شده و شرطبندی و فروش برده، پورنوگرافی‌کودکان، فروش اسلحه و مهمات جنگی و... اشاره نمود (Dalins& Wilson& Marc, 2018: 33).

فضای‌دارک‌وب، مجموعه‌ای از خدمات پنهان‌شده از دید موتورهای جستجو و کاربران عادی بوده و توسط مجرمان‌سایبری برای ارائه انواع خدمات و کالاهای غیرقانونی استفاده می‌شود. فعالیت های مجرمانه سایبری در فضای‌دارک‌وب 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,). (النابوسی و همکاران،۲۰۱۸: ۴۵).

امروزه از تحلیل شبکه‌های‌اجتماعی برای بررسی انواع پدیده‌ها و فرآیندهای اقتصادی و سازمانی استفاده می‌شود. تجزیه‌وتحلیل شبکه‌های‌اجتماعی به صورت موثر برای مقابله با پولشویی، سرقت‌هویت، کلاهبرداری‌آنلاین، حملات‌سایبری و به‌ویژه، روش‌های ارائه‌شده در این شبکه‌ها در بررسی بسیاری از عملیات غیرقانونی با اوراق‌بهادار 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 برروی 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 ارسال‌شده 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، وب‌سایت ها 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 موقعیت‌مکانی 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 فضای‌دیپ‌وب کدگذاری شده و ایمن بوده و دسترسی به شبکه‌ها را نمی‌توان مسدود کرد که این امر، اتصالات و

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

۲،۲،۲. خصوصیات دارک‌وب

داده‌های ارسال‌شده توسط برنامه‌های کاربردی مبتنی بر وب در بخش وب‌سطح، در برابر نقض های امنیتی و سایر حملات بسیار آسـیب پـذیر هستند. از سویی دیگر، دارک‌وب ویژگی‌های قابل توجهی، مانند حفظ‌حریم‌خصوصی کاربران در هنگام دسترسی یا اسـتفاده از اینترنـت، حفـظ ناشناس‌بودن و ارائه محرمانه‌بودن، تبادل اطلاعات با سانسوراینترنتی، خرید کالاهای محدود، آزادی بیان و غیـره را ارائـه مـی‌دهـد. برخـی از مزایای دارک‌وب عبارتند از:

–ناشناس‌بودن 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 نشده‌انـد و پـس از جسـتجو، هیچگونه تاریخچه‌ای در مرورگر به جا نمی‌گذارند؛ این ناشناس‌بودن سطح امنیتی بالایی را در فضای‌دارک‌وب فراهم می‌کنـد، زیـرا هویـت و مکان کاربران پنهان بوده و به دلیل سیستم رمزگذاری چند لایه، قابل ردیابی نمی‌باشد؛

–خرید کالای محدود: خرید برخی از کالاها در دارک وب قابل توجیه است؛ بـه عنـوان مثـال، برخـی از داروهـا، ماننـد قـرص‌هـای خـواب 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 عدم‌افشای هویت افراد در فضای دارک‌وب می باشـد؛ دارک‌وب این امتیاز را برای ابراز آزادانه نظر در مورد هر موضوعی، بدون هیچ ترسی فراهم نموده و افراد می‌تواننـد نظراتشـان را در مـورد هـر موضوعی بدون تردید و ترس از تهدیدات جانی و امنیتی بیان کنند (Griffith & Xu& Ratti,2017: 29).

۳،۲. مرورگرتور، مسیر دسترسی به دیپ‌وب و دارک‌وب

دارک‌وب شامل وب‌سایت‌هایی است که در قسمت پنهان یا سایت های فهرست نشده اینترنت وجود دارند؛ این فضا در شبکه ای خاص وجـود دارد که در وب‌سطح قابل مشاهده نیست. کاربران تنها با استفاده از مرورگر تور که نقطه اصلی در دسترسی به فضای‌دیپ‌وب است، قـادر بـه مشاهده و دسترسی فضای‌دارک‌وب هستند. مرورگر تور عمدتاً برای بسیاری از اهداف خاص توسعه یافته است؛ این مرورگر نخستین بار توسط آزمایشگاه تحقیقات دریایی ایالات متحده آمریکا در قـرن بیسـت و یکـم توسـعه یافـت و هـدف از توسـعه آن، فـراهم‌کـردن طبقـه‌بنـدی و محرمانه‌ماندن اطلاعات نیروهای مسلح ایالات متحده آمریکا که درگیـر عملیـات‌هـای‌نظـامی در خـارج از خـاک آمریکـا بودنـد، مـی باشـد (Biswas& Fidalgo& Evanovich,2017: 63).

مرورگر تور بر اساس مدل تکنیک(مسیریابی پیازی) عمل می‌کند که در آن اطلاعات کاربر ابتدا رمزگذاری شده و سـپس از طریـق رلـه‌هـای 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 پنهان‌کردن هویت کاربر استفاده می‌شود. با یک پرش از نقطه اتصالات از رایانه کاربر به نقطه هدف از طریـق زنجیـره رلـه‌ای واسـطه عمـل می‌کند (Yadava & Bhushanb & Saxenaa, 2020: 15). این موارد در سرتاسر جهان قابل مشاهده و کاملاً توسط داوطلبانی اجرا می‌شوند که به همین‌دلیل آماده‌اند تا برخی از ظرفیت‌های انتقال‌داده را کنار بگذارند. هنگامی که نگرانی اصلی در دسترسی به فضای‌دارک‌وب، ناشناس بودن و سرعت شبکه مرورگر تور باشد، رله‌های بیشتری قابل استفاده هستند، زیرا هر رله، حجم بسیار زیادی از انتقال‌داده را بـرای ارائـه دارد. اگر تعداد رله‌ها بیشتر باشد، ردیابی کاربر سخت‌تر می‌شود؛ یک لایه رمزگذاری‌شده در هر رله بعدی، رمزگشایی‌شده و باقی‌داده‌ها بـه هـر رلـه ارسال می‌شود تا زمانی که به سرورموردنظرخود برسد. برای سرور هدف، رله‌خروج به عنوان منبـع داده نشـان داده مـی‌شـود، در نهایـت، ایـن داده‌های رمزگذاری شده، مجدداً رمزگذاری می‌شوند تا فقط رله‌ورودی بتواند آن را رمزگشایی نماید. هر رله دارای داده‌هایی می‌باشد کـه بایـد بداند از کجا داده‌ها را دریافت کرده و به کجا داده‌ها را منتقل می کند (Mane & Khot2020: 25).

۴،۲. دارک‌وب و دیپ‌وب از منظر حقوق‌بین‌الملل

در ارتباط با فضای‌دارک‌وب و فضای‌دیپ‌وب در حقوق بین‌الملل می‌توان به موضوع هک‌شدن سیستم‌های دولتی اشاره نمود که این عمل غیرقانونی برای سرقت داده‌های دولتی در جنگ‌های پنهان و خاموش میان دولت‌ها مرسوم می باشد. هکرهایی که برای دولت روسیه کار می‌کردند به رایانه‌های کمیته ملی دموکرات نفوذ کردند و ایمیل های مربوط به انتخابات ریاست جمهوری ۲۰۱۶ را سرقت کردند. هکرهایی که در دولت چین ردیابی شده بودند، به رایانه‌های دولت ایالات متحده نفوذ کردند و پرونده‌های پرسنلی بیش از ۲۲ میلیون کارمند را کپی کردند. هکرهای کره‌شمالی در واکنش به فیلمی که رهبری کره‌شمالی را مسخره می‌کرد، وارد رایانه های شرکت سونی در ایالات متحده شدند. گزارش‌ها حاکی از آن است که ایالات متحده و اسرائیل، کامپیوترهای دولتی ایران را هک کردند تا سانتریفیوژهای خود را در یک نیروگاه هسته‌ای ایران غیرفعال کنند ؛ اما تمام هک‌های دولتی به منظور جاسوسی یا انتقام نیست، در برخی از موارد، دولت‌ها به عنوان بخشی از تحقیقات جنایی قانونی، رایانه ها را هک می‌کنند. در دهه‌های اخیر، همکاری‌های بین‌المللی در تحقیق و اجرای قوانین‌کیفری به یک امر عادی تبدیل شده است. شبکه پیچیده‌ای از معاهدات جهانی، منطقه ای و دوجانبه در حال حاضر وجود دارد که به طیف گسترده‌ای از جرایم مانند جرایم سایبری، فساد، جرایم‌سازمان‌یافته‌فراملی، موادمخدر و تروریسم پرداخته است. علاوه بر این موارد، شبکه ای از معاهدات عمدتاً دوجانبه بر استرداد و کمک‌های حقوقی متقابل برای جرائم قابل مجازات در هر دو حوزه قضایی متمرکز است؛ کشورها همچنین از طریق سازمان‌های بین‌المللی، خواه اینترپل، شورای اروپا، یا کمیسیون پیشگیری از جرم و عدالت سازمان‌ملل‌متحد، یا از طریق اجلاس‌های وزیران موقت در مورد پیشگیری از جرم، همکاریهای‌گسترده‌ای دارند سفارت‌خانه‌ها در سرتاسر جهان از افرادی تشکیل شده‌اند که متهم به تحقیق در مورد جنایات‌فراملی بوده که اغلب به آنها وابسته قانونی می‌گویند. تماس‌های تلفنی فراملی، فکس‌ها، ایمیل‌ها و جستجوهای اینترنتی توسط مقامات مجری قانون در همه‌جا وجود دارد. آنها دیگر محدود به یادداشت‌های دیپلماتیکی که گاهی اوقات از یک سفارت‌خانه به یک وزارت خارجه یک کشور که ممکن است در دهه‌های گذشته وجودداشته‌باشد، نیستند. به صورت خلاصه، دولت‌ها دیگر به این موضوع که رفتارمجرمانه در قلمرو یک دولت مورد توجه دولت‌های دیگر است، واکنشی نشان نداده و به آسانی به دنبال همکاری عمل‌گرایانه بر مبنای متقابل برای مقابله با تهدیدات فراملی هستند. با توجه به ماهیت بدون مرز اینترنت، همکاری بین دولت‌ها بخش مهمی از تحقیقات جرایم رایانه ای را تشکیل می‌دهد (بنوشی، ۱۴۰۰: ۱۲۰).

۵،۲. ضرورت توجه به فضای‌دارک‌وب و دیپ‌وب در حقوق‌بین‌الملل

مهم بودن و ضروری‌بودن توجه به فضای‌دارک‌وب از منظر حقوق‌داخلی و حقوق‌بین‌الملل، نیازمند توجه نمودن به مفهوم‌های وب‌سطح و وب‌عمیق(دیپ‌وب) می باشد که تفکیک‌نمودن این دو فضا، ضرورت توجه به دیپ‌وب را هویدا می‌کند. وصف ذاتی دیپ‌وب که آن را مهم و متمایز می‌نماید، قرار گرفتن در حجاب گمنامی به لطف وجود امکانات سامانه‌های ناشناس‌کننده می‌باشد. این قسمت از وب‌جهانی توسط موتورهای جستجو، فهرست‌نشده و فقط به تقاضای مستقیم فرد یا افراد با وارد نمودن نشانی صفحه‌ها، توسط افراد پدیدآور یا کاربرهای تعریف‌شده، قابلیت دسترسی دارند. همچنین با بهره‌مندی از امکانات سامانه‌های ناشناس‌کننده، طرف‌های ارتباط، عمداً ردپای اینترنتی، هویت، موقعیت مکانی و محتویتشان را از دید شاهدین بیرونی مخفی نمایند (Goldberg,2017: 09). بر همین اساس، میزان و ابعاد گمنامی در دیپ‌وب با وب‌سطح قابل قیاس نبوده و در بحث وب‌سطح، گرچه ممکن است اشخاص بخشی از هویت خود را به صورت‌هایی مانند استفاده‌نمودن از یک اسم مستعار مخفی کنند، سطحی از گمنامی که در آن و هویت کامل فرد و موقعیت‌مکانی و دیگر موارد مهم قابل شناسایی در وب‌سطح نیست (Raghavan & Garcia-Molina,2011: 55)).

اولین و قطعی‌ترین علت در توجیه نمودن ضروری‌بودن توجه و واکنش حقوق بین‌الملل به فضاهای‌دارک‌وب و دیپ‌وب، یک واکنش فراسرزمینی مناسب می‌باشد. هیچ کشوری نمی تواند ادعای داشتن کنترل بر فضای‌وب را مطرح کند. فضای‌وب، یک مهم در موضوع حقوق‌بین‌الملل شناخته شده و تنظیم‌گری و قانون‌گذاری در حوزه‌های متعدد فضای‌وب، مانند دیپ‌وب به تنهایی توسط هیچ دولتی میسر نخواهد بود. برخی از دولت‌ها به عللی از قبیل عدم وجود آگاهی، دانش‌فنی و نیروی انسانی متخصص، قادر به واکنش حقوقی کافی و مناسب به فضای‌دیپ‌وب نیستند. این موضوع سبب افزایش یافتن استفاده‌های زیان‌بار و نادرست از این فضا در قلمرو دولت‌ها و ورود آسیب به

شهروندان می‌گردد. همچنین با توجه به ویژگی‌های فراسرزمینی، فضای‌دیپ‌وب 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 مقابله‌کردن با این اعمال، امری دشوار است. برهمین‌اساس، اثرات انفعال برخی از دولت‌ها، در عمل متوجه تمامی دولت‌ها و جامعه جهانی خواهد بود. اقدامات حقوقی بین المللی از یک جهت، کاستی‌های فنی و انسانی این دسته از دولت‌ها برای تقابل و کنترل فضای‌دیپ‌وب 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 فراهم‌شده، توسط فضای‌دیپ‌وب واقع می‌گردد، نه تنها تهدیدی برای جوامع و دول مختلف می باشد، بلکه در ابعادی گسترده‌تر می‌تواند یک تهدید علیه صلح‌وامنیت بین‌المللی نیز به‌شمار آید. به عنوان نمونه، یکی از فعالیت‌های رایج در فضای‌دیپ‌وب که عمدتاً در قالب رمزبازارها(بازارهای‌مجازی) صورت می‌پذیرد، خرید‌وفروش تسلیحات غیرمجاز می‌باشد. این شکل از معاملات، چارچوب‌های کنونی حقوق‌بین‌الملل را در زمینه کنترل تسلیحات را تهدید می‌کند. از جهتی دیگر، یکی از نگرانی‌های جدی در ارتباط با فضای‌دیپ‌وب، استفاده گروه‌های‌تروریستی از ویژگی‌ها و امکانات ناشناس‌ساز این محیط برای مقاصدی، مانند انجام‌تبلیغات، تدارک‌اطلاعات، تأمین‌مالی، جذب‌عضو، دستیافتن به تسلیحات و به تبع آن تسهیل نمودن حملات‌سایبری می‌باشد. از آنجایی که فناوری‌هایی مانند فضای‌دیپ‌وب، سبب تسهیل فعالیت‌های گروه‌های تروریستی می‌شود، توجه حقوقی در ابعاد بین‌المللی به این موضوع برای کنترل‌نمودن خطرهای ناشی از این شکل از سوءاستفاده نمودن از فضای‌دیپ‌وب یک امر ضروری است، چنان‌که در گزارش سال ۲۰۱۷م ارائه‌شده دبیرکل‌سازمان‌ملل در زمینه تهدیدات گروه تروریستی داعش برای امنیت و صلح‌بین‌المللی 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 می باشد که از جمله آن‌ها می‌توان به افزایش استفاده از فضای‌دیپ‌وب و کدگذاری اشاره نمود. برهمین‌اساس، استفاده گروه‌های‌تروریستی از فضای‌دیپ‌وب در راستای گسترش فعالیت‌های‌تروریستی، خود به تهدیدی جدی و مهم برای صلح‌وامنیت بین‌المللی بدل شده است (Denker, 2019: 120).

اکتفانمودن به عملکرد حاکمیت محور کشورها در حوزه فضای‌دیپ‌وب، می‌تواند منتج به بروز یکسری ناهنجاری‌های بین‌المللی و نقض‌شدن چارچوب‌های‌اساسی و بنیادین مستقر و موجود در حقوق‌بین‌الملل شده و مسئولیت‌بین‌المللی آنها را درپی داشته است؛ برای مثال، می‌توان به گرایش برخی از دولت‌ها به استفاده از روش‌های تعقیب شبکه ای برای تقابل با جرم‌های ارتکابی در فضای‌دیپ‌وب اشاره نمود. با توجه به معلوم نبودن هویت و موقعیت مکانی افراد کاربر در فضای‌دیپ‌وب، این خطر وجود دارد که رایانه و شخص موضوع عملیات‌اجرایی این دسته از دولت‌ها، در قلمرو صلاحیتی دولتی دیگر باشد و در نتیجه، با اجرای این عملیات، صلاحیت‌اجرایی و قانونی یک دولت در قلمرو صلاحیتی یک دولت دیگر اعمال می‌گردد که بر طبق چارچوب‌های حقوق‌بین‌الملل حاضر، این اقدامها، اعمال‌نمودن صلاحیت فراسرزمینی به‌شمار آمده و مورد قبول و مشروع نیست. از جهتی دیگر، دولت‌هایی که با مجرمانه محسوب نمودن اصل استفاده از فضای‌دارک‌وب و فضای‌دیپ‌وب، تلاش در ممنوع و محدود نمودن دسترسی افرادکاربر به این فضاها داشته و همچنین در راه نقض هنجارهای قبول شده فضای‌دیپ‌وب، در حال حرکت هستند. واکنش این گروه از دولت‌ها که فضای‌دیپ‌وب را به صورت اجمالی، تهدیدی علیه امنیت ملی خود محسوب می‌کنند، عمدتاً فراتر از حد ضرورت و تناسب بوده و می تواند منتج به تضییع‌شدن حقوق‌بشری آنلاین افراد کاربر گردد. این عوامل سبب‌شده تا فضای دیپ وب توجه حقوق بین‌الملل را به‌خود جلب‌کند، به صورتی که کمیسر اتحادیه‌اروپا در زمینه مهاجرت عنوان نموده که فضای‌دارک‌وب در حال تبدیل‌شدن به یک پناهگاه برای جرایم سازمان یافته می‌باشد و این موضوع، تهدیدی برای جامعه و اقتصاد اروپا محسوب‌شده و تنها در مقیاسی جهانی می‌توان با آن مقابله نمود (Kavallieros& Myttas& Kermitsis& Lissaris, E. Giataganas, & Darra, 2021: 03).

۶,۲. جایگاه کنونی فضای‌دارک‌وب در حقوق‌بین‌الملل

افراد کاربر فضای‌دارک‌وب برای جلوگیری‌نمودن از نظارت و دخالت گسترده دولت‌ها و بازیگران‌خصوصی این عرصه، به وصف گمنام بودن این فناوری و حمایت‌هایی که از آن در پناه حقوق‌بشر امکان دارد، امید بسته‌اند (Faizan& Khan, 2019: 41).

برهمین‌اساس، کارکردهای‌مثبت‌فضای‌دارک‌وب عمدتاً مورد حمایت حقوق‌بین‌الملل‌بشر واقع‌شده‌است. البته در اسناد و رویه‌های حقوق‌بین‌الملل، کماکان ادله‌کافی برای قبول یک حق مستقل با نام حق‌برگمنامی وجود ندارد؛ اما این موضوع به معنای عدم‌امکان حمایت از گمنامی در

نظام‌بین‌الملل‌حقوق‌بشر نیست (غفوری، ۱۳۹۹ :۲۵). ممنوع بودن گمنامی فراهم‌شده در فضای‌دارک‌وب، با حق‌برآزادی‌عقیده‌وبیان و حق‌برحریم‌خصوصی دارای تطابق نبوده و با این وجود، از یک جهت، از کارکردهای‌منفی فضای‌دارک‌وب را نمی توان غافل شد و از جهتی دیگر، هر دو حق‌برحریم‌خصوصی و حق‌برآزادی‌عقیده‌وبیان حقوقی مطلق نبوده و بر طبق مصالح‌اجتماعی می توانند محدود شوند؛ از این رو، حق‌برگمنامی، حقی مطلق نبوده و بر اساس ملاحظات مشروعی که در چارچوب نظام‌بین‌المللی‌حقوق‌بشر قبول گردیده اند، قابلیت محدودشدن دارند. راهکار عاقلانه برای تدوین نمودن قواعدبین‌المللی در حوزه فضای‌دیپ‌وب، اولویت دادن به اصل‌برآزادی استفاده از فضای‌دیپ‌وب برای حمایت‌نمودن از کارکردهای‌مثبت و در نقطه مقابل، تحدیدوتعدیل‌نمودن آن برطبق واقعیت‌های موجود و ملاحظات‌مشروع پذیرفته‌شده در حقوق‌بین‌الملل در زمینه کنترل‌نمودن کارکردهای منفی این فضا می‌باشد. اکنون می‌توان ادعا نمود که فضای دیپ وب، به عنوان یک موضوع دارای اهمیت و وصف بین‌المللی، در ابعاد بین‌المللی با واکنش حقوقی خاص و مناسب و فراگیر، همراه نبوده است (Ertan& Floyd& Pernik ,2019: 16).

فضای‌دیپ‌وب، بخشی مهم و ناپیدا از فضای‌وب و جدیدتر و نشناخته‌تر از آن می‌باشد؛ اکنون در حالی سخن از واکنش‌های حقوقی در ابعاد بین‌المللی بیان می‌شود که باگذشته ۳۰ سال از رواج فراگیر اینترنت، کماکان عدم وجود یک نظام حقوقی جامع و منسجم در ابعاد بین‌المللی برای فضای‌اینترنت، احساس می‌گردد. تلاش‌هایی که تاکنون برای نظام‌مند نمودن فضای‌اینترنت در ابعاد بین‌المللی انجام شده است، موفقیت چندانی در ایجادکردن یک نظم‌حقوقی‌جامع که پاسخگوی ویژگی‌های‌ذاتی فضای‌وب و چالش‌های بین‌المللی آن باشد، نداشته‌اند. بخشی قابل توجه از انفعال حقوق‌بین‌الملل در مقابل فضای‌دیپ‌وب، ریشه در علت ناکامی ایجاد یک چارچوب‌حقوقی‌بین‌المللی برای فضای‌اینترنت به صورت کلی دارد. دلیل اصلی در واکنش ناکافی بوده نظام‌حقوق‌بین‌الملل نسبت به فضای‌وب و سختی محقق‌شدن اجماع بین‌المللی، شکافی‌گسترده در مواضع و دیدگاه‌های‌دولت‌ها در زمینه مسائل چالشی حوزه فضای‌وب، مانند حق‌برحریم‌خصوصی، حق‌برآزادی‌بیان، حق‌برگردش‌آزاداطلاعات و... می باشد. به عنوان نمونه، اکثر کشورهای‌اروپایی در مواجهه با محتوای‌زیان‌بار در فضای‌آنلاین، بر حذف‌شدن آن‌ها تأکید دارند، در حالی که کشورایالات‌متحده‌آمریکا، بر اساس اصلاحیه نخست قانون اساسی خود، حق‌برآزادی‌بیان را نسبت به حفاظت از جامعه و افرادشهروند در مقابل محتوای‌زیان‌بار، یک اولویت محسوب نموده است. همچنین در مورد تقابل احتمالی حق‌برآزادی‌بیان و حق‌برحریم‌خصوصی اتحادیه‌اروپا، حریم‌خصوصی شهروندان را واجد اولویت و کشور ایالات‌متحده‌آمریکا، حق‌برآزادی‌بیان را مقدم محسوب نموده است. برخی دیگر از دولت‌های قدرتمند، مانند جمهوری‌خلق‌چین و روسیه نیز در تقابل با فضای‌دیپ‌وب بیش از هر چیز دیگر، بر موضوع امنیت‌ملی توجه نموده و موضع خود را در مقابل این قبیل تحولات را بر مبنای این ملاحظه تنظیم می‌نمایند. نبود یک واکنش حقوقی مناسب و خاص، به فضای‌دیپ‌وب در ابعاد بین‌المللی، اثراتی مانند امنیت و مصونیت افرادکاربرهنجارشکن، محروم‌شدن افرادکاربرقانونمند از حقوق مشروع خود در برخی از دولت‌ها و قرارگرفتن دولت‌ها در معرض مسئولیت‌بین‌المللی را در پی دارد. یکسان‌سازی مقررات‌ملی و تدوین‌نمودن سندهای‌دوجانبه و چندجانبه در زمینه همکاری‌های‌اجرایی و قضایی در زمینه جرایمی که در فضای‌دیپ‌وب صورت می‌گیرد، می‌تواند سبب کاستیهایی در راهکارهای صرفاً ملی و نواقصات ناشی از نبود قواعد بین‌المللی در این حوزه را در کوتاه‌مدت تا حد زیادی جبران نماید (Breckheimer, 2010:).

نتیجه‌گیری

فضای‌اینترنت را می‌توان به‌طورکلی 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. میزان۹۶٪ فضای وب به علت پنهان بودن جزء فضای‌دیپ‌وب محسوب می‌شود، فضای‌اینترنت همانند یک کوه یخ می باشد 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 فضای‌دیپ‌وب و شناسایی تهدیدات‌سایبری مورد استفاده قرار گیرد. از آنجایی که فضای‌اینترنت به سرعت در حال تکامل بوده و محمدود کردن دسترسی به فضای‌دیپ‌وب تقریباً امری غیرممکن می‌باشد، نیاز به توسعه‌مکانیزم و ابزارهای‌استاندارد برای نظارت بر این فضا احساس می‌شود. فضای فضای‌دیپ‌وب، به دلیل وجود ویژگی‌هایی، مانند ناشناس‌بودن، در تمایز بین کاربران‌مخرب و معتبر ناتوان بوده و مقامات‌اجرایی بایستی با اجرای‌تکنیک‌هایی که از حریم‌خصوصی‌کاربران و همچنین دستگیری مجرمان مراقبت می‌کند، با این چالش مقابله کنند؛ این کار را می‌توان با بررسی سایت‌های کلاهبردار به جای کاربران‌متقلب به صورت موثر انجام داد. گشت‌وگذار در وب‌سایتهای موجود در فضای‌دارک‌وب، عملی اشتباه یا غیرقانونی محسوب نمی‌گردد، اما درگیر شدن در فعالیت‌های‌غیرقانونی موجود در فضای‌دارک‌وب، عملی اشتباه است. مقابله و برخورد با جرایم موجود در فضای‌دارک‌وب و فضای‌دیپ‌وب، به علت ناشناس بودن گردانندگان سایت‌های موجود در این فضا، امری محال و سخت بوده که در حقوق‌بین‌الملل با توجه به گسترده بودن دامنه این جرایم، وجود همکاریهای‌بین‌المللی در این زمینه احساس می‌شود. در حقوق‌بین‌الملل، مقابله با جرایم موجود در فضای‌دارک‌وب و فضای‌دیپ‌وب، که در یک نقطه از دنیا متمرکز نبوده و در هر کشور، انجام این جرایم مقدور است، نیازمند قوانینی جامع و همچنین یک سازمان‌تخصصی در این زمینه می‌باشد تا با وجود یک استقلال‌قضایی‌بین‌المللی 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 فضای‌دیپ‌وب ناتوان هستند، به این علت که ردیابی مجرمین، کاری بسیار سخت بوده و در فرضی که مجرمین ردیابی‌شده و در قلمرو حاکمیتی یک کشور دیگر باشند، در اکثر موارد، کشورها برای دستگیری و استردادمجرمین با همدیگر همکاری نمی‌کنند که این موضوع سبب‌شده تا فضای‌دیپ‌وب، 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 امریکا، 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 امریکا»، 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 Grides”, 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). Resmî 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/eaaa015. ISSN 0967-0769.
19. Fischer, Susanna Fredrick. (2001). “Saving Rosencrantz & Guildentern 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.