Women's Studies, **Institute for Humanities and Cultural Studies (IHCS)**
Quarterly Journal, Vol. 12, No. 2, Summer 2021, 257-290

Investigating Cyber Violence Against Women and the Umbrella of National and International Legislation

Zahra Norouzi*

AbdolHamid Afrakhteh**

Abstract

Women are one of the main victims of violence in the world. With the development of societies and the globalization of communication, acts of violence against women have changed and manifested in various forms. Violence in cyberspace is one of the emerging forms of this social harm. The unique features of cyberspace, such as universality, lack of territorial boundaries, anonymity of users, and ease of identification, have created the conditions for norm-breakers, like the physical world, to pose threats to individuals. One of the main and most dangerous threats in this space is the abusive actions that target women and girls in cyberspace. Violence against women in cyberspace has consequences that endanger their physical and mental health, reinforce gender discrimination, and violate women-related human rights standards. The right to freedom of expression and the free access to information and the right to privacy and the protection of privacy are human rights standards applicable to the protection of women against cyber-violence. The present article, through a descriptive-analytical method and by analyzing the legal sources in this field, tries to reflect on cyber violence against women within the framework of the rules and standards of national and international law. The basic premise of this article is based on the fact that the simultaneous application of national and international regulations and policies, as well as the use of a mixed and self-regulatory approach by exploiting the unique features of cyberspace to reduce cyber violence against women.

Keywords: Cyberspace, Cybercrime, Cyber Violence, Women's Rights, National Law, International Law

* Instructor, Department of Arabic Language and Literature, Payame Noor University, z.norouzi1356@gmail.com

** Instructor, Department of Social Sciences (Political Science), Payame Noor University (Corresponding Author), abdolhamidafrakhteh@gmail.com

Date received: 12/07/2020, Date of acceptance: 22/08/2020

پژوهش‌نامهٔ زنان، پژوهشگاه علوم انسانی و مطالعات فرهنگی
فصل‌نامهٔ علمی (مقالهٔ علمی ـ پژوهشی)، سال دوازدهم، شمارهٔ دوم، تابستان ۱۴۰۰، ۲۵۹ – ۲۹۰

واکاوی خشونت سایبری زنان و چتر حمایت قانون‌گذاری ملی و بین‌المللی

زهرا نوروزی*

عبدالحمید افراخته**

چکیده

یکی از اصلی‌ترین قربانیان خشونت در جهان زنان هستند. با پیشرفت جوامع و جهانی‌شدن ارتباطات اعمال خشونت علیه زنان تغییر شکل داده و به اشکال مختلف بروز پیدا می‌کند. خشونت در فضای سایبری یکی از اشکال نوظهور این آسیب اجتماعی است. ویژگی‌های منحصربه‌فرد فضای سایبر ازجمله جهان‌شمولی، نبود مرزهای سرزمینی، گمنامی کاربران و سهولت در جعل هویت، شرایطی را ایجاد کرده تا هنجارشکنان همانند جهان فیزیکی، تهدیداتی را متوجه اشخاص کنند. یکی از اصلی‌ترین و پرمخاطره‌ترین تهدیدات در این فضا، اقدامات متخلفانه‌ای است که زنان و دختران را در فضای سایبر نشانه می‌گیرند. ایراد خشونت علیه زنان در فضای سایبری پیامدهایی دارد که سلامت جسمانی و روانی آنان را به مخاطره می‌اندازد، موجب تقویت تبعیض جنسیتی می‌شود و ناقض موازین حقوق بشری مرتبط با بانوان است. حق بر آزادی بیان و دسترسی آزاد به اطلاعات و حق بر خلوت و حمایت از حریم خصوصی از موازین حقوق بشری قابل‌اعمال در جهت صیانت از زنان در برابر خشونت سایبری است. نوشتار حاضر، از رهگذر شیوه توصیفی – تحلیلی و با تحلیل منابع حقوقی این حوزه می‌کوشد به تأمل درباره خشونت سایبری علیه زنان در چارچوب قواعد و موازین حقوق ملی و بین المللی دست یابد. فرض اساسی این مقاله بر این مبنا استوار است که اعمال هم‌زمان مقررات و سیاست‌های مدون ملی و بین‌المللی و در کنار آن، توسل به رویکرد

* مربی گروه زبان و ادبیات عرب، دانشگاه پیام نور، z.norouzi1356@gmail.com

** مربی گروه علوم اجتماعی (علوم سیاسی)، دانشگاه پیام نور (نویسندهٔ مسئول)، abdolhamidafrakhteh@gmail.com

تاریخ دریافت: ۱۳۹۹/۰۶/۲۲، تاریخ پذیرش: ۱۳۹۹/۱۰/۰۱

مختلط و خود انتظامی با بهره‌برداری از ویژگی‌های انحصاری فضای سایبر در کاهش خشونت سایبری علیه زنان راهگشا خواهد بود.

کلیدواژه‌ها: فضای سایبری، جرائم سایبری، خشونت سایبری، حقوق زنان، قوانین ملی، قوانین بین‌المللی

۱. مقدمه

فضای بی‌مرز سایبر، جهانی موازی با جهان فیزیکی را به وجود آورده است که درواقع کنترل و اداره حقوقی آن از حیطه اعمال قدرت یک حاکمیت برنمی‌آید. بنابراین، برای حاکمیت بر این فضا و مقابله با جرائم روزافزون و پیچیده ارتکابی در آن همکاری و معاضدت جوامع ملی و بین‌المللی برای قاعده‌مندی نیاز است، به‌گونه‌ای که هیچ مجرمی بدون مجازات نماند و این مهم به دست نمی‌آید مگر با تدوین قوانین و مقررات ملی و بین‌المللی هماهنگ و در بعضی مواقع متحدالشکل، زیرا جرائم ارتکابی در این فضا مرزهای جغرافیایی و سنتی را پشت سر می‌گذارند و به سبب ویژگی‌هایی که دارند، می‌توان برخی ازاین‌گونه جرائم را در زمره آن دسته جرائمی به شمار آورد که برای مقابله با آنها اعمال صلاحیت جهانی ضرورت دارد. با وجود فعالیت‌های گوناگون سازمان‌های بین‌المللی جهت ارائه مقررات پیشنهادی در جهت یکسان‌سازی و هماهنگ‌سازی مقابله با جرائم در فضای مجازی، هنوز هم جامعه جهانی به هدف خود دست نیافته است، بنابراین، وجود مقررات مدونی که کاستی‌های سایر مقررات را برطرف کند، لازم‌الاجرا باشد و بتواند مقبولیت جهانی را به دست آورد، ضروری است. خشونت علیه زنان، از آسیب‌های مهم اجتماعی است که با وجود پیشرفت‌های فرهنگی و فکری، در بیشتر کشورها، حتی کشورهای توسعه‌یافته و در تمامی گروه‌های اجتماعی و طبقاتی دیده می‌شود (یزدخواستی و شیری، ۱۳۸۷). خشونت را افراد در محیط‌های متنوعی تجربه می‌کنند، به‌گونه‌ای که هم در محیط‌های آموزشی (بازرگان و همکاران،۱۳۸۲؛ ویبل،۲۰۰٤) و هم در محیط خانواده (چلبی، ۱۳۸۱؛ جوادیان،۱۳۸۱) به‌کرات دیده شده است. همچنین فراوانی این آسیب در بین زنان بسیار بیشتر از مردان است (مارابی،۱۳۸٤؛دهقانی،۱۳۸۱؛ امیدبخش و بختیاری،.۱۳۸۱). با افزایش دسترسی افراد به فضای سایبری، خشونت نه‌تنها در جهان واقعی بلکه در جهان مجازی نیز افزایش یافته و در مقابل از دامنه روابط در جهان واقعی کاسته می‌شود (حسین‌زاده و دیگران، ۱۳۹۱). ارتباطات و تعاملات در فضای اینترنتی بر همه اقشار

ازجمله زنان تأثیر داشته است. (Cyber Vioence gender report,۲۰۱٤). گزارش سازمان ملل در مورد خشونت سایبری – جنسیت، خشونت سایبری را چنین تعریف می کند؛ «هر نوشته و رفتار تحقیر آمیز در پیغام‌های کاربران، اجبار به عمل جنسی در فضای اینترنت، تهدید و استفاده از الفاظ جنسی و هم چنین تهدید کلامی و رفتارهای خشن، خشونت علیه زنان محسوب می‌شود و خشونت و زورگویی علیه زنان در فضای سایبری را یکی از علت‌هایی می‌داند که چرخه خشونت علیه زنان را در عالم واقع تندتر می‌چرخاند. پیترسون و دنسلی (Densley & Petetson,۲۰۱۷) از نظریه‌پردازان اخیر که به بررسی انواع خشونت در فضای سایبر پرداخته‌اند انواع خشونت را شامل؛ تهدید (Threaten) افراد به خصوص تهدید زنان و دختران جوان در این حوزه می‌دانند همچنین ایجاد شرمساری (Embarrass) برای افراد از طریق نوشتن و پیام گذاشتن زیر عکس و یا پست‌های افراد (Comment on someone photo or post) (ang,2015)، رفتارهای فریبکارانه آنلاین (Online Trolling) با اهداف نامعلوم (Trapnell & Buckele,۲۰۱٤)، انتقام از طریق تصاویر پورنو (Revenage Porn) (Franklin,2014)، زورگیری سایبری (Cyber Stalking) (Beech et, al, 2018) و خشونت جنسی در از دیگر انواع خشونت سایبری می‌باشد. درباره ورود زنان در فضای سایبر دو دیدگاه وجود دارد؛ دیدگاه نخست نشان می‌دهد که زنان از فضای سایبر سود می‌برند و تکنولوژی زنان را قدرتمند می‌کند دیدگاه دوم معتقد است که این تکنولوژی منجر به سوءاستفاده از زنان شده است؛ درواقع زنان دچار آسیب اجتماعی و احساسی در استفاده از تکنولوژی می‌شوند (پیرس،۲۰۱۳). همچنین با ورود زنان به فضای سایبری اصطلاحی به نام «سایبرفمینیسم» «feminism Cyber» شکل گرفته که حاکی از آن است که ذهنیت زنانه می‌تواند منطق فناوری را دگرگون کرده و خسارات ناشی از آن را کم کند، آنها معتقد بودند باید از فضای سایبری برای همه‌گیر کردن گفتگو در مورد اموری مانند هویت، جنسیت و قدرت استفاده شود (شاه قاسمی، ۱۳۸۵). علاوه بر شکل‌گیری ذهنیت زنانه در فضای سایبری، آسیب‌ها و خشونت‌هایی علیه زنان شکل گرفته شده است. در گزارش کمیسیون «برادباند» «Broadband»، حدود یک‌سوم زنان به‌صورت آنلاین در معرض برخی از اشکال خشونت سایبری هستند، مطابق این گزارش، برخی اشکال رایج خشونت سایبری علیه زنان و دختران عبارت‌اند از: اذیت و آزار آنلاین، هتک حیثیت، طراحی صدمه جسمانی، تهاجم جنسی، قتل و ترغیب به خودکشی .-Driven to Cyber) (Violence-gender reportsuicide,2013. دانشگاه مریلند آمریکا نیز در پژوهشی دانشگاهی در

سال (۲۰۱٤) عنوان کرد که کاربران زن به‌طور متوسط ۲۵ برابر بیشتر از کاربران مرد با پیغام‌های تهدیدگر، فحاشی، پیغام‌هایی با کلمات رکیک و جنسیت زده و خشونت کلامی مواجه می‌شوند و قربانیان این آزار نیز بیشتر در زنان بین ۱۸ تا ۳۰ ساله بوده‌اند و در بسیاری از کشورها، زنان به دلیل ترس از عواقب اجتماعی، مایل به گزارش‌دهی ارتکاب خشونت سایبری علیه خود نیستند(رقم سیاه جرم) (Cyber Vioence-gender report,2013) زنان به علت ترس از آبرو و حیثیت درباره این تجربه ناخوشایند حرف نمی‌زنند و فضا را هم برای مردانی که دست به این‌گونه رفتارها می‌زنند، امن‌تر کرده‌اند. بنابراین خشونت نه‌تنها در جهان واقعی بلکه در جهان مجازی نیز در حال شکل‌گیری است، در حال حاضر خشونت در فضای سایبری علیه زنان و دختران به موضوعی مهم تبدیل شده است که میلیون‌ها نفر از زنان و دختران در سراسر جهان به دلیل نوع «جنسیت» خود در معرض خشونت عمدی در فضای سایبر قرار دارند. خشونت علیه زنان و دختران هیچ مرز، نژاد و فرهنگ خاصی را شامل نمی‌شود. در حال حاضر جوامع انسانی و به ویژه زنان در سراسر جهان از جمله ایران با این آسیب به‌عنوان مشکلی اساسی که دارای پیامدهای جدی می‌باشد مواجه هستند. بدیهی است که قلمروی نقش‌آفرینی دولت برای پیشگیری و مقابله، و نیز کارایی ضمانت اجراهای دولتی مانند جرم انگاری و مجازات اقدامات خشونت‌بار در فضای سایبری، با توجه به ماهیت آن، با محدودیت‌هایی مواجه است؛ چنانچه آمار بالای ارتکاب خشونت سایبری در کشورهای اروپایی علیرغم پیشرفت زیاد تکنولوژی در جوامع مزبور دلالت بر این واقعیت می‌کند؛ لذا در کنار ضمانت اجراهای قانونی و لزوم قطعیت پیگرد قضایی، تعقیب، محاکمه و مجازات مرتکبین خشونت سایبری علیه افراد ازجمله زنان و دختران، توجه به ایجاد مکانیسم‌های درونی بازدارنده یا تدابیر «خودکنترلی»، ضروری به نظر می‌رسد که قطعاً تقویت پایبندی افراد جامعه به اصول و ارزش‌های اخلاقی و آموزه‌های مذهبی ازجمله مهم‌ترین موارد آن است و البته این نگاه، حلقه مفقوده‌ای است که در رویکرد نهادهای بین‌المللی ازجمله سازمان ملل متحد مغفول مانده است. (زندی، ۱۳۸۹). ازاین‌رو، هدف از پژوهش حاضر، با روش توصیفی- تحلیلی و با بهره‌مندی کتب مربوط به فضا و جرایم سایبری و رایانه‌ای و اسناد حقوقی کنوانسیون‌های مختلف و دیگر قوانین و مقررات بین‌المللی بررسی خشونت علیه زنان در فضای سایبر و شناسایی چترهای حمایتی و خلأهای حمایتی قوانین ملی و بین‌المللی در این حوزه است.

۲. پیشینهٔ پژوهش

پژوهش‌های صورت گرفته در ایران در زمینه علت شناسی خشونت و بزه دیدگی زنان در فضای سایبری، بسیار اندک و ناکافی است. آنچه ضرورت تحقیق و اکتفا نکردن به ادبیات پژوهشیِ ترجمه‌ای در این زمینه را توجیه می‌کند، اول، پویایی جرم سایبری است که روزآمد بودن پژوهش‌ها را می‌طلبد و مهم‌تر اینکه، پژوهش‌های ترجمه‌ای و اقتباسی به جهت اختلافات اساسی با مبانی فرهنگی-اجتماعی کشور ما کارآمدی لازم را ندارند؛ زیرا خشونت و بزه دیدگی سایبری زنان، در اکثر جوامع غربی، قبح کمتری نسبت به بزه دیدگی در جامعه ایران اسلامی دارد. به‌این‌ترتیب در حوزه موضوع حاضر، پژوهش‌های اندکی را می‌توان به‌عنوان پیشینه مرتبط معرفی نمود. در یک پژوهش (Broadhurst & Jayawardena, 2001) با عنوان «شبکه‌های اجتماعی آنلاین و شاهدبازی»، این نتیجه به دست آمد که قوی‌ترین متغیر در میزان خشونت و بزه دیدگی کاربران شبکه‌های اجتماعی، نوع عکس یا ایمیل آنها است. در یک مطالعه میدانی (Shick Choi, 2011) با عنوان «فعالیت‌های روزمره سایبری؛ بررسی تجربی سبک زندگی اینترنتی» موضوع بزه دیدگی کاربران، فارغ از جنسیت ایشان، در دستور کار قرار گرفت. نتایج این مطالعه به‌این‌ترتیب است که اولاً، افرادی که سبک زندگی بر خط رایانه محور خود را جدی نمی‌گیرند، به‌احتمال بیشتری قربانی جرائم سایبری خواهند بود. ثانیاً، نتایج نشان می‌دهد که برخی الگوهای سبک زندگی، به‌طور مستقیم، با قربانی شدن در فضای سایبری ارتباط دارند ثالثاً نتایج این تحقیق نشان می‌دهد که وجود امنیت رایانه‌ای، مهم‌ترین عنصر حفاظت کننده از فرد در مقابل جرائم سایبری است. همین نتایج توسط مک کود (McQuade, 2006) ارائه شد و بیان داشت که «نظریه فعالیت‌های روزمره، نتایج مهمی برای شناخت جرائم رایانه و سایر ابزارهای فناوری اطلاعات و سیستم‌های اطلاعاتی و پیشگیری از آنها دارد». دربندی فراهانی، (Darbandi farahani,2012) در پژوهشی با عنوان «رویکرد بزه دیده شناسی به جرائم سایبری»، برخی نظریات بزه دیدگی را با جرائم سایبری مورد کنکاش قرار داده است. تحقیق مذکور، بدون راستی آزمایی یافته‌های جرم‌شناسی درصدد تعمیم آنها به جرائم سایبری است. این تحقیق، مسائل مختلفی را در بزه دیده شدن یک کاربر دخیل می‌داند و بخشی از علل را درگرو عملکرد و تعاملات کاربر معرفی می‌نماید. ابوذری، (Aboozari, 2016)، در پژوهشی با عنوان جرم‌شناسی جرائم سایبری، به علت شناسی جرائم سایبری از رهگذر چند نظریه جرم‌شناختی پرداخته است. جملگی این نظریه‌ها، از زوایای گوناگون درصدد تحلیل

علت‌شناختی جرم سایبری هستند برخی از این نظریه‌ها از منظر زیستی، روانی، اخلاقی و اجتماعی، موضوع را پی گرفته‌اند. در این پژوهش، ذیل مبحث نظریه‌های عقلانی، مرور مختصری به نظریه‌های بزه دیدگی شده است؛ لکن این پژوهش هم علاوه بر اختصار، به سنجش رهیافت‌های جرم‌شناسی با بزه‌دیدگی کاربران ایرانی نپرداخته است. زررخ، (Zarrokh,2010) در یک پژوهش کلی با عنوان «بزه دیده شناسی سایبری»، با طرح دو نظریه بزه دیدگی، درصدد تبیین علت شناختی بزه دیدگی سایبری و نقش بزه دیده در رخداد بزه سایبری برآمده است. وی غالب بزه دیده‌های سایبری را به‌طور مستقیم یا غیرمستقیم، دخیل در بزه دیده شدن دانسته است. این پژوهش که مقدم بر دیگر تحقیقات مرتبط است و غالباً به‌عنوان یکی از منابع این مدخل در پژوهش‌های آتی مورداستفاده قرار گرفته، علاوه بر آنکه روزآمد نیست، به اثبات آماری مطالب مطرح شده نپرداخته و موضوع را به‌صورت عام و کلی در فضای مجازی دنبال کرده و جنسیت خاصی را مورد تدقیق قرار نداده است. به‌غیراز موارد پیش‌گفته، پژوهشی که در همین راستا موضوع را دنبال کرده باشد، دیده نشد؛ لکن پژوهش‌های دیگری هم در خصوص موضوعات مرتبط و نزدیک به موضوع این پژوهش وجود دارند که برای رعایت اختصار، از پرداختن به آنها صرف‌نظر می‌شود.

بنابراین نتایج پژوهش‌های داخلی در این حوزه نشان می‌دهد عدم آگاهی زنان، پایین بودن خودکنترلی، عدم اطلاع‌رسانی و آموزش و عدم کنترل در فضای سایبر از علل بزه دیدگی زنان در فضای سایبر است و در حوزه علوم اجتماعی تأکید بر تهدیدات فضای سایبری و آزار و اذیت‌ها در این فضا شده بود. در خارج از کشور پژوهش‌هایی در این حوزه صورت گرفته است که نتایج آنها نشان می‌دهد؛ زنان همواره اشکالی از خشونت‌های آنلاین را تجربه کرده‌اند و خشونت‌های سایبری علیه زنان شامل توهین‌های سایبری، آزارجنسی، پورنوگرافی، دریافت ایمیل از افراد ناشناس و وادار کردن به خودکشی می‌باشد که در بسیاری از کشورها به دلیل ترس از عواقب اجتماعی مایل به گزارش دهی ارتکاب خشونت سایبری علیه خود نیستند که باعث شکل‌گیری رقم سیاه جرم می‌شود.

۳. مبانی نظری

۱.۳ فضای سایبر

فضای سایبر یا فضای مجازی(شبکه‌های مبتنی بر وب و وب‌محور) که جرائم موردنظر این پژوهش در آن ارتکاب می‌یابد و امروزه این جرائم در شاخه نسبتاً مستقل و در حال

شکل‌گیری تحت عنوان حقوق سایبر یا نظام حقوقی فضای مجازی مطالعه می‌شود، به دنیایی گفته می‌شود که با استفاده از فناوری اطلاعات تکنولوژیهای نوین ارتباطات و علوم رایانه، اینترنت و امکانات مجازی همانند دنیای واقعی در کیفیت زندگی افراد جامعه تأثیرگذار است. فضای مجازی در این معنا «به مجموعه‌هایی از ارتباطات درونی انسان‌ها از طریق کامپیوتر و وسایل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می‌شود. در این فضا مرز بین دنیای درون و بیرون تقریباً ناپدید می‌شود و دیگر زمان معنایی ندارد. درواقع می‌توان گفت فضای مجازی گستره‌ای از ذهن است که می‌تواند تمامی اشکال زندگی واقعی را بسط و معنا دهد» (پورنقدی،۱۱:۱۳۹۳). بنابراین، جرائم موضوع این پژوهش در فضای سایبر یا فضای مجازی(شبکه‌های مبتنی بر وب و وب‌محور) و بیشتر با ماهیت ملی و بین‌المللی موضوعیت دارد و مواردی مانند دسترسی غیرمجاز، شنود غیرقانونی، اعمال علیه محرمانگی، تولید و توزیع برنامه‌های رایانه‌ای ارتکاب جرم، تمامیت و در دسترس بودن سیستم‌های رایانه‌ای، شبکه‌ها و داده‌های رایانه‌ای، انتشار مطالب نژادی و تنفرانگیز، فحشا، هرزه‌نگاری، ایجاد شرمساری و هتک‌حرمت، نقض حریم خصوصی و سوءاستفاده از تصاویر شخصی افراد، حملات اینترنتی، افشای اسرار تجاری، جاسوسی، سرقت و کلاه‌برداری اینترنتی، نقض حقوق مالکیت معنوی در فضای مجازی و... را دربرمی‌گیرد.

۲.۳ خشونت سایبری

خشونت حالتی از رفتار است که با استفاده از زور فیزیکی و یا غیر فیزیکی فرد خشن خواسته خود را به دیگران تحمیل می‌کند. خشونت ممکن است در اثر خشم اتفاق افتد. خشونت ازنظر لغوی به معنای خشکی، تندی و سختی است(دهخدا،۱۳۷۳). در سال ۱۹۹۳ بیانیه حذف خشونت علیه زنان در سازمان ملل این تعریف را برای خشونت علیه زنان بیان کرد؛ «به هر نوع اقدام خشونت‌آمیز که به آسیب بدنی، جنسی یا روانی در زنان منجر شود (یا احتمال بروز آن زیاد شود) برای زنان رنج‌آور بوده یا به محرومیت اجباری از آزادی فردی یا اجتماعی منجر شود». خشونت علیه زنان اصطلاحی تخصصی است که برای توصیف کلی کارهای خشونت‌آمیز علیه زنان به کار می‌رود. مجمع عمومی سازمان ملل متحد خشونت علیه زنان را «هرگونه عمل خشونت‌آمیز بر پایه جنسیت که بتواند منجربه آسیب فیزیکی؛ جنسی یا روانی زنان بشود» تعریف کرده است که شامل تهدید به

این اعمال و اجبار یا سلب مستبدانه آزادی (چه در اجتماع و چه در زندگی شخصی) می‌شود» (زندی، ۱۳۸۹).

خشونت سایبری بروز آسیب‌های روانی و یا تحریک دیگران برای انجام خشونت‌های فیزیکی علیه دیگران که نتیجه نقض قوانین حقوقی حفاظت فردی است. خشونت مدنظر در این پژوهش عملی آسیب‌زننده در فضای مجازی است که با اعمال فیزیکی صدمات فیزیکی و روانی را به قربانی وارد می‌سازد نکته‌ای که باید به آن توجه داشت این است که در این نوع از خشونت اصلی‌ترین فاکتور در تعریف آن فضایی است که در آن فرد مورد هجمه قرار می‌گیرد (همت‌پور و دیگران،۱۳۹٦). در تعاریف ارائه‌شده بالا تمامی صدمات در فضای واقعی به قربانی وارد می‌شود ولی در این تعریف مبدأ ورود صدمه فضای مجازی است.

۳.۳ جرائم سایبری

در اواسط دهه **۱۹۹۰** میلادی، نسل جدیدی از فناوری رایانه (که درواقع باید آن را ماحصل فناوری ارتباطی و اطلاعاتی نامید) تجلی پیدا کرد. رایانه‌ها در یک روند تکاملی بسیار سریع، به سیستم‌های رایانه‌ای متشکل از چندین وسیله رایانه‌ای که قابلیت ارتباط بین سیستم‌ها و شبکه‌های بین‌المللی را داشتند، تبدیل شدند. رایانه‌ها به‌وسیله شبکه‌ها، روزبه‌روز ارتباط گسترده‌تری پیداکرده و از طریق مخابرات و ماهواره، هرگونه دریافت، انتقال، صدور علائم، تصاویر، صداها، نوشته‌ها و نشانه‌ها را مقدور ساخته‌اند. لذا با توجه به این قابلیت شگرف فناوری ارتباطی، تحول عظیم در دنیای ارتباطات و عصر فناوری اطلاعات به وجود آمد که از مشخصه‌های این فناوری جدید، شکل‌گیری ارتباط بین افراد ملل دنیا در یک فضای مجازی و در محیط شبکه‌های بین‌المللی است که به‌نوبه خود، سهم بسزایی در تغییر شکل و کارکرد روابط اجتماعی دارد و به همان نسبت در تغییر الگوی ماهیت جرائم کلاسیک نیز تحول ایجاد کرده است(زرگر،۱۳۸۵:۲۰٦). امروزه چهار اصطلاح جرایم رایانه‌ای، کامپیوتری، اینترنتی و سایبری به کار می روند، ولی عینا به یک معنی نیستند. رایانه و کامپیوتر معادل همدیگرهستند. اولی فارسی و دومی انگلیسی است و این دو متفاوت از اینترنت و سایبراند. جرایم اخیر فقط در بستر شبکه جهانی اینترنت (اتصال رایانه‌ها به هم) قابل تحقق‌اند. اما دسته اول لزومی به اتصال به شبکه جهانی اینترنت ندارند. مثالی می زنیم. تولید یا انتشار یا توزیع نرم افزارهایی که صرفا برای ارتکاب

جرم کاربرد دارند می توانند به صورت آفلاین (بدون اتصال بـه اینترنـت، و در واقـع بـدون اتصال رایانه‌ها به هم) تولید یا انتشار یا توزیع شوند (ماده ۷۵۳ قانون مجازات اسـلامی)، امـا عدم پالایش(فیلتر) محتوی مجرمانه از ناحیه ارایه دهنده خدمات دسترسـی و میزبـانی فقـط در بستر اینترنت مطرح است (مواد ۷٤۹ و ۷۵۱ قانون مجازات اسـلامی) یـک نکتـه ظریـف دیگر، در تفاوت بین اینترنت و سایبر است. اینترنت، فضای سایبر (همان فضـای مجـازی در زبان فارسی) را به وجود می آورد به عبارتی دیگـر، سـایبر یعنـی فضـای ناشـی از اینترنـت (اتصال رایانه های مختلف به هم) نه سامانه‌های رایانـه‌ای و پروتکـل‌هـا و دیگـر تجهیـزات سخت افزاری و نرم افزاری که اینترنت را به وجود می‌آورند؛ سایبر محصول اینترنـت اسـت و اینترنت محصول ارتباط رایانه‌ها بـه هـم بـا تجیهـزات‌رایانـه‌ای؛ و جـرایم سـایبری یعنـی جرایمی که در فضای اینترنت ارتکاب می‌یابند. از خصوصیات متمایزکننده این نـوع جـرائم با جرائم پیشین، عدم وابستگی ارتکاب جرم به حضور فیزیکی مجرم در محـل بـروز نتـایج جرم، زمان ارتکاب، مکان ارتکاب، بزه دیده و شکل ارتکاب است. به این نوع جرائم کـه در این نوع فضا (مجازی) وقوع پیدا می‌کند؛ جرائم سایبری گفتـه مـی‌شـود. در فضـای سـایبر برای جستجو و کشف جرائم، مشکلات پیچیده‌تر می‌شود. به‌طـور مثـال در دنیـای واقعـی، سرقت از بانک کاملاً مشخص است؛ زیـرا بعـد از سـرقت در خزانـه بانـک، پـولی موجـود نیست. ولی در فناوری رایانه‌ای، خزانه می‌تواند بدون هیچ علامتی خـالی شـود. (بیونـد، ۲۸: ۱۹۹۷ به نقل از باستانی، ۱۳۸۳). در تعریفی دیگر از جرم سایبری و یـک تعریـف عمـومی، جرم سایبری را به‌عنوان هرگونه فعالیتی که در آن رایانه‌ها یا شبکه‌ها، ابزار، هدف یـا مکـانی برای فعالیت تبهکاری هستند، توصیف می‌کند. پیش‌نویس کنوانسیون بین‌المللـی بـه تقویـت حفاظت در برابر جرائم سایبری و تروریسم اشاره دارد. جرائم سایبری اعمـالی در رابطـه بـا سیستم‌های سایبری است. برخی تعریف‌ها، در تلاش برای در نظر گرفتن اهداف و نیـت‌هـا هستند و جرائم سایبری را دقیق‌تر تعریـف مـی‌کننـد. امـا بایـد توجـه داشـت کـه در ابعـاد بین‌الملل و داخلی، تعریف دقیق و شفافی از جرم سایبری صـورت نگرفتـه اسـت. بنـابراین براساس داشته‌های موجود و تعریف جرم در نگاه حقوقی جمهوری اسلامی ایران که اذعـان می‌دارد: جرم، هر فعل یا ترک فعلی است که در قانون برای آن مجازات تعیـین شـده باشـد، بنابراین جرم سایبری را می‌توان تلویحاً چنین تعریف کرد که: هر فعل یا تـرک فعلـی اسـت که در فضای سایبر به وقوع می‌پیوندد و برابر قـانون بـرای آن مجـازات تعیـین شـده باشـد (صبح‌خیز، ۲۷:۱۳۹۱).

٤. روش‌شناسی پژوهش

روش انجام تحقیق در این مبحث، توصیفی- تحلیلی است و گردآوری داده ها و اطلاعات مورد نیاز این پژوهش به روش کتابخانهای و اسنادی، از طریق مطالعه وبگاههای علمی – حقوقی معتبر و مصوبات نهادهای حقوقی و بین‌المللی و همچنین مطالعه کتب مربوط به فضا و جرایم سایبری و رایانه‌ای و اسناد حقوقی کنوانسیون‌های مختلف و دیگر قوانین و مقررات بین‌المللی انجام شده است.

٥. چالش‌های زنان در فضای سایبری

١.٥ فردگرایی و اصالت فرد

آنچه در فضای مجازی بسیار مشهود است گسترش اهمیت فرد و حیطه خصوصی در برابر جمع و حوزه عمومی است. افراد در فضای مجازی درعین‌حال که در اجتماعات می‌توانند حضور داشته باشند؛ اما چون می‌توانند هویت واقعی خود را پنهان کنند، می‌توانند در همان حال خود را جدا از دیگران و تنها حس کنند، این ویژگی باعث تقویت توانایی و قابلیت‌های فردی مشخص شده است و او را قادر می‌کند تا پنهانی‌ترین روح و شخصیت خود را به فعلیت برساند. نبود مراتب قدرت در فضای مجازی باعث می‌شود که فردیت افراد در محل حل نشود و به تعبیر گیدنز شخص در جماعت مجازی، روش زندگی با احترام به استقلال فردی را می‌آموزد و عمل می‌کند(گیدنز،١٣٨٦). اساس فرد و هویت‌های فردی آن‌قدر سیال و متغیرند که جمع به معنای سنتی آن نمی‌تواند در فضای مجازی تشکیل شود. فردیت‌های تقویت‌شده عاملیت خود را در فضای جامعه افزایش خواهد داد و باعث حرکت‌ها و جنبش‌هایی خواهد شد که برابر روندهای عادی جامعه قرار دارد و آنها را روندهای معکوس می‌نامند، عاملی معتقد است که روندهای معکوس همگی بیانگر قوی شدن فرد و غلبه هنجارهای فردی بر هنجارهای جمعی و عادات اجتماعی هستند. این تکثر فرهنگی به‌طورقطع ارتباط معناداری با گسترش ارتباطات انسانی دارد که سهم قابل‌توجه آن مرتبط با عضویت‌های جدید در جوامع مجازی است. (Amelli,2011)

۲.۵ موقتی بودن ارتباط‌ها و پیوندها

همه‌چیز در فضای مجازی موقتی است، هیچ تضمینی برای ادامه فعالیت و کنش یک عضو در یک جماعت مجازی وجود ندارد و به همین جهت هیچ احساس مسئولیتی درباره یکدیگر ندارند و تنها به شکلی عاطفی، لحظه‌ای و هیجانی شکل می‌گیرد و تصمیم‌گیری می‌شود.

۳.۵ هنجارشکنی در اینترنت

فضای مجازی به علت مبهم بودن هویت‌ها، نبود ارتباط چهره به چهره و نبود هرم قدرت، محیط بسیار مساعدی برای تخطی از هنجارها و ارزش‌ها و کژروی‌های اخلاقی و عقیدتی است. این انحرافات می‌تواند نظیر گپ‌های جنسی، وارد شدن به سایت‌های مستهجن و پورنوگرافی و ایجاد وبلاگ و قرار دادن منوی غیراخلاقی باشد.

۴.۵ کاهش روابط اجتماعی واقعی

جذابیت فضای مجازی به حدی است که کاربران در ابتدای دسترسی به اینترنت ساعت‌ها به روی آن نشسته و متوجه گذشت زمان نمی‌شوند. مطالعه‌ای که در ابتدای همه‌گیری اینترنت توسط گرانت انجام‌شده به این نتیجه رسیده که استفاده بیشتر از اینترنت منجر به کاهش ارتباطات اجتماعی شده است. این نتایج بر این پایه بود که نزدیکی فیزیکی یکی از عوامل اساسی ایجاد روابط اجتماعی به‌ویژه از نوع صمیمانه و عاطفی آن است، اما هرگز روابط اجتماعی نمی‌تواند در فضای مجازی بازتولید شود(Amelli,2011).

۵.۵ هرج‌ومرج و بی‌نظمی

هرگونه اقتدار خطر ابتلا به استبداد را دارد اما در برابر آن حذف اقتدار نیز باعث تنازع و درگیری‌ها شده و به چیزی ختم می‌شود که آنارشیزم اینترنتی نامیده می‌شود. ماهیت آنارشیک یا حداقل ساختار نیافته شبکه‌ها مفهوم سلسله‌مراتب را در آنها دشوار می‌کند. ویژگی مشترک که جماعت و سلسله‌مراتب را به هم پیوند می‌دهد مفهوم هویت است. که نه‌تنها درک شخص از خود، بلکه شخص از دیگران است؛ لذا با وجود هویت‌های غیرواقعی و چندگانه چیزی به نام سلسله‌مراتب قدرت نمی‌توان ایجاد کرد. مورد دیگر

حجم عظیمی از اطلاعات در فضای مجازی است که بدون مدیریت به هرج‌ومرج تبدیل می‌شود. واقعیت دیگر فضای مجازی مضمحل شدن فضای خصوصی انسان‌هاست که حس امنیت را در افراد پایین خواهد آورد و افراد و گروه‌های نفوذگر توانایی حضور خود را در خصوصی‌ترین جنبه‌های زندگی انسان‌ها به نمایش خواهند گذاشت (مظاهری، ایرانشاهی، ۱۳۸۹).

۶.۵ خشونت

پاتریشیا ولش بیان می‌کند: «زنان در برخورد با نگرش‌های کلیشه‌ای در محیط‌های آرام اینترنت، به شیوه‌هایی عمل می‌کنند، تا «بر همُکنش» انجام دهند. بااین‌همه اینترنت جایگاه محیط‌های کینه‌توزانه‌تری است و در پاره‌ای از آنها، زنان به گونه ویژه‌ای آسیب‌پذیرند و احساس ناراحتی می‌کنند.» زیرا مردان به تعبیر «سوزان‌سی‌هرینگ» رویکردی پرخاشگرانه و پیشی‌طلبانه دارند. درنتیجه برخی از سایت‌ها، محیطی برای کامیابی تباهی پسران جوان و محیطی وسوسه‌انگیز برای برخی از زنان می‌باشد. به‌طور نمونه، ماجرای جرم اینترنتی «بیکر» شهرتی جهانی به هم زد، او کسی است که در داستان‌پردازی‌های اینترنتی خود در یکی از سایت‌ها، ماجرای خیالی تجاوز به عنف و قتل دختری را که از همکلاسی‌های دانشگاهی‌اش بود، وارد یک سایت خبری سکسی نمود و از طریق طرح گرافیکی، آن را توصیف کرد و موجب وحشت زنان شد.

۷.۵ آزار جنسی

در کنار خشونت، آزار جنسی، پدیده دیگری است که در دنیای اینترنتی نصیب زنان شده است. در فضای مجازی، برخی کاربران «به شکل رکیک و آشکار به مسائل جنسی می‌پردازند که باعث برانگیختن زنان می‌شود و با شوخی‌های نامناسب موجب رنجش خاطر آنها می‌شوند و حتی در بعضی محیط‌های اینترنت، زنان آماج آزار جنسی قرار می‌گیرند. نتیجه خشونت و آزار جنسی در دنیای مجازی، سلب امنیت از زنان است، یکی از کاربران زن می‌گوید: «به‌گونه‌ای باورنکردنی دچار بدبینی شده بودم، می‌خواستم اطمینان یابم که درهای ساختمان کوچک ما همواره بسته است، تمرین خود پدافندی می‌کردم» (مظاهری، ایرانشاهی، ۱۳۸۹).

۸.۵ تحقیر منزلت

در کنار خشونت، آزار جنسی و ناامنی، آزارهـای حیثیتـی و تحقیـر منزلـت، پدیـده دیگـری است که با برنامه از پیش تعیین شده، یا بدون برنامه و تفننی عاید زنان می‌گردد.

با ذکر برخی از چالش‌های حضور زنان در فضای سـایبری کـه بـدان‌هـا اشـاره گردیـد **می‌توان گفت** وجود فرصت‌هـای بزهکـاری و نیـز فقـدان موانـع فیزیکـی جهـان واقعـی، «انگیزش یافتگی» برای ارتکـاب جـرم را در بسـیاری از بزهکـاران بـالقوه و بالفعـل فضـای مجازی بالابرده است؛ و به باور برخی پدیـده «عمـومی شـدن بزهکـاری در فضـای سـایبر» محقق شده است. به تبع این موضوع، گونـه‌هـای بـزه علیـه زنـان در پـارادایم مجـازی نیـز عمومیت یافته است و ادعای «زنانه شدن بزه دیدگی در فضـای سـایبر» مقـرون بـه صـحت است تا جایی که گفته می‌شود، برای بزهکارانی که به دنبال سوءاستفاده‌های جنسـی از زنـان هستند، فضای سایبر نظیر «شبکه‌های اجتماعی» که قابلیت حضور آنلاین و دسترسـی مکـرر به بزه‌دیده در آنها وجود دارد، جایگزین تفریحگاه‌ها شده است.

٦. اشکال بزه‌دیدگی سایبری زنان

می‌توان تمام انـواع بـزه دیـدگی سـایبری زنـان در فضـای سـایبری را در چنـد مـورد عـامِ «آزار سایبری»، «تحریف نگاری»، «تجاوز به حریم خصوصی» خلاصه نمود.

۱.۶ آزار سایبری

اذیت و آزار سایبری در شبکه‌های اجتماعی به شیوه‌های مختلفی انجـام مـی‌شـود؛ گذاشـتن پیام‌هایی بر روی صفحه بزه دیده به‌صورت مکـرر، ارسـال مـداوم درخواسـت بـرای رابطـه دوستی، ارسال دائمی پیام‌های ابراز مخالفت با بزه دیده و مواردی ازاین‌دست مصادیق جـرم آزار سایبری محسوب مـی‌شـوند (Willard, 2007). بـدکلامی توسـط گروهـی از مزاحمـان سایبری برای بیان نفرت علیه زنان نیـز، گونـه دیگـری از عنـوان مزاحمـت سـایبری اسـت؛ این‌گونه از مزاحمت را به‌عنوان حمله سـایبری اوبـاش گونـه، توصـیف کـرده‌انـد (Citron, 2009). بنا بر آمار موجود در میان جرائم سایبری، توهین و آزار سـایبری بیشـترین شـیوع را دارند. (Williams,2012). در ادامه به برخـی از مصـادیق آزار زنـان در شـبکه‌هـای اجتمـاعی اشاره می‌شود:

۱.۱.۶ شایعه‌پراکنی سایبری

به ارسال شایعات تحقیرآمیز یا شرمسار کننده درباره قربانی در چت‌روم، گروه‌های خبری یا تابلوهای اعلانات اینترنتی اشاره دارد (McFarlane,2003). رایج‌ترین شکل تهمت و هتک حیثیت سایبری، ارسال کنایه‌های جنسی کذب درباره قربانی است (Petrocelli,2005) . گاه این شایعات به جهت شیوع بالا و انتشار در میان طیف زیادی از دوستان بزه دیده، موجب انزوا یا ترک گروه‌های مشترک با آنان می‌گردد.

۲.۱.۶ ناسزاگویی سایبری

در این روش، فرد مزاحم، ممکن است به‌طور دائم هدف خود را در شبکه‌های اجتماعی، هم بر روی صفحه او، هم در بین گروهی که عضو آن است، مورد تحقیر و زورگویی قرار دهد (Langos, 2013). این نوع بزهکاری ممکن است شامل ارسال مداوم پیام‌های متنی به صفحه صاحب پروفایل و یا سایر مکان‌ها شود.

۳.۱.۶ مسدودسازی کاربر

در یک گروه یا جمعیت که برای اجازه دادن به افراد برای بیان عقاید شخصی‌شان، ساخته شده است و عموماً در یک گروه یا جمعیتی که غالب آنها اشتراکاتی از حیث جنسیت، مذهب و عقیده و... دارند اعضاء گروه ممکن است فرد خاصی را با ممنوع ساختن او به خاطر عقاید یا وضعیت خاصش، بزه دیده سازند.

۲.۶ تحریف‌نگاری سایبری

تحریف نگاری به معنای دگرگون کردن محتوای داده‌های دیگری است. این رفتار در حوزه جرائم مرتبط با محتوا است؛ از همین روی با جعل رایانه‌ای یا تخریب متفاوت است (Aalipour,2011). تحریف نگاری، بیش از هر مزاحمت دیگری آبروی بزه دیده را مخدوش می‌سازد و جنبه عمومی بیشتری نسبت به دیگر انواع مزاحمت دارد.

۱.۲.۶ قلب تصاویر

مصداق بارز این نوع از بزه دیدگی، شامل مورفینگ می‌شود. در این مورد، تصاویر کاربر شبکه اجتماعی از آلبوم‌های شخصی وی گرفته می‌شود، سپس به‌استثنای قسمتی از عکس

مانند سروصورت که معرف آن شخص خاص باشد بقیه عکس مورد تغییر و دست‌کاری قرار می‌گیرد. مورفینگ یا تحریف نگاری به چند صورت نمود می‌یابد: گاهی دگرگونی در محتوای دیگری به‌گونه‌ای است که به حالت استهجان یا ابتذال درمی‌آید. گاهی دگرگونی، سبب هتک حیثیت می‌شود که در اینجا با بررسی عرف، بزه شناسایی می‌شود. علاوه بر این هرزگی سایبری می‌تواند به‌وسیله هک کردن پروفایل کاربر زن، عملی گردد بدین‌صورت که ابتدا فرد مزاحم، پروفایل را هک می‌کند، سپس تصویر اصلی را تغییر می‌دهد و روی صفحه پروفایل زن، قرار می‌دهد و پس‌ازآن، از نام و اطلاعات و نیز تصویر تغییریافته استفاده می‌کند تا برای دوستان او، همچنین مخاطبان گسترده‌تری، پیام‌های مستهجن بفرستد (Sanders, 2010).

۲.۲.۶ همانندسازی

در این نوع از بزهکاری، بزهکاران پروفایل همانندسازی شده، یا تقلبی از بزه دیده را با استفاده از سرقت اطلاعات شخصی کاربر ایجاد می‌کنند. سپس پروفایل همانندسازی شده از دوستان کاربر اصلی می‌خواهد تا با او دوست شوند و بدین گونه برخلاف مواردی که تنها از اطلاعات عضو اصلی برای اهداف پلید استفاده می‌شود، در این مورد یک گام فراتر در بزه دیده سازی به‌وسیله ایجاد شکاف در حریم خصوصی سایر کاربران نیز برداشته می‌شود. متأسفانه امروزه کاربران زن بیشتر شبکه‌های اجتماعی محبوب و با دامنه بالای آزادی عمل غالباً با این مشکل روبرو می‌شوند. چالش‌های فراروی هویت در فضای مجازی، مدیریت آن را ضروری ساخته است. اهمیت هویت و عناصر هویتی در شبکه‌های اجتماعی موجب شده تا پدیده‌ای به نام سرقت هویت در این فضا از موضوعیت زیادی برخوردار شود و اشکال مختلفی به خود بگیرد(Bocij, 2003).

۳.۶ تجاوز به حریم خصوصی

۱.۳.۶ دسترسی غیرمجاز

دسترسی غیرمجاز عبارت است از رخنه غیرقانونی به سامانه رایانه‌ای حفاظت‌شده که گاه در زبان فنی به آن هک یا رخنه گری گفته می‌شود؛ ممکن است ثمره نامطلوب هک، مسدود کردن یک کاربر و ممنوع ساختن او از بیان دیدگاه‌هایش یا قرار دادن دیدگاه و

نظری مخالف نظر فرد بزه دیده توسط شخص هکر باشد که خود مزاحمتی مضاعف برای او به شمار می‌رود. نتیجه نامطلوب دیگری که عمل مجرمانه دسترسی غیرمجاز برای بزه‌دیده زن می‌تواند داشته باشد، افشا و انتشار محتویات حریم خصوصی بزه دیده توسط بزهکار است. مرتکبان این جرم، با انگیزه‌های مختلف مبادرت به انتشار یا در دسترس قراردادن فیلم، تصویر یا صدای اشخاص در فضای سایبر می‌نمایند. در این شیوه، اهداف خاصی برگزیده می‌شوند و پروفایل آنها هک می‌شود. اطلاعات شخصی آنها برای اهداف پلید مورداستفاده قرار می‌گیرد؛ و در این صورت امکان هرگونه سوءاستفاده از اطلاعات شخصی بزه دیده وجود دارد(Sanders, 2010).

۲.۳.۶ تعقیب ایذائی سایبری

«استالکینگ» یا تعقیب ایذائی سایبری به وضعیتی اطلاق می‌شود که یک کاربر در تمام گروه‌هایی که به آنها پیوسته، مخفیانه تعقیب شده و صفحات دوستانش به امید دیدن پست‌های او، نوشته‌های شخصی او فعالیت‌های آنلاین او، پیوسته زیر نظر باشد. حتی برخی مزاحمان سایبری به‌منظور تعقیب و اطلاع یافتن از فعالیت‌های روزانه و محل‌های رفت‌وآمد بزه دیدگان، کارآگاه خصوصی استخدام می‌کنند (Bocij, 2003).

حفاظت از حریم خصوصی در فضای سیال مجازی بسته به تدابیر ایمنی که کاربر توان استفاده از آنها را دارد، ممکن است قوی‌تر یا ضعیف‌تر از فضای واقعی باشد، گاه کاربر به آخرین ابزارهای رمزنگاری مجهز است و توان استفاده از آنها را دارد؛ اما در اغلب موارد کاربران، به‌ویژه زنان، سواد رسانه‌ای بالایی در این زمینه ندارند و با تشکیل یک صفحه در شبکه‌های اجتماعی، حریم خصوصی آنان با تهدید مواجه می‌شود.

۷. فضای سایبر و قانون‌گذاری

برای جلوگیری از خشونت سایبری و ایجاد امنیت در فضای سایبر به‌ویژه برای زنان نیاز به قانون‌گذاری در این فضا در دو سطح ملی و بین‌المللی می‌باشد. جرم سایبری اغلب دارای بعد بین‌المللی است. پست‌های الکترونیکی با محتوای غیرقانونی، اغلب از میان تعدادی کشور حین انتقال از فرستنده به گیرنده عبور می‌کنند، یا محتوای غیرقانونی خارج از کشور ذخیره می‌شود. در پیگرد جرائم سایبری همکاری نزدیک بین کشورهای درگیر بسیار مهم است. توافقات قانونی دوطرفه موجود بر پایه فرآیندهای رسمی، پیچیده و اغلب زمان‌بر

است. انجام توافقات برای پاسخ سریع به رویدادها، همچنین درخواست‌ها برای همکاری بین‌المللی ضروری است. تعدادی از کشورها، نحوه همکاری قانونی دوطرفه‌شان را براساس اصل مجرمیت دوگانه قرار می‌دهند. پیگردها در سطح جهانی در کل، محدود به جرائمی هستند که در همه کشورهای شرکت‌کننده جرم شمرده می‌شوند. اگرچه تخلفاتی وجود دارد که در هرجایی از دنیا می‌توانند مورد پیگرد قانونی قرار گیرند بااین‌وجود تفاوت‌های منطقه‌ای، نقش مهمی را در این امر بازی می‌کنند. جرم‌انگاری محتوای غیرقانونی در کشورهای مختلف، متفاوت است. موضوعاتی که ازلحاظ قانونی می‌توانند در کشوری منتشر شوند، ممکن است در کشور دیگری غیرقانونی باشند.

قانون‌گذاری ملی، بین‌المللی، خودانتظامی و مختلط از اقسام روش‌های قانون‌گذاری در فضای سایبر به شمار می‌آیند. روش قانون‌گذاری ملی، حاکی از رویکرد حاکمیت انحصاری دولت‌ها بر فضای سایبر، و روش‌های بین‌المللی، خودانتظامی و مختلط، متأثر از نگرش مبتنی بر دکترین تعمیم نظریه میراث مشترک بشریت بر فضای سایبر است.

۱.۷ رویکرد قانون‌گذاری ملی

در این روش، نهادهای قانون‌گذاری ملی نسبت به قانون‌گذاری و جرم انگاری در فضای سایبر اقدام می‌کنند (Graham J. H. Smith,2002). باید توجه داشت که در این روش اولاً، نمی‌توان از جرم انگاری تمام جرائم در فضای سایبر، اطمینان خاطر داشت و ثانیاً، این روش می‌تواند موجب تعارض قوانین در فضای سایبر شده و اصل قانونی بودن جرم و مجازات و اصل منع مجازات مضاعف را تحت تأثیر قرار دهد. ازآنجاکه این روش، مستعد تصویب قوانین فراسرزمینی و انحصاری سازی فضای سایبر است، می‌تواند منجر به تصویب قوانین انسدادی توسط کشورها برای جلوگیری از اعمال صلاحیت کشورهای خارجی شود. از سوی دیگر، عملکرد برخی کشورها ازجمله چین در قانون‌گذاری حداکثری، منجر به خودسانسوری در فضای سایبر شده است(Hu Ling,2011). ازآنجاکه قانون‌گذاری در فضای سایبر توسط مراجع ملی، مبتنی بر یکی از مبانی شناخته‌شده صلاحیت است در ادامه به نقد و بررسی قانون‌گذاری در فضای سایبر بر مبنای صلاحیت سرزمینی، صلاحیت شخصی، صلاحیت واقعی و صلاحیت جهانی پرداخته می‌شود (ضیایی، شکیب‌نژاد،۱۳۹۶).

۱.۱.۷ صلاحیت سرزمینی

لازمه توسل به صلاحیت سرزمینی در فضای سایبر، وجود مرزهای دقیق است تا مقررات دولتی در حیطه آن عینیت یابد(افضلی و همکاران،۱۳۹۲). عدم امکان اجرای قواعد سنتی بر فضای بی‌انتهای سایبر از پیچیدگی‌های این فضاست. یکی دیگر از معضلات صلاحیت سرزمینی در فضای سایبر، ناپیدا بودن محل ارتکاب جرم در این فضاست. اغلب نمی‌توان محل وقوع جرم را شناسایی کرد. حتی اگر تارنماها با کد کشوری به‌عنوان محل وقوع جرم ملاک گرفته شود، این اشکال در مورد تارنماهای با کد عمومی باقی می‌ماند. هرچند برخی کشورها معیارهایی مانند محل وقوع سامانه‌های رایانه‌ای، داده‌های رایانه‌ای و ذخیره اطلاعات را به‌عنوان معیار تعیین سرزمین در نظر گرفته‌اند، قانون‌گذاری‌های متعارض موجب می‌شود یک عمل درآن‌واحد در صلاحیت سرزمینی چند کشور قرار گیرد.

۲.۱.۷ صلاحیت شخصی

اعمال صلاحیت شخصی در فضای سایبر، مستلزم احراز تابعیت مجرم یا بزه دیده است. شناسایی مجرم در این فضا منوط به تعیین شناسه اوست. درحالی‌که فرد به‌راحتی با استفاده از برنامه‌های رایانه‌ای، قادر به جعل شناسه خود است. ثانیاً، لازمه اعمال صلاحیت شخصی منفعل در این فضا، انجام تحقیقات در رایانه‌های واقع در خارج از کشور (ولو از راه دور) است که موجب نقض حاکمیت سرزمینی کشور محل اطلاعات خواهد شد. علاوه بر این، اعمال موسع صلاحیت شخصی در فضای سایبر به روند تجارت الکترونیک در فضای سایبر، لطمه خواهد زد(James R. Pielemeier,2009).

۳.۱.۷ صلاحیت واقعی

اعمال صلاحیت واقعی نیز با این اشکال روبه‌روست که ضابطه دقیقی برای توسل به آن وجود ندارد. البته دست دولت‌ها برای اعمال صلاحیت واقعی کاملاً باز نیست و باید از اعمال موسع صلاحیت واقعی امتناع کرد. لذا در این زمینه لازم است میان اعمال صلاحیت واقعی و اصل آزادی اینترنت، موازنه‌ای عادلانه برقرار شود که درنتیجه آن، اعمال صلاحیت واقعی در فضای سایبر در چارچوب موازین حقوق بشری صورت پذیرد (Wittzack,2010). دادگاه آلمان در قضیه توین در رابطه با انکار هولوکاست توسط یک استرالیایی در تارنمایی در استرالیا، صلاحیت واقعی را اعمال کرد. دادگاه فرانسه نیز در رابطه ارائه یادبودهای

نازی‌ها در یک سرور مستقر در ایالات‌متحده معتقد بود که حقوق کیفری فرانسه نقض شده است. همچنین طبق قانون میهن‌دوستی آمریکا، اداره تحقیقات فدرال مجاز است با قرار قضایی به پیام‌های پست‌های صوتی افراد، دسترسی داشته باشد یا مقامات مجاز بدون رعایت الزامات قانون شنود، اطلاعات رایانه‌ای افراد را رهگیری کنند.

۴.۱.۷ صلاحیت جهانی

صلاحیت جهانی، یکی دیگر از مبانی قانون‌گذاری در فضای سایبر است. باید توجه داشت که برخی اقدامات در برخی مناطق، مورداعای صلاحیت هیچ دولتی نیست و لذا اعمال صلاحیت در خصوص آنها نه‌تنها مداخله در حاکمیت دیگر دولت‌ها نیست، بلکه برای جلوگیری از تبدیل‌شدن آن منطقه به پناهگاه امن متخلفین و پرهیز از شکل‌گیری «سرزمین بی‌قانون» لازم است. دزدی دریایی در آب‌های آزاد در گذشته و اقدامات مجرمانه در اینترنت در زمان حاضر از نمونه‌های این وضعیت است. ماده ۲۲ کنوانسیون جرائم سایبری شورای اروپا (کنوانسیون بوداپست) جایگاه صلاحیت جهانی در فضای سایبر را تأیید می‌کند(Cottim,2010). مبانی صلاحیت جهانی برای برخی جرائم سایبری مانند تحریک به نسل‌کشی در معاهدات بین‌المللی موجود است و قوانین داخلی دولت‌ها، برخی جرائم سایبری را مانند هرزه‌نگاری کودکان، مشمول صلاحیت جهانی قرار داده‌اند.

درمجموع، قانون‌گذاری ملی، مشکلاتی برای دولت‌ها و کاربران ایجاد خواهد کرد. این شیوه موجب اعمال فراسرزمینی قوانین خواهد شد که تعارض قوانین میان دولت‌ها را به دنبال خواهد داشت و همچنین موجب اعمال هم‌زمان چند نظام حقوقی بر کاربران فضای سایبر و متعاقباً سردرگمی کاربران خواهد شد. لذا کاربران، خودبه‌خود ملزم به رعایت قوانین متعدد و حتی متناقض خواهند بود، درحالی‌که ممکن است از محتوای آن قوانین بی‌خبر باشند. در این شیوه همچنین خطر چند کیفری وجود دارد؛ خصوصاً آنکه افراد نمی‌دانند کدام قانون را باید پاس بدارند و درنهایت مجبور خواهند بود مضیق‌ترین قانون را رعایت کنند. درواقع، ماهیت جهان‌شمولی موجب می‌شود افراد بر اساس معیارهای مختلف صلاحیتی، تحت شمول قوانین چند کشور قرار گیرند. بااین‌حال، موافقت‌نامه‌های معاضدت قضایی و تعهدات حقوق بشر می‌توانند این معضل را کاهش دهند (ضیایی، شکیب‌نژاد، ۱۳۹۶).

۲.۷ رویکرد قانون‌گذاری بین‌المللی

روش قانون‌گذاری بین‌المللی با توجه به یکپارچگی اینترنت و مشکلات ناشی از قانون‌گذاری ملی مطرح شد. این شیوه در بهترین شکل با انعقاد معاهدات بین‌المللی محقق می‌شود. به‌طور مثال، ماده ۳ پروتکل الحاقی به کنوانسیون حقوق کودک، مورخ ۲۰۰۰ درخصوص فروش، فحشا و هرزه‌نگاری کودکان به‌صراحت بر نقش اینترنت در توزیع هرزه‌نگاری کودکان اشاره دارد و از کشورها می‌خواهد این‌گونه افعال را جرم انگاری کنند. همچنین یکی از مهم‌ترین کنوانسیون‌های مربوط به فضای سایبر، کنوانسیون بوداپست درخصوص جرائم سایبری است. بااین‌حال، این کنوانسیون نمی‌تواند به‌عنوان معاهده‌ای جامع تلقی شود، چه آنکه اولاً، تمام جرائم سایبری را دربرنمی‌گیرد و ثانیاً، این کنوانسیون صرفاً برای کشورهای اروپایی لازم‌الاجراست. درهرصورت، معاهدات منطقه‌ای و دوجانبه، پاسخگوی حل مشکلات نبوده و معاهده اینترنتی در سطح بین‌المللی موردنیاز است. برخی از قواعد آمره، نظیر ممنوعیت دزدی دریایی، برده‌داری و نسل زدایی نیز در فضای سایبر قابل‌اعمال است (Kurbalija,2014).

سازمان‌های بین‌المللی نیز در فرایند بین‌المللی سازی قانون‌گذاری در فضای سایبر، نقش قابل‌توجهی داشته‌اند. پیش از همه، آنسیترال با تصویب قانون نمونه آنسیترال در خصوص تجارت الکترونیکی در سال ۱۹۹٦ نقش چشمگیری در هماهنگ‌سازی قوانین ملی کشورها درباره مسائل مربوط به تجارت الکترونیک داشته است. گروه هشت نیز در اولین اقدام خود در سال ۱۹۹۷ کمیته فرعی جرائم رایانه‌ای را برای مقابله با جرائم سایبری تأسیس و متعاقباً یک برنامه اقدام ده اصلی را در این رابطه تصویب کرد. مجمع عمومی سازمان ملل متحد در سال‌های ۲۰۰۰ و ۲۰۰۳ تلاش‌هایی برای تنظیم امنیت اطلاعاتی و سایبری انجام داد. پس از تلاش اتحادیه اروپا برای تصویب کنوانسیون جرائم سایبری، اتحادیه عرب به پیشنهاد ایالات‌متحده عربی یک مدل قانونی در خصوص همسان‌سازی قوانین ملی کشورهای عربی را در سال ۲۰۰۳ پذیرفت. شورای همکاری خلیج‌فارس نیز در کنفرانس ۲۰۰۷ به دولت‌ها توصیه کرد که رویکردی متحدانه را در خصوص مواجهه با موضوعات سایبری اتخاذ کنند. سازمان کشورهای آمریکایی، سازمان همکاری و توسعه اقتصادی، سازمان همکاری و اقتصادی آسیا – اقیانوسیه و سازمان کشورهای مشترک‌المنافع نیز در یکسان‌سازی قواعد بین‌المللی تلاش‌هایی داشته‌اند.

اما شاید مهم‌ترین تلاش، اجلاس جهانی جامعه اطلاعات در سال ۲۰۰۳ باشد که در آن تشکیل سازمان بین‌المللی اینترنت و انعقاد معاهده‌ای اینترنتی پیشنهاد شد. اتحادیه بین‌المللی مخابرات در مه ۲۰۰۷ آژانس جهانی جرائم سایبری و متعاقباً گروه کارشناسان ارشد را با هدف ارائه پیشنهادهایی برای جرم انگاری سایبری بنیان‌گذاری کرد(Schjolberg,2009). بالاخره سند اصلاحی مقررات اتحادیه بین‌المللی مخابرات با اعطای وجهه حقوقی بین‌المللی به قانون‌گذاری در فضای اینترنت با رأی اکثریت کشورها به تصویب رسید. باید توجه داشت که فناوری محوری فضای سایبر موجب می‌شود که سهم کشورهای مختلف در تنظیم نظام حقوقی حاکم بر فضای سایبر متفاوت باشد. به همین دلیل، یکی از مدل‌های پیشنهادی در قانون‌گذاری بین‌المللی در فضای سایبر، تقسیم وظایف و امتیازات بر مبنای مؤلفه‌هایی مانند قدرت، ثروت و تخصص است. این روش که از آن تحت عنوان «هندسه متغیر»یاد می‌شود، در ساختار شورای امنیت، صندوق بین‌المللی پول و سازمان تجارت جهانی اعمال شده است. این راهکار در ماده ٤٩ اعلامیه اجلاس جهانی جامعه اطلاعاتی نیز مندرج است که مسیر مشارکت همه ذی‌نفع‌ها (اعم از عمومی و خصوصی) را در مدیریت فضای سایبر هموار می‌سازد (ضیایی، شکیب‌نژاد،١٣٩٦). در این روش به‌عنوان‌مثال می‌توان برای دولت‌ها و سازمان‌های فنی، حق رأی بیشتر و برای نمایندگان جامعه مدنی، حق رأی کمتری اختصاص داد. مشکل محتمل در استفاده از روش هندسه متغیر این است که ایجاد چنین نظامی نیازمند مذاکراتی طولانی و جزئی برای جلب منافع همه گروه‌هاست(Kurbalija,2014).

۳.۷ رویکرد خودانتظامی

ازنظر برخی حقوق‌دانان، به جهت ماهیت یکپارچه و فرامرزی فضای سایبر، قواعد سنتی صلاحیت، مناسب بافت اینترنت نیست و باید برای اینترنت، حاکمیتی جداگانه به رسمیت شناخت. نتیجه این نگرش، شیوه خودانتظامی در قانون‌گذاری در فضای سایبر خواهد بود. در روش خودانتظامی به‌جای دولت‌ها، شرکت‌های سایبری یا مالکان تارنما ملزم به ایجاد محدودیت در فضای سایبر هستند. مهم‌ترین دلیل خودانتظامی فضای سایبر این است که فضای سایبر برخلاف دولت‌ها غیرمتمرکز و جهانی است. همچنین این روش، علاوه بر اینکه کارایی قانون‌گذاری ملی را داراست، به‌مراتب، ساده‌تر و ارزان‌تر بوده و به دلیل نقش پیشگیرانه این روش از آمار جرائم در فضای سایبر نیز کاسته خواهد شد. روش

خودانتظامی در عمل با مشکلاتی روبه‌روست. اولاً، به دلیل حذف نهاد دولت به‌عنوان رکنی فرادستی، موجب هرج‌ومرج در فضای سایبر خواهد شد. ثانیاً، ازنظر حامیان مشترکات «ابتکاری»، الزام تأمین‌کنندگان خدمات اینترنتی به خودسانسوری، خلاقیت در محیط دیجیتال را تحت‌الشعاع قرار می‌دهد. همچنین لازمه اقدام نهادهای فنی و صاحبان تارنماها، داشتن پشتوانه قانونی توسط دولت‌هاست، درحالی‌که دولت‌ها در حال حاضر از این نظر حمایت نمی‌کنند(Murray,2007).

۴.۷ رویکرد مختلط

برخی معتقدند که نباید مدیریت اینترنت را به قانون‌گذاری ملی یا قانون‌گذاری بین‌المللی یا شیوه خودانتظامی واگذار کرد. هر یک از سه شیوه قانون‌گذاری در خصوص مشروعیت یا اجرا، اشکالاتی دارد. برخلاف قانون‌گذاری بین‌المللی که از بالاترین سطح اجرا و پایین‌ترین سطح مشروعیت برخوردار است، خودانتظامی دارای بالاترین سطح مشروعیت و پایین‌ترین سطح اجراست. همچنین قانون‌گذاری ملی، حالتی بینابین بوده و همواره با ضعف نسبی در اجرا و مشروعیت مواجه است. انتخاب روشی مختلط، زمینه را برای حل معضلات ناشی از مشروعیت و اجرا و همچنین نیل به تفاهم میان همه بازیگران فعال در فضای سایبر باز خواهد کرد. خصیصه برخی جنبه‌های اینترنت مانند جرائم و تجارت اینترنتی به‌گونه‌ای است که نیازمند قانون‌گذاری است، درحالی‌که مناسب است جنبه‌های زیربنایی فضای سایبر با توجه به تخصصی بودن در اختیار نهادهای غیردولتی حفظ شود. همچنین همکاری بین‌المللی برای یکسان‌سازی حقوقی لازم است. کنوانسیون بوداپست به شیوه مختلط توجه داشته و در ماده ۲۳ به همکاری بین‌المللی و در ماده ۱۱ به قانون‌گذاری متقابل توجه کرده است (ضیایی، شکیب‌نژاد،۱۳۹۶).

۸. رویکرد ایران در قانون‌گذاری فضای سایبر

رویکرد ایران در حیطه مدیریت داخلی اینترنت، مبتنی بر قانون‌گذاری ملی است. پیرو ابلاغ «سیاست‌های کلی شبکه‌های اطلاع رسانه‌ای رایانه‌ای» از سوی مقام رهبری، شورای عالی انقلاب فرهنگی، «مقررات و ضوابط شبکه‌های اطلاع‌رسانی رایانه‌ای» را در سال ۱۳۸۰ تصویب کرد. طبق این قانون به‌موازات حق دسترسی آزاد به اطلاعات، بر رعایت

حقوق داخلی در موضوعات اجتماعی، فرهنگی و فنی کشور تأکید شد. مقررات پراکنده دیگری مانند آیین‌نامه نحوه اخذ مجوز ضوابط فنی نقطه تماس بین‌المللی، آیین‌نامه واحدهای ارائه‌کننده خدمات اطلاع‌رسانی و اینترنت رسا (ISP)، مصوبات کمیسیون تنظیم مقررات ارتباطات در سال ۱۳۸٤، قوانین پنج‌ساله توسعه و قانون تجارت الکترونیک نیز وجود دارد، لیکن نخستین قانون جامع و متمرکز در ایران، قانون جرائم رایانه‌ای، مصوب ۱۳۸۸ و قوانین اصلاحی آن، مندرج در قانون آیین دادرسی کیفری ۱۳۹۲ است.

اگرچه رویکرد قوانین داخلی ایران بر روش قانون‌گذاری ملی تکیه دارد، نگرش انتقادی ایران به نحوه مدیریت زیرساخت‌های سایبری در سازمان اینترنتی، انتصاب اسامی و کدهای رقمی (آیکان) مبیّن پذیرش روش بین‌المللی در این عرصه از سوی ایران است. آیکان یکی از مراجع مهم در شیوه خودانتظامی در فضای سایبر است که درعین‌حال از قوانین داخلی امریکا تبعیت می‌کند. انتقاد دولت‌ها به آیکان، مربوط به اساسنامه این سازمان است که طبق آن، وزارت بازرگانی امریکا دارای حق وتو بر تصمیمات سازمان بوده و تغییرات سازمان باید به تصویب دولت امریکا برسد(Casey,2008). بدین‌جهت در یادداشت ایران بر پیش‌نویس چهارم گزارش دبیرکل اتحادیه بین‌المللی مخابرات چنین آمده است: «مهم‌ترین بخش‌های اینترنت که مربوط به سیاست عمومی است تحت حاکمیت همکاری میان دولت‌ها یا سازمان‌های بین‌المللی نیست بلکه تحت حاکمیت دولت‌های انفرادی است... موضوع فاجعه‌بار آن است که برخی دولت‌ها کنترل اساسی بر بخش‌های حیاتی اینترنت دارند.» حمایت ایران از نتایج اجلاس اتحادیه بین‌المللی مخابرات که منجر به ایجاد فشار بر ایالات‌متحده و تغییر اساسنامه آیکان شد، مؤید عدم مخالفت ایران با شیوه قانون‌گذاری بین‌المللی عادلانه است (ضیایی، شکیب‌نژاد،۱۳۹٦).

رأی مثبت ایران به سند اصلاحی اتحادیه بین‌المللی مخابرات در سال ۲۰۱۲ نیز بیانگر حمایت از رویکرد بین‌المللی است. رویکرد ایران در کنار کشورهای دیگری نظیر چین و کوبا در تقابل با سیطره ایالات‌متحده بر این فضا، مبتنی بر مشارکت بیشتر سازمان ملل و دولت‌ها در مدیریت کلان فضای سایبر است(Berry,2006). این امر منجر به اتخاذ تصمیماتی در جریان اجلاس جهانی جامعه اطلاعاتی ۲۰۰۵ تونس شد که مسیر را بر بین‌المللی سازی فضای سایبر هموار ساخت؛ همان‌طور که در نامه نماینده دائم ایران در سازمان ملل به دبیر کل این سازمان به ایجاد فضای مشارکت جمعی دولت‌ها، بخش خصوصی، جامعه مدنی و نهادهای بین‌المللی اشاره شده است.

امروزه طرح شبکه ملی اطلاعات و مجموعه قوانین حاکم بر فضای سایبر در ایران، نشان‌دهنده رویکرد ملی ایران به قانون‌گذاری در فضای سایبر است. بااین‌حال، اعمال روش قانون‌گذاری ملی در قوانین داخلی و پذیرش روش بین‌المللی در مدیریت آینده این فضا حاکی از تمایل ایران به اعمال روش مختلط در قانون‌گذاری در این فضا است.

۹. صلاحیت قانون‌گذاری در فضای سایبر در حقوق ایران

با توجه به اینکه امروزه رویکرد اصلی ایران، قانون‌گذاری ملی در عرصه فضای سایبر است باید شیوه‌های قانون‌گذاری ایران بررسی شود. این قانون‌گذاری با اتکا بر اقسام صلاحیت، شامل صلاحیت سرزمینی، شخصی، واقعی و جهانی امکان‌پذیر است. ماده ۳ قانون مجازات اسلامی، مصوب ۱۳۹۲ و قوانین مرتبط با فضای سایبر، ازجمله قانون تجارت الکترونیکی، مصوب ۱۳۸۲، قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای، مصوب ۱۳۷۹، قانون جرائم رایانه‌ای، مصوب ۱۳۸۸ و مقررات اصلاحی آن، مندرج در آیین دادرسی کیفری ۱۳۹۲ اصل را بر صلاحیت سرزمینی قرار داده‌اند. تقریباً در تمام مواد قانون جرائم رایانه‌ای و مواد مرتبط در قانون آیین دادرسی کیفری، عبارت «هرکس» بدون توجه به تابعیت مرتکب به کار رفته است. هرچند معیار صلاحیت سرزمینی در جرائم گوناگون سایبری متفاوت است، معیار صلاحیت سرزمینی در ماده ۱ (دسترسی غیرمجاز) ، ماده ۲ (شنود غیرمجاز) و ماده ۳ (جاسوسی رایانه‌ای) قانون جرائم رایانه‌ای، معیار وقوع «سامانه‌های رایانه‌ای» در قلمرو ایران است. معیار صلاحیت سرزمینی در مواد ٦ و ۷ قانون جرائم رایانه‌ای نیز وقوع «داده‌های رایانه‌ای» در قلمرو ایران است. بند (الف) ماده ٦٦٤ قانون آیین دادرسی کیفری، معیار دیگری اضافه می‌کند و «ذخیره اطلاعات» در قلمرو ایران را نیز مشمول صلاحیت سرزمینی ایران قرار می‌دهد. به‌علاوه بند (ب) این ماده، تارنماهای دارای دامنه مرتبه بالای کد کشوری ایران (ir) را در حکم خاک ایران قلمداد کرده و جرائم ارتکابی در این تارنماها را به مانند جرائم ارتکابی در قلمرو ایران می‌داند.

صلاحیت شخصی فعال در ماده ۷ قانون مجازات اسلامی به‌طور موسع آمده است و تمامی جرائم ازجمله جرائم رایانه‌ای را دربرمیگیرد. ماده ۸ قانون مجازات اسلامی نیز به صلاحیت شخصی منفعل، اختصاص یافته است، هرچند اعمال آن، مشروط به جرم انگاری متقابل شده است. اغلب جرائم ارتکابی در فضای سایبر از سوی بارگذاران ارتکاب می‌یابد. لذا قانون جرائم رایانه‌ای در اغلب موارد، همانند ارتکاب هتک حیثیت و نشر اکاذیب در

مواد ١٦ و ١٧ بارگذار را مجرم تلقی کرده است و لـذا او مشـمول صـلاحیت قـانونی ایـران می‌شود. بااین‌حال، مـاده ١٤ در بـاب انتشـار، توزیـع، معاملـه، تولیـد، ذخیـره یـا نگهـداری محتویات مستهجن، علاوه بر بارگذار، پیاده ساز را نیز مشمول مجازات دانسته است.

صلاحیت واقعی در ماده ۵ قانون مجازات اسـلامی آمـده اسـت و صـراحتاً اقـدام علیـه امنیت داخلی یا خارجی را در حیطه صلاحیت ایـران مـی‌دانـد. همچنـین مطـابق بنـد (پ) ماده ٦٦٤ قانون آیین دادرسی کیفری، ارتکاب جـرم در خـارج از ایـران علیـه سـامانه‌هـا یـا تارنماهای مورداستفاده قوای سه‌گانه، نهاد رهبری، نمایندگی‌هـای رسـمی دولـت، نهادهـای ارائه‌کننده خدمات عمومی و علاوه بر این، حمله گسـترده بـه تارنماهـای مرتبـه بـالای کـد کشوری را در شمول صلاحیت محاکم ایران کرده اسـت. در خصـوص صـلاحیت جهـانی، ماده ۹ قانون مجـازات اسـلامی، جرائمـی را کـه طبـق عهدنامـه‌هـا و مقـررات بـین‌المللـی تحت صلاحیت جهانی قرار گرفته در صلاحیت تمامی کشورها و ازجمله ایران می‌دانـد. در قوانین ایران در این خصوص صراحتی وجود ندارد. بـااین‌حـال، جـرائم موضـوع بنـد (ت) ماده ٦٦٤ قانون آیین دادرسی کیفری راجع به جرائم رایانه‌ای علیـه اطفـال کمتـر از ۱۸ سـال می‌تواند تحت شمول صلاحیت جهانی ایران قرار گیرد.

بنابراین قوانین ایران در اغلب موارد، بخصوص موضوعات مرتبط با سامانه‌هـا، داده‌هـا و تارنماهای اینترنتی با تعیین صلاحیت بر مبنای مکان داده‌ها، صلاحیت سـرزمینی را پذیرفتـه است (ضیایی، شکیب‌نژاد،١٣٩٦). این قـوانین، صـلاحیت شخصـی را دربـاره جـرائم علیـه اشخاص، صلاحیت واقعی را راجع به سامانه‌ها تارنماهای حکومتی و صـلاحیت جهـانی را صـرفاً در خصـوص سوءاسـتفاده از اطفـال شناسـایی کـرده اسـت. لـذا رویکـرد ایـران در صلاحیت قـانون‌گـذاری در فضـای سـایبر، دربردارنـده طیـف متنـوعی از صـلاحیت‌هـای قانون‌گذاری سرزمینی، شخصی، واقعی و جهانی است؛ هرچند در عرصه منطقه‌ای با نظر بـه عضویت ایران در سازمان همکاری‌های اسلامی می‌توان یکسان‌سازی قوانین ملـی در سـطح منطقه را پیشـنهاد داد. ایـن روش در گذشـته در اتحادیـه اروپـا، اتحادیـه عـرب و شـورای همکاری خلیج‌فارس نیز تجربه شده است. این امر با توجه بـه دیـدگاه مشـترک کشـورهای عضو سازمان کنفرانس اسلامی به برخی مقـولات فضـای سـایبر، همچـون هـرزه‌نگـاری و قلمرو آزادی بیان در حوزه مذهب، ممکن‌الحصول خواهد بود.

۱۰. نتیجه‌گیری

نمود نخستین و بدیهی منع خشونت علیه زنان در استاد بین‌المللی، در نخستین ماده منشور ملل متحد است که یکی از اهداف سازمان ملل متحد را ایجاد همکاری بین‌المللی برای ترویج و ترغیب احترام به حقوق بشر و آزادی همگان، فارغ از مواردی همچون جنسیت دانسته است؛ بنابراین تبعیض علیه زنان خود از موارد خشونت قلمداد می‌شود که مقابله با آن، از الزامات حقوق بشری است. چنان‌که در تعریف شورای اقتصادی – اجتماعی، تساوی جنسیتی به‌منزله بهره‌مندی زنان و مردان از موقعیت برابر در تمام جنبه‌های اجتماعی، سیاسی و اقتصادی مشابه است؛ مگر آنکه یک تفاوت بیولوژیک موجب رفتار متفاوت شود. افزون بر بند ۱ ماده ۲ و ماده ۳ میثاق بین‌المللی حقوق مدنی و سیاسی که بر تساوی حقوق زنان و مردان ازنظر حقوق مدنی و سیاسی پیش‌بینی شده در میثاق تأکید دارد، قید عبارت «غیرانسانی و ظالمانه» مندرج در ماده هفتم به ممنوعیت خشونت علیه زنان قابل تسری است. ماده ۳ و ۱۰ میثاق بین‌المللی حقوق اقتصادی، اجتماعی و فرهنگی نیز بر تضمین حقوق برابر زنان اصرار دارد. همچنین کنوانسیون منع شکنجه و دیگر رفتارها یا مجازات‌های ظالمانه، غیرانسانی یا تحقیرکننده، شکنجه را در معنایی گسترده شامل اقدامات رنج‌آوری می‌داند که با موافقت مقامات رسمی با ممانعت نکردن آنها روی می‌دهد؛ بنابراین برخی موارد خشونت علیه زنان که با مساعدت دولت‌ها همراه است، ممکن است در این تعریف قرار گیرند. اهمیت صیانت از زنان در برابر آسیب تا بدان جاست که مجمع بهداشت جهانی در اجلاس چهل و نهم خود در سال ۱۹۹۶ منع خشونت را اولویت سلامت عمومی دانسته و در قطعنامه‌ای به آثار خشونت علیه زنان و دختران بر سلامت جهانی پرداخته است.

خشونت علیه زنان بارزترین نوع نقض حقوق بشر در ارتباط با زنان است. با پیشرفت تکنولوژی و جهانی‌شدن ارتباطات خشونت علیه زنان عرصه‌ای جدید برای بروز یافته است. یکی از این عرصه‌ها فضای سایبری است. فضایی که با پنهان ماندن هویت و عدم قانونمندی افراد به‌راحتی هنجارهای دنیای واقعی را شکسته و در برآوردن امیال ضد انسانی خود گام برمی‌دارند. در دنیای معاصر که بیشتر ارتباطات و فعالیت‌های افراد به‌نوعی وابسته به استفاده از اینترنت و عضویت در دنیای سایبری است بسیاری از افراد نابهنجار با حضور در این فضا سعی در آسیب رساندن به زنان به‌عنوان قشر آسیب‌پذیر می‌کنند. طی چند سال گذشته با توسعه کشورها و تحقق رویای دهکده جهانی این

تکنولوژی در کنار آثار مثبتی که برای جهانیان داشته معایبی را هم به همراه داشته است. یکی از این معایب که امروزه به علت فراگیر شدن، توجه دولت‌ها و حتی سازمان ملل را به خود جلب کرده است پدیده خشونت در فضای مجازی است. زنان که نیمی از جمعیت جوامع را به خود اختصاص می‌دهند در دنیای مجازی هم به‌مثابه جهان واقعی حضوری پررنگ دارند اما برخلاف تمام تلاش‌هایی که سازمان‌های بین‌المللی و دولت‌ها در ارتقای جایگاه زنان و ایجاد برابری جنسیتی در دنیای واقعی داشته‌اند در دنیای مجازی به علت عدم قانونمندی و نبودن قدرت نظارت بر افراد چنین برابری وجود نداشته و حتی زنان بیشتر از دنیای واقعی هدف خشونت قرار می‌گیرند. زنان در فضای مجازی با انواع مختلفی از خشونت از فحاشی و تحقیر تا تهدید و آزار و اذیت جنسی روبه‌رو هستند. افزایش روزافزون خشونت مجازی علیه زنان در سطح جهانی نگرانی جوامع را برانگیخته و زنگ خطری را برای سازمان‌های حامی زنان به صدا درآورده است. اهمیت بررسی علل این افزایش خشونت از آنجاست که زنان نیمی از جمعیت جوامع بشری را به خود اختصاص می‌دهند. حضور زنان در دهه‌های اخیر در عرصه‌های مختلف فعالیت‌های اجتماعی و اقتصادی موجب شده است تا نقش اساسی آنها در تکامل و پیشرفت جوامع برجسته‌تر از گذشته شود. زنان و دختران جامعه امروز مادران نسل آینده خواهند بود این زنان و دختران برای تربیت نسلی پویا و سالم نیاز به امنیت و آرامش در جهت رشد و بالندگی دارند چه در دنیای واقعی چه در دنیای مجازی، دنیایی که با گذر زمان حضور افراد در آن پررنگ‌تر از دنیای واقعی خواهد بود. در پی همین نقش‌آفرینی زنان در تکامل جوامع باید دولت‌ها در پی ایجاد قوانین و مقررات حقوقی و نهادهایی برای حمایت از زنان برآیند. سازمان‌های مختلف ازجمله نهاد زنان ملل متحد نیز باید با اقدامات خود سعی در رفع خشونت و ارتقای جایگاه زنان در جهان و ایجاد برابری جنسیتی داشته باشند.

دولت جمهوری اسلامی ایران در جهان امروز به‌واسطه تحول در مفهوم حوزه‌های علم و تکنولوژی ناگزیر است با پذیرفتن تحولات باب جدیدی را در حوزه مدیریت و نظارت و کنترل بر فضاهای جدید عرصه تکنولوژی بخصوص فضای مجازی و شبکه‌های مجازی بگشاید. درواقع بحث اصلی این است که می‌توان این مدیریت و نظارت را در مقوله قوانین حقوقی و مسئولیت مدنی کاربران صورت داد و مبانی و محتوای فضای مجازی را با ارکان مکتبی و مذهب نظام همسو نمود. همچنین برای نظارت و اجرای قوانین مدنی مبتنی بر

مسئولیت مدنی لازم است مبانی سنتی، مذهبی بر ماهیت فضای جدید مجازی منطبق و کارآمد گردد.

کتاب‌نامه

اسلوین، جیمز (۱۳۸۰)، اینترنت و جامعه، مترجمین: علی گیلوردی و علی رادباوه، تهران: نشر کتابدار.

افضلی، رسول، (۱۳۹۲)، محمدباقر قالیباف و میثم احمدی فیروزجائی؛ «تبیین تحولات مفهوم مرز در فضای سیاسی مجازی»، پژوهش‌های جغرافیای انسانی، دوره ٤٥ ،شماره ۱.

امیر مظاهری، امیر مسعود، ایرانشاهی، اعظم (۱۳۸۸). «چالش‌های تعامل اجتماعی زنان ایرانی در فضای مجازی از دید زنان فعال در فضای مجازی» .مطالعات رسانه‌ای.دوره ۵، شماره ۱ ، پیاپی۸، بهار.

بازرگان، زهرا ناهید صادقی ، غلامعلی لواسانی، مسعود(۱۳۸۲)، «بررسی وضعیت خشونت کلامی در مدارس راهنمایی شهر تهران: مقایسه نظرات دانش آموزان و معلمان»، مجله روانشناسی و علوم تربیتی، دوره ۳۳، ش۲.

بختیاری، افسانه ؛ امیدبخش، نادیا (۱۳۸۲)، «بررسی علل و آثار خشونت علیه زنان در خانواده در مراجعین به مرکز پزشکی قانونی بابل»، مجله پزشکی قانونی، سال نهم ، ش۳۱.

پورنقدی، بهزاد (۱۳۹۱)، «پدافند غیرعامل و بررسی تهدیدات نظم و امنیت در فضای سایبری»، فصلنامهٔ علمی تخصصی دانش انتظامی کردستان، دورهٔ سوم، ش ۱۱، ص ۱۰٤-۸۳.

جوادیان، رضا(۱۳۸۱)، «بررسی پدیده خشونت در خانواده‌های پدر معتاد»، پایان‌نامه کارشناسی ارشد، دانشگاه علوم بهزیستی و توانبخشی.

چلبی، مسعود(۱۳۸۱)، «فضای کنش، ابزار تنظیمی در نظریه‌سازی»، محله انجمن جامعه‌شناسی ایران، دوره چهارم، شماره۱.

حسین‌زاده، علی حسین؛ مومبینی، علی؛ فروتن کیا، شهروز(۱۳۹۱)، «بررسی سرمایه اجتماعی کاربران اینترنتی در فضای سایبر و غیرسایبر(موردمطالعه: دانشجویان دانشگاه شهید چمران اهواز)»، فصلنامه برنامه‌ریزی رفاه و توسعه اجتماعی، دوره ٤،شماره۱۳.

دهخدا، علی اکبر (۱۳۷۳)، لغت نامه، چاپ اول (دورهٔ جدید)، تهران، مؤسسهٔ انتشارات و چاپ دانشگاه تهران.

دهقانی، مریک، ریاضی کرمانی خدیجه (۱۳۸۱)، «بررسی خشونت خانوادگی در خانم‌های باردار و علل مرتبط با آن در بیمارستان‌های شهر کرمان در سال ۱۳۸۰»، (پایان‌نامه دکتری دانشکده پزشکی، دانشگاه علوم پزشکی کرمان).

زندی، محمدرضا (۱۳۹۲)، «تحقیقات مقدماتی در جرایم سایبری»، تهران، انتشارات جنگل.

سازمان جهانی بهداشت(۱۳۸۰)، خشونت علیه زنان، ترجمه شهرام رفیعی فر و سعید پارسی نیا، تهران، تندیس.

سلیمی، احسان(۱۳۹۱)، «بزه دیدگی زنان در فضای سایبر»، (پایان نامه کارشناسی ارشد رشته حقوق دانشگاه تهران).

شاه قاسمی،احسان (۱۳۸۵)، «مروری بر زمینه‌های تأثیر فضای مجازی بر نظریه‌های ارتباطات»، مجله جهانی رسانه، دوره۱، شماره۲.

ضیایی, سید یاسر, شکیب نژاد, احسان (۱۳۹٦)، «قانونگذاری در فضای سایبر: رویکرد حقوق بین‌الملل و حقوق ایران». مجله حقوقی بین المللی, ۳٤ (شماره ۵۷ (پائیز – زمستان), ۲۲۷-۲٤۹.

طاهری جبلی، محسن (۱۳۹۲)، «جرم و کامپیوتر»، مجله حقوقی دادگستری، شماره ۹.

غفاری،حسن (۱۳۸۸)، واکاوی آسیب‌های فرهنگی علیه زنان(قسمت اول): فصلنامه کتاب زنان، ش۲۰.

گیدنز، آنتونی (۱۳۸٦)، جامعه‌شناسی، ترجمه منوچهر صبوری، تهران ، نی.

مکبراید، شن(۱۳۹۲)، یک جهان، چندین صدا (ارتباطات در جامعه امروز و فردا)، مترجم: ایرج پاد، چاپ اول، تهران، انتشارات صداوسیمای جمهوری اسلامی ایران (سروش).

همت‌پور، بهاره؛ رضا، علی محسنی؛ مظاهری، امیرمسعود (۱۳۹٦)، «شناسایی و تبیین جامعه شناختی خشونت علیه زنان در فضای سایبر (مورد مطالعه: زنان٤۵-۲۰ ساله شهر تهران)، پژوهشنامهٔ زنان، پژوهشگاه علوم انسانی و مطالعات فرهنگی، سال هشتم، شمارهٔ چهارم، زمستان، ۱۳۱ – ۱۰۵.

یزدخواستی، بهجت (۱۳۸۷)، «ارزش‌های پدرسالاری و خشونت علیه زنان»، مطالعات زنان، سال ششم، شماره سوم.

Aalipour, Hasan (2011), Informati n Techn logy Penal Law, Tehran, Khorsandi Publishing, First Printing.

Aameli, saeed reza (2011) cyb rspac , Tehran, Publishing Tehran University, First Printing.

Abuzari, Mehrnoush (1395) Criminology of Cyber Crimes, Tehran, Publishing of Mizan, First Printing.

Andrew D. Murray, The Regulation of Cyberspace, Routledge Cavendish, Oxon, 2007, pp. 76-77 & 124

Ang, R. P(2015).. Adolescent cyberbullying: A review of characteristics, prevention, and intervention strategies. Aggression and Violent Behavior, 25, (1).

Beech, A. R., Elliott, I. A., Birgden, A., & Findlater, D. (2008). The internet and child sexual offending: A criminological review. Aggression and Violent Behavior, 13(3).

Bocij, P. (2003). V ct ms of cyberstalking: An exploratory study of harassment perpetrated via the Internet. F rst Monday. Retrieved on 28th June, 2010, from http://131.193.153.231/www/issues/ issue8_10/

BROADHURST, RODERIC AND JAYAWARDENA, KASUN (2011) Online Social Networking and Pedophilia: An Experimental Research “Sting” In: Cyber Criminology: Exploring Internet Crimes And Criminal Behavior, CRC Press.

Cyber violence against women and girl (2014). A report by UN broad band commission. Available on: www.googlebook.com.

darbandi Farahani, Elham (2012), The criminal approach to cybercrime, Master's Thesis for Criminal Law and Criminology, University of Moody.

Frith, Emily (2017) social media and children mental health: a review of the evidence , educational policy institute.

Graham J. H. Smith, Internet Law and Regulation, Sweet and Maxwell, London, 2002, p. 533.

Haji deh abadi, mohammad ali, salami, ehsan (2016) Generalization of cybercrime, collection of articles international conference on: restorative justice & crime prevention, Tehran, publishing mizan. (Persian)

Halder, D. And Jaishankar, K. (2010) Cyber Crime and Victimization of Women: Laws, Rights, and Regulations.

Hershey, PA, USA: IGI Global. Herath, T, rao, H.r upadhyaya, s. (2012) internet crime: how vulnerable are you? Do gender social influence and education play a role in vulnerability? Psychology of cybercrime business science reference.

Hindelang, M. J. Gottfredson, M. R. & Gaffalo, J. (1978). Victims of Personal Crime: An Empirical Foundation for a Theory of Personal Victimization. Cambridge, MA: Allinger.

Holtfreter, k. M. D. reisig, and T.C. Pratt (2008) law self -control, routine activities, and fraud victimization, criminology and Criminal Justice, 46, 1.

Hu Ling, Shaping the Virtual State: Internet Content Regulation in China (1994-2009), University of Hong Kong, Hong Kong, 2011.

James R. Pielemeier, Why General Personal Jurisdiction over Virtual Stores Is a Bad Idea, Quinnipiac Law Review, vol. 27, 2009, p. 671.

Javan jafari, abdoreza, shahideh, farhad (2013) The Role of Women Victims of Sex Crimes, Criminal Law Research, vol.7.

John W. Berry, The World Summit on the Information Society (WSIS): A Global Challenge in the New Millennium, Network of Illinois Learning Resources in Community Colleges, vol. 56, 2006.

Jovan Kurbalija, An Introduction to Internet Governance, Diplo Foundation, Malta, 2014.

Jovan Kurbalija, An Introduction to Internet Governance, DiploFoundation, Malta, 2014, pp. -91-92.

Kafashi, majeid. Pirjalili, Zahra. (2015) Spending Leisure Time in Women in Virtual Space (Tehran, 1394) Journal of Women and Society.SpecialIssue, pp.105-122. (Persian)

Karmen, A. (2007) Crime Victims, an Introduction to Victimology. Wadsworth Publishing.

Kordealivand, ruhdien, mohammadi, Mehdi, mirzaee, mohammad (2017) The typology of cybercrime in computer crime law, The first national cybercrime combating conference, Tehran, cyber police press. (Persian)

Langos, Colette (2013) Cyberbullying, Associated Harm and the Criminal Law (PhD Thesis, University of South Australia, 2013), 55 –60.

Marcum, Catherine, D. (2011), "Adolescent Online Victimization and Constructs of Routine Activities Theory", In: Jaishankar, K. (Ed), Cyber Criminology: Exploring Internet Crimes and Criminal Behavior, CRC Press.

McFarlane, L. & Bocij, P. (2005). An exploration of predatory behaviour in cyberspace: Towards a typology of cyber stalkers. First Monday, 8. Retrieved from http://fi rstmonday.org

McKim, J. (2006, July 12). Pimp pleads guilty to prostituting minor. Orange Count Register.Retrievedfromhttp://www.ocregister.com/ocregister/news/atoz/article 1209170.php

McQuade, S. C. (2006). Und rstanding and managing cybercrime. Boston, MA: Pearson/Allyn and Bacon.

Mitchell, K. Finkelhor, D. & Wolak. J. (2007). Youth internet users at risk for the mo e se ious online sexual solicitations. American Journal of Preventive Medicine, 32.

Mokhta i, Maryam & malek ahmadi, hakimeh, (2017) Pornography and hyper-reality, Culture strategy, vol.38. (Persian)

Monfared, Under the Supervision of Ali Hossein Najafi Ebrahbandadi, Tehran: Size, First Edition.

Mustaine, E. And Tewksbury, R. (1998) Predicting Risks of Larceny Theft Victimization: A Routine Activity Analysis Using Refined Lifestyle Measures, Criminology, Vol. 36.

Petersom.,J.Densley., J. .(2017), Cyber Violence: What do we know and where do we from here?.Aggression and Violent Behavior,No3,. available at ScienceDirect.

Petrocelli, J. (2005). Cyber Stalking, Law & Order, Vol. 53, NO.12.

Rebecca E. Casey, ICANN or ICANN t Represent Internet Users, Faculty of the Virginia Polytechnic Institute and State University, Virginia, 2008, pp. 1-2.

Robert Uerpmann-Wittzack, Principles of International Internet Law, German Law Journal, vol. 11, 2010, pp. 1255-1256.

Sadebeek, liave (2004). Internet ethnography: online and offline, international journal of qualitative method, vol,3, no.2

Sanders, T. (2010). The sex industry, regulation and the internet. In Jewkes, Y. & Yar, M. (Eds.), Handbook of Internet crimes (pp. 302–319). Cullompton, UK: Willan.

SHICK CHOI, KYUNG (2011) Cyber-Routine Activities: Empirical Examination of Online Lifestyle, Digital Guardians, and Computer-Crime Victimization, Cyber Criminology: Exploring Internet Crimes And Criminal Behavior, CRC Press.

Stein Schjølberg and Solange Ghernaouti-Hélie, A Global Protocol on Cybersecurity and Cybercrime, Cybercrimedata, Oslo, 2009, p. i.

Van Wilsem, J. (2011) Worlds Tied Together? Online and Non-Domestic Routine Activities and Their Impact on Digital Threat Victimization, European Journal of Criminology, Sage.

Willard, Nancy (2007), Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats and Distress (Research Press, 2007),

Williams, Matthew (2012), Virtual criminal: Crime, Deviation and Online Regulation, Translated by: Amir Hossein Jalali Farahani and Mahboubeh

Yucedal, B. (2010) Victimization in Cyber Space: An Application of Routine Activity and Lifestyle Exposure Theories. Available In: https://etd.ohiolink.edu/rws_etd/ document/ get/kent1279290984/inline

Zararkh, Ehsan, (2010) Cyber Victims,***of***Journalof Legislation and Strategy, No. 64.