Comparative Studies in Jurisprudence, Law, and Politics

Cybercrime Prevention with Emphasis on Hacktivism

1. Nasrin Emami: PhD Student of Criminal Law and Criminology, Ardabil Branch, Islamic Azad University, Ardabil, Iran
2. Homa Davoodi Garmaroudi*: Assistant Professor, Department of Criminal Law and Criminology, Karaj Branch, Islamic Azad University, Karaj, Iran. Email: homa_nam@yahoo.com (Corresponding Author)
3. Batoul Pakzad: Assistant Professor, Department of Criminal Law and Criminology, North Tehran Branch, Islamic Azad University, Tehran, Iran

ABSTRACT

Addressing hacktivism requires not only attention to substantive and procedural criminal policies but also a thorough examination of the prevention domain. The methods that can be effective in combating a criminal phenomenon are as follows: 1) proactive or interventionist methods, which aim to reduce the harm caused by emerging crimes and require precise inspection and supervisory frameworks; 2) reactive methods, which are concerned with the post-occurrence phase of a criminal phenomenon and how to address it. This study aims to analyze the motivations of individuals engaging in hacktivism and the personality factors related to the perpetrators, existing and possible supervisory measures to combat hacktivism, and potential strategies for preventing it. This article, conducted in a descriptive-analytical manner using a library-based approach, examines hacktivism from the perspective of crime prevention. The findings suggest that hacktivism is often associated with a strong desire to challenge conventional structures, draw attention to misconduct, and instigate significant social changes. Additionally, considering the unique characteristics of cyberspace and its differences from the physical world, it can be concluded that criminal policy to address hacktivism requires adopting differential preventive measures.

Keywords: *hacktivism, cyberspace, cybercrime, prevention, differential preventive measures.*

How to cite: Emami, N., Davoodi Garmaroudi, H., & Pakzad, B. (2023). Cybercrime Prevention with Emphasis on Hacktivism. *Comparative Studies in Jurisprudence, Law, and Politics*, *5*(2), 107-127.

Submit Date: 05 July 2023
Revise Date: 28 August 2023
Accept Date: 08 September 2023
Publish Date: 20 September 2023

پژوهش‌های تطبیقی فقه،
حقوق و سیاست

پیشگیری از جرایم سایبری با تأکید بر هکتیویسم

۱. نسرین امامی: دانشجوی دکتری حقوق‌جزا و جرم‌شناسی، واحد اردبیل، دانشگاه آزاد اسلامی، اردبیل، ایران
۲. هما داودی گرمارودی*: استادیار گروه حقوق‌جزا و جرم‌شناسی، واحد کرج، دانشگاه آزاد اسلامی، کرج، ایران. پست الکترونیک: homa_nam@yahoo.com (نویسنده مسئول)
۳. بتول پاکزاد: استادیار گروه حقوق‌جزا و جرم‌شناسی، واحد تهران شمال، دانشگاه آزاد اسلامی، تهران، ایران

چکیده

مقابله با هکتیویسم علاوه بر توجه به سیاست‌جنایی ماهوی و شکلی، نگاهی دقیق به حوزه پیشگیری را می‌طلبد. روش‌هایی که برای مقابله با یک پدیده‌مجرمانه می‌توانند کارساز باشند عبارتند از: ۱-روش‌های رویارویی‌پیشینی یا کنش‌گرا که هدفشان کاهش آسیب‌های ناشی از جرایم در حال ظهور بوده، نیازمند چهارچوب‌های بازرسی و نظارتی دقیق است. ۲-روش‌های رویارویی‌پسینی یا اقدامات‌واکنشی که مربوط به مرحله بعد از بروز پدیده‌مجرمانه و نحوه برخورد با آن می‌باشد. هدف این پژوهش این است که با بررسی انگیزه‌های افراد در ارتکاب هکتیویسم و عوامل شخصیتی مربوط به مرتکب آن، تدابیر نظارتی موجود و قابل‌تصور برای مقابله با هکتیویسم و راهکارهای ممکن برای پیشگیری از آن را مورد تحلیل قرار دهیم. مقاله حاضر، به صورت توصیفی–تحلیلی و به شیوه کتابخانه‌ای به بررسی هکتیویسم از منظر پیشگیری از جرم، می‌پردازد. یافته‌های پژوهش حاکی از این است که هکتیویسم، غالباً با تمایلی شدید برای به‌چالش‌کشیدن ساختارهای مرسوم، جلب‌توجه به رفتارنادرست و ایجاد تغییرات‌اجتماعی قابل توجه همراه است. از طرفی با توجه به ویژگی‌های خاص فضای‌سایبر و تفاوت‌های آن با دنیای فیزیکی، می‌توان نتیجه گرفت که سیاست‌جنایی برای مقابله با هکتیویسم، نیازمند اتخاذ تدابیر پیشگیرانه افتراقی است.

واژگان کلیدی: هکتیویسم، فضای مجازی، جرایم‌سایبری، پیشگیری، تدابیر پیشگیرانه افتراقی.

نحوه استناددهی: امامی، نسرین.، داودی گرمارودی، هما. و پاکزاد، بتول. (۱۴۰۲). پیشگیری از جرایم سایبری با تأکید بر هکتیویسم. *پژوهش‌های تطبیقی فقه، حقوق و سیاست*، ۵(۲)، ۲۰۷-۱۰۷.

تاریخ ارسال: ۱۴ تیر ۱۴۰۲
تاریخ بازنگری: ۶ شهریور ۱۴۰۲
تاریخ پذیرش: ۱۷ شهریور ۱۴۰۲
تاریخ چاپ: ۲۹ شهریور ۱۴۰۲

مقدمه

با ظهور اینترنت و استفاده از فناوری‌های دیجیتال در فضاهای اجتماعی، سیاسی و اقتصادی، سیاست و سازمان‌دهی اجتماعی دگرگون شده است. تشکل‌های نوینی شکل گرفته، اهداف و ارزش‌های سیاسی جدیدی نیز ابداع شده‌اند. در این وضعیت، پدیده هکتیویسم هم ظهور پیدا کرده است که ریشه در اعماق این تحولات فناورانه اجتماعی-سیاسی دارد و به نظر می‌رسد زاده اجتناب‌ناپذیر این عصر مدرن است که چالش‌های فراوانی را در زمینه قانون و سیاست‌جنایی، برای سیستم‌های حقوقی به همراه آورده است. هکتیویسم پدیده‌ای است که ارتکاب آن با دسترسی به اینترنت و بدون تجهیزات خاصی از هر نقطه جهان، امکان‌پذیر است. هکتیویست‌ها با استفاده از این قدرت و فراگیرشدن اینترنت، تلاش می‌کنند تا از این فناوری، برای انتشار اطلاعات و تبلیغ دیدگاه‌های خود استفاده کنند. بر این مبنا علاوه بر اینکه کشورها باید در راستای پیشگیری از ارتکاب هکتیویسم قواعد ملی نظارتی مناسبی را در خصوص فضای‌سایبری و استفاده سالم از این فضا داشته باشند، لازم است تا همکاری بین‌المللی بیشتری برای پیشگیری و مقابله مؤثر با این پدیده به عنوان یک روش منطقی برای بازدارندگی از ارتکاب هکتیویسم صورت گیرد.

۱- پیشینه پژوهش

زهرا فرهادی‌آلاشتی و عبدالرضا جوان‌جعفری‌بجنوردی (۱۳۹۶, ص. ۹۴) در مقاله خود در خصوص پیشگیری موقعیت‌مدار در فضای‌سایبر، با تأکید بر تأثیر مثبت فضای‌سایبر بر حق جریان آزاد اطلاعات، به تأثیر این ویژگی بر تسهیل ارتکاب بزه برای بزهکاران سایبری اشاره نموده، آن را موجب ورود خسارات فراوان به کاربران شبکه دانسته‌اند. در این مقاله آمده است: «امروزه بزهکاران نیاز به جابه‌جایی فیزیکی ندارند و با استفاده از فضای‌سایبر می‌توانند آماج مناسب خود را هزاران کیلومتر دورتر از خود شناسایی نمایند و خسارات کلانی را بر آن‌ها وارد نمایند. تدابیر موقعیت‌مدار سالب و یا محدود کننده دسترسی، روشی مناسب و سریع برای پیشگیری از بزه‌دیدگی شمار فراوانی از کاربران به حساب می‌آیند و ارتکاب بزه برای بزهکاران احتمالی را دشوار می‌نمایند».

حیدری‌نژاد (۱۳۹۷, ص. ۲۹)، در مقاله‌ای با عنوان «پیشگیری وضعی در جرایم‌سایبری از منظر حقوق‌کیفری ایران وجهان»، پیشگیری وضعی را یکی از اقدامات و تدابیر مهم سیاست‌کیفری در مواجهه با جرایم‌سایبری دانسته است؛ اما بر این مهم نیز تأکید نموده که این نوع پیشگیری با محدودیت‌هایی از جمله نقض موازین حقوق‌بشر روبرو است.

در مقاله‌ای تحت عنوان « فعالیت‌های روتین سایبری: بررسی تجربی سبک زندگی آنلاین، نگهبانان دیجیتال، و قربانی شدن جرایم رایانه‌ای» از «کیونگ شیک چو[1]» که در بخشی از کتاب «جرم شناسی سایبری در بررسی جرایم اینترنتی و رفتار مجرمانه» تدوین «کی جایشانکار[2]» به چاپ رسیده است، آمده است: « ایجاد دیدگاه‌های اجتماعی برای ترویج سبک زندگی آنلاین مناسب و رسیدن به امنیت رایانه‌ای مؤثر، احتمال قربانی شدن برای جرایم رایانه‌ای را کاهش می‌دهد. این مسأله تا حد زیادی توسط برنامه‌های عدالت کیفری پیشگیری از جرم نادیده گرفته شده است. اگرچه تعداد کاربران رایانه روزانه افزایش می‌یابد، برنامه‌های پیشگیری از جرم رایانه‌ای به طور کامل در دسترس کاربران آنلاین نیست. در واقع، برنامه‌های پیشگیری از جرم رایانه‌ای را می‌توان به عنوان برنامه‌های پیشگیری از جرم مبتنی بر مدرسه دسته‌بندی کرد، زیرا

[1]-Kyung-Shick Choi
[2]- K.Jaishankar

برخی از کالج‌ها و دانشگاه‌ها دوره‌های مقدماتی و تخصصی را در زمینه جرایم‌رایانه‌ای و مسائل امنیت اطلاعات برگزار می‌کنند». (K.Jaishankar, 2011, p. 243)

با توجه به اینکه تابه‌حال به زبان فارسی، پژوهشی اختصاصی در خصوص هکتیویسم و پیشگیری از آن انجام نشده است و مطالعات مرسوم حقوق‌کیفری و جرم‌شناسی که در ایران در حوزه جرایم‌سایبری صورت گرفته، اشاره‌ای به هکتیویسم و تفاوت‌های ظریف آن با دیگر جرایم‌سایبری و امکان‌سنجی پیشگیری از آن نداشته‌اند و اندک مطالعات موجود هم که نامی از هکتیویسم برده‌اند، مربوط به حوزه فناوری اطلاعات و ارتباطات می‌باشد، ضرورت توجه به این موضوع به صورت ساختارمند در حوزه پیشگیری از جرم احساس می‌شود.

۲- مبانی نظری پژوهش

۲-۱- تعریف هکتیویسم

هکتیویسم واژه‌ای کلی است که هیچ تعریف مورد توافق جهانی برای آن وجود ندارد. تعاریفی که از هکتیویسم بیان می‌شود، از نظر ذهنی بر اساس رویکرد اشخاص و نوع بینش و انگیزه‌های آن‌ها متفاوت است و گاهی وقت‌ها آن کسی که از دید عده‌ای هکتیویست نامیده می‌شود، از نگاه دیگری هواخواه آزادی و حق است و اقداماتش در این راستا شایسته ستایش می‌باشد.

«سالومون[1]»، هکتیویسم را « ترکیب اعتراض سیاسی مردمی با هک رایانه‌ای » می‌داند.(Solomon, 2017, p. 720)

«دنینگ[2]»، هکتیویسم را پدیده‌ای می‌داند که در آن هک با فعالیت‌سیاسی همگرا می‌شود. (Denning, 2001, p. 263)

«تیم جردن[3]» می‌نویسد: «هکتیویسم یک هک با انگیزه سیاسی است. هکتیویسم کنشگری است! در رگ‌های الکترونیکی که روابط اجتماعی و جهانی ما را در قرن بیست و یکم جان می‌بخشد، آزاد می‌شود.» (Jordan, 2001, p. 119)

«توماس جی‌هالت[4]» هکتیویسم را به چالش کشیدن قوانین جرایم سایبری، با هدف بیان نمادین مخالفت یا تسهیل بیان سیاسی در فضای مجازی عنوان نموده است. (Karagianopoulos, 2018, p. 8)

۲-۲-پیشینه و ادبیات هکتیویسم

داستان ظهور هکتیویسم، همگرایی دو مفهوم هک و کنش‌گری را ترسیم می‌کند. اصطلاح «هک»، برای اولین بار در اواخر دهه ۱۹۵۰در موسسه فناوری ماساچوست[5] استفاده شد. متخصصان کامپیوتر در ام‌آی‌تی، چیزی را ایجاد کردند که آن‌ها را «هک» یا «میان‌برهای برنامه‌نویسی» می‌نامیدند؛ تا بتوانند وظایف محاسباتی خود را با سرعت بیشتری انجام دهند...این افراد خلاق در نهایت به عنوان « هکر» (به معنای مثبت) شناخته شدند. معنای اصلی « هک »، فقط احساس لذت در خود فرآیند کار است. (Li, 2013, p. 136)

[1]-solomon
[2]-Dening
[3]-Tim Jordan
[4]-Thomas J. Holt
[5]-Massachusetts Institute of Technology(MIT)

هک کردن در معنای امروزی، در دهه ۱۹۷۰ با دستکاری شبکه سیستم‌های ارتباطی تلفن، که به عنوان «فریکینگ[۱]» نیز شناخته می‌شود، آغاز شد.« جان دریپر[۲]» معروف‌ترین فریکر[۳] دهه هفتاد بود که به دلیل دستکاری شبکه و سیستم‌های ارتباطی تلفنی دستگیر شد. دریپر در نهایت به همکاری با بنیانگذاران اپل، «استیو وزنیانگیک[۴]» و «استیو جابز[۵]»، ادامه داد. (Warren V. Held, 2012, p. 5)

در حال حاضر، پرکارترین و محبوب‌ترین گروه هکتیویست، « آنانیموس»[۶] است. آنانیموس، سابقه طولانی دارد. این گروه که در سال ۲۰۰۳...بدون رهبری متمرکز تشکیل شد، با این فرض عمل می‌کند که هر کسی می‌تواند به سادگی، با انجام اعمالی به نام آن، عضوی از آنانیموس باشد. (Warren V. Held, 2012, p. 29) از دیگر گروه‌های هکتیویستی معروف می‌توان به ویکی‌لیکس[۷]،دارک‌مارکت[۸]،گوست نت[۹]،لولز سکیوریتی[۱۰]،رد هک[۱۱]، گروه زئوس اوکراین[۱۲] و گروه عدالت علی اشاره کرد.

۳- تعریف پیشگیری

«پیشگیری» در لغت به معنای جلوگیری‌کردن، مانع‌شدن، مانع سرایت شدن آمده است. در تعریف گسن[۱۳] پیشگیری « مجموعه اقداماتی خارج از نظام کیفری است که هدف غایی آن منحصراً یا به صورت جزئی محدودکردن دامنه ارتکاب جرم، غیرممکن کردن، مشکل کردن و کم کردن احتمال وقوع جرم باشد. » (جعفری, ۱۳۸۷, ص. ۱۴۷)

موریس کوسن[۱۴]« جرم‌شناس کانادایی»، در تعریف پیشگیری گفته است: « مجموعه اقدام‌ها و تدابیر غیرقهرآمیز که با هدف خاص مهار بزهکاری، کاهش احتمال جرم و کاهش وخامت جرم پیرامون علل جرایم اتخاذ می‌شود. » (جعفری, ۱۳۸۷, ص. ۱۴۷)

ماده ۱ قانون پیشگیری از وقوع جرم « پیش‌بینی، شناسایی و ارزیابی خطر وقوع جرم و اتخاذ تدابیر و اقدامات لازم برای از میان بردن یا کاهش آن[۱۵] »را به عنوان پیشگیری دانسته است.

۳-۱- مراحل پیشگیری

دکتر نجفی‌ابرندآبادی مراحل پیشگیری از جرم را به عنوان یک سلسله عملیات فکری، علمی و مطالعاتی تحت عنوان امکان‌سنجی معرفی نموده، این عملیات را شامل هفت مرحله دانسته‌اند :

---

[1]-phreaking
[2]-John Draper
[۳] - کسانی که از فناوری یا شماره‌های کارت اعتباری تلفن استفاده می‌کنند تا برای مدت طولانی از تماس‌های از راه دور به صورت رایگان استفاده کنند.
[4]- Steve Wozniak
[5]- Steve Jobs
[6]- Anonymous
[7] -WikiLeaks
[8]- Dark market
[9]- Ghost Net
[10]- Lulz security
[11]- Red hack
[12] -Zeus group of Ukraine
[13]- Gossin
[14]- Morris Cosen
[۱]-مصوب ۱۳۹۴/۰۹/۱۷ مجلس شورای اسلامی

۱-تحلیل منسجم ویژگی‌های یک جرم؛

۲-انتخاب آماج پیشگیری؛

۳-توجیه جرم‌شناختی طرح پیشگیری؛

۴-تعیین یک هدف واقعی به جای یک هدف کلی برای پیشگیری؛

۵-انتخاب نوع پیشگیری؛

۶-تعیین مقام و مرجع صالح برای پیشگیری؛

۷- ارزیابی عملی پیشگیری.

۳-۲- انواع تدابیر پیشگیرانه

انتخاب نوع پیشگیری در فرایند پیشگیری از جرم نقشی اساسی را در رسیدن به هدف بر عهده دارد.

الگوی سه‌گانه پیشگیری از جرم در قالب پیشگیری اولیه، پیشگیری ثانویه و پیشگیری سومین، در ارتباط مستقیم با زمان و نحوه مداخله جهت پیشگیری از جرم می‌باشد.

در پیشگیری اولیه تلاش بر این است که به طور کلی افراد به سمت ارتکاب جرم نروند. در این راستا تمام اشخاص و اموالی که ممکن است هدف جرم واقع شوند در مرکز توجه قرار دارند. در واقع پیشگیری اولیه، مجموعه تدابیر و اقداماتی را که با هدف شناسایی و تغییر شرایط و اوضاع و احوال جرم‌زای محیط فیزیکی و اجتماعی اعمال می‌شود، در بر می‌گیرد. (معظمی گودرزی, ۱۴۰۱, ص. ۱۷۱)

در پیشگیری ثانویه، حمایت از افراد در آستانه خطر خاص بزه‌دیدگی مدنظر است. علاوه بر آن مکان‌هایی هم که در خطر صحنه‌جرم‌شدن می‌باشند مورد توجه هستند. در این نوع پیشگیری، تلاش برای یافتن تدابیر مناسب و زودهنگام برای جلوگیری از ار تکاب بزه است.

در پیشگیری سومین، تلاش برای یافتن روش‌های اصلاح و درمان و جلوگیری از تکرار جرم توسط محکومان سابق، جلوگیری از بزه‌دیدگی مجدد بزه‌دیدگان سابق و جلوگیری از ارتکاب دوباره جرم در محل‌هایی است که پیشتر صحنه جرم واقع شده‌اند.

در حوزه پیشگیری از جرم تقسیم‌بندی دیگری نیز در قالب پیشگیری‌کنشی یا غیرکیفری[1] و پیشگیری واکنشی یا کیفری[2] مطرح می‌شود. به عبارتی، پیشگیری از جرم دو ماهیت عمده دارد که یکی در حقوق‌کیفری مطرح می‌شود و دیگری در جرم‌شناسی. در حقوق‌کیفری، پیشگیری از وقوع جرم، یک هدف است که با اعمال ضمانت‌اجراهای‌کیفری، دنبال می‌شود؛ ولی در جرم‌شناسی، پیشگیری از وقوع جرم یک روش یا تدبیر است که برای خنثی‌سازی انجام جرم یا از بین بردن فرصت یا زمینه آن به کار گرفته می‌شود. به جهت این دو ماهیت مهم پیشگیری از وقوع جرم، این نهاد یکی از کلیدی‌ترین مفاهیم سیاست‌جنایی تلقی می‌شود که هم در حقوق‌جزا محوریت دارد و هم در جرم‌شناسی‌کاربردی. (الهی منش, ۱۴۰۱, ص. ۱۹۶)

۳-۳- عناصر پیشگیری

کنترل موفقیت‌آمیز جرم، بستگی به راهبردهای پیشگیری از جرم بر اساس شناخت عمیق جرم و ویژگی‌های آن دارد.

پیشگیری چهار عنصر دارد که عبارتند از:

[1]- Non Penal Prevention
[2]- Penal Prevention

الف-قهرآمیز نبودن: به این معنا که تدابیر پیشگیری تدابیر و اقداماتی جدا از اصلاح و درمان و اقدامات کیفری و قهرآمیز حقوق جزا هستند و برای اعمال این تدابیر رضایت ذی‌نفع لازم و ضروری است.این اقدامات یا نسبت به خود فرد در نظر گرفته می‌شود یا نسبت به وضعیتی که فرد در آن قرار دارد.

ب-اختصاصی بودن: تدابیر پیشگیرانه اقداماتی هستند که غایت و هدف اصلی آن‌ها پیشگیری است و انجام این اقدامات به منظور پیشگیری صورت می‌پذیرد و نمی‌توان به اقداماتی که در نتیجه انجام آن‌ها در کنار هدف اصلی، احتمال پیشگیری هم باشد نام تدابیر پیشگیرانه نهاد.

ج-کم کردن آثار ارتکاب جرم: هدف تدابیر پیشگیرانه این است که جلوی روند گذار از تفکر مجرمانه به فعل مجرمانه را بگیرد؛ در این میان اگرچه ممکن است با اقدامات پیشگیرانه نتوان به طور کامل جلوی ارتکاب جرم را گرفت، اما حداقل می‌توان با تدابیر پیشگیرانه باعث کاهش آثار زیان‌بار مادی و معنوی جرم شد.

د-شناسایی عوامل خطر: برای اثربخشی اقدامات پیشگیرانه، باید عوامل خطر که به طور کلی افراد را مستعد ارتکاب جرم می‌کند یا در مورد برخی افراد به طور خاص آن‌ها را مستعد ارتکاب جرم می‌کند، شناسایی شود. عواملی مثل ترک‌تحصیل و رفت و آمد در محیط‌های جرم‌زا.

۴- علت شناسی هکتیویسم

علل و عواملی که سبب بروز جرایم می‌شوند متفاوتند و بسته به مؤلفه‌های مختلف از یکدیگر مجزا می‌شوند. سه‌ضلعی جرم از بزهکار، بزه‌دیده و موقعیت جرم تشکیل شده است. آنچه که در خصوص این مثلث در جرایم‌سایبری و پدیده هکتیویسم خودنمایی می‌کند این است که به لحاظ ویژگی‌های خاص فضای‌سایبری تشخیص بزهکار و بزه‌دیده و مکان و زمان ارتکاب جرم به راحتی امکان‌پذیر نیست.

به طور کلی در ارتکاب تمام جرایم علت‌های مرتبط با بزهکار، شامل استعداد مجرمیت، آمادگی برای بزهکاری و نداشتن مهارت خویشتن‌داری و پرهیز از ارتکاب جرم، داشتن امکانات لازم برای ارتکاب جرم و داشتن مهارت ارتکاب جرم و علل مربوط به بزه‌دیده، که زمینه‌ساز ارتکاب بزه توسط بزهکار است، شامل استعداد بزه‌دیدگی، وجود آماج جرم مناسب و نبود مهارت‌های مدیریت خطر می‌باشند. علت‌های مرتبط با ضلع سوم این مثلث یعنی موقعیت جرم نیز عبارتند از تقارن زمانی و مکانی بزهکار و بزه‌دیده، حضور عوامل مشوق جرم و غیبت عوامل بازدارنده جرم.(برگرفته از (محمدنسل, ۱۳۸۹, ص. ۳۲۳)) بررسی تأثیر عوامل مربوط به هر یک از اضلاع این مثلث در ارتکاب جرم، می‌تواند در یافتن روش‌های کاربردی برای پیشگیری از ارتکاب جرم راهگشا باشد.

« جایشانکار» به عنوان بنیانگذار رشته دانشگاهی جرم‌شناسی سایبری، در مطالعات خود بر دلایل پیدایش جرم در فضای‌مجازی و تأثیر آن بر محیط فیزیکی (به ویژه بر کاربران فضای‌مجازی) تمرکز دارد. این شاخه جدید جرم‌شناسی، بر پیش‌فرض‌های اساسی زیر تکیه دارد که جایشانکار از آن به عنوان « نظریه گذارفضا » یاد می‌کند:

الف) افرادی که تمایلشان به ارتکاب جرم و جنایت در محیط فیزیکی را در خود سرکوب می‌کنند، تمایل دارند در فضای مجازی، رفتار انحرافی از خود نشان دهند.

ب) افراد به دلیل انعطاف‌پذیری هویت، ناشناس بودن و فقدان عوامل بازدارنده در فضای‌سایبری، قادر به ارتکاب جرایم در این فضا هستند.

ج) رفتار مجرمانه از محیط فیزیکی به فضای مجازی منتقل شده است.

د) مرتکبین به دلیل ویژگی‌های فضای مجازی به راحتی می‌توانند فرار کنند یا پنهان شوند.

ه) افرادی که در محیط فیزیکیِ خود مرتکب رفتار مجرمانه می‌شوند، اغلب در فضای مجازی گروه‌های مجرمانه تشکیل می‌دهند.

و) برخی آشنایی‌ها سبب تشکیل گروه‌هایی برای انجام جرایم‌سایبری می‌شوند.

ز) افرادِ برخاسته از جوامع بسته، بیشتر در فضای مجازی مرتکب جرم می‌شوند.

ح) تضاد بین هنجارها و ارزش‌های محیط فیزیکی و ارزش‌های فضای‌سایبری، اغلب منجر به جرایم‌سایبری می‌شود.

نظریه گذار فضا، توضیحی در مورد ماهیت رفتار افرادی است که رفتار منطبق و ناسازگار خود را در فضای فیزیکی و فضای مجازی بروز می‌دهند. انتقال فضا، شامل حرکت افراد از یک فضا به فضای دیگر است. به عنوان مثال از فضای فیزیکی به فضای مجازی و بالعکس.نظریه گذار فضا استدلال می‌کند که افراد وقتی از فضایی به فضای دیگر می‌روند، متفاوت رفتار می‌کنند. (Mesko, 2018, p. 191)

۴-۱- نقش انگیزه در هکتیویسم

اصطلاح « هکتیویست »، شخصی را توصیف می‌کند که هک رایانه را به منظور بیان اعتراض سیاسی انجام می‌دهد (Arquilla, 2001, p. 241)؛روش‌های مورد استفاده در گروه‌های هکتیویست بسته به اهداف و انگیزه‌های آن‌ها متنوع است. هکتیویسم پدیده‌ای است که نشأت گرفته از اجتماع و وضعیت آن است و با اعتقادات و ارزش‌های مورد پذیرش افراد سر و کار دارد و با هدف حمایت از این اعتقادات یا باورهای فردی-جمعی صورت می‌پذیرد. گاه تحریکاتی که از جانب اشخاص یا حتی دستگاه‌های دولتی نسبت به برخی باورها و اعتقادات افراد صورت می‌گیرد و گاهی اتخاذ سیاست‌های اقتصادی و اجتماعی خاص توسط دولت می‌تواند زمینه‌ساز حرکات اعتراضی هکتیویست‌ها شود و این اعتراض را با انتشار بیانیه در رسانه‌های گروهی، هک سرویس‌های اطلاعاتی دولت و مواردی از این قبیل پاسخ دهند. در واقع، هرگونه اختلافات مذهبی، اختلافات عقیدتی، تبعیض نژادی و مواردی از این دست می‌تواند هکتیویست‌ها را تحریک به حمله به سایت‌ها و زیر ساخت‌های حیاتی یک دولت کند. در حقوق‌کیفری انگیزه معمولاً اهمیتی در ارتکاب جرم ندارد و آنچه که بیشتر مدنظر است قصد مجرمانه و سوءنیت است. البته انگیزه شرافتمندانه در برخی موارد می‌تواند عاملی برای تخفیف مجازات باشد؛ اما برعکس، این عنصر در علت‌شناسی جرم و پیشگیری از بزهکاری بسیار حائز اهمیت است.

انگیزه« مقصودی است که فرد به‌منظور آن دست به ارتکاب جرم می‌زند.» (محمد کوره پز, ۱۳۹۳, ص. ۱۴۱) برخی از جرم‌شناسان معتقدند برای اینکه یک جرم بر اساس مبانی جرم‌شناختی یعنی علت‌شناسی جرم محقق شود، باید سه عنصر انگیزه، فرصت و ابزار با یکدیگر جمع شوند. انگیزه، با قصد مجرمانه متفاوت است و در واقع هدف ارتکاب آن را تشکیل می‌دهد. بنابراین اگر انگیزه مجرمانه‌ای در فرد ایجاد نشود، قصد مجرمانه نیز در او شکل نخواهد گرفت. به بیان دیگر، انگیزه بر قصد مقدم است و به این دلیل چنانچه بتوان انگیزه‌های مجرمانه را خنثی کرد، جرمی ارتکاب نخواهد یافت. ازا ین رو با توجه به اهمیت این عنصر، از انگیزه به عنوان قاعده مثلث جرم یاد می‌شود. (باقری اصل, ۱۳۸۷, ص. ۱۳۱)

اینترنت، وسیله‌ای است که توسط آن با دسترسی به اطلاعات و خدمات‌دولتی، به صورت آنلاین در فعالیت‌های زندگی روزمره درگیر هستیم. بسیاری از ما فارغ از نژاد و جنسیت و مذهب از طریق اینترنت به سایر رسانه‌ها از همه نوع دسترسی پیدا کرده، اخبار و اطلاعات را جستجو و منتشر می‌کنیم. با استفاده از این تبادل دانش و تسهیل فعالیت است که بسیاری دیگر از حقوق اساسی بشر، به طور فزاینده‌ای حمایت می‌شوند. با بهره‌گیری از اینترنت، آزادی عقیده و بیان خود را تمرین می‌کنیم ودر زمان انتخابات، سیر این روند سیاسی یا اخبار و اطلاعات مربوط به آن را پیگیری می‌کنیم و با آن، به سمت مشارکت سیاسی می‌رویم.

در حوزه هکتیویسم، که شامل استفاده از ابزارها و تکنیک‌های هک با ماهیت مخرب و برای اهداف سیاسی است، اینترنت عمدتاً برای جلب توجه به یک علت که همان علت اعتراض‌سیاسی است عمل می‌کند؛ چرا که چنین حوادثی به طور مرتب توسط رسانه‌های خبری گزارش می‌شود و به این ترتیب، هکتیویست‌ها احساس قدرت می‌کنند. به عنوان مثال آن‌ها می‌توانند رایانه‌های دولتی را کنترل کنند و توجه رسانه‌ها را به خود جلب کنند. در این میان، حتی اگر در تغییر سیاست موفق نباشند، حداقل نتیجه‌ای که به دست می‌آورند این است که می‌توانند برای خود شهرتی کسب کنند.

بر اساس ماهیت فعالیت‌های هکتیویستی، باید راهی برای طبقه بندی یا شناسایی انگیزه مرتکبین این فعالیت‌ها وجود داشته باشد. از آنجا که جنبش‌های هکتیویستی بسیار پراکنده هستند و افراد زیادی مجموعه هکتیویست را تشکیل می‌دهند که هر یک با فلسفه خاص خود به گروهشان پایبند هستند، لذا درک انگیزه این گروه‌ها به دلیل گستردگی آن کار سختی است؛ اما شناخت انگیزه‌های مربوط به هکتیویسم به ما امکان می‌دهد تا درک کلی بهتری از اینکه چه اعمالی و چگونه در فضای‌سایبری در قالب هکتیویسم انجام می‌شود و آیا راهی برای پیشگیری از آن‌ها وجود دارد یا خیر، داشته باشیم، که این امر می‌تواند مستقیماً با تأمین منافع حیاتی مربوط به امنیت ملی در سراسر جهان در ارتباط باشد. در واقع با شناخت علل وقوع بزه بحث ارزیابی و نظارت نمود بیشتری می‌یابد. علل وقوع بزه به ما نشان می‌دهد که چه تدابیری برای بازرسی و نظارت بر فضای سایبر قابل انجام است و پیشگیری از جرم، در چه زمان‌ها و مکان‌هایی و توسط چه افراد و نهادهایی و نسبت به کدام آماج باید اجرا و اعمال شود.

اجرای تدابیر پیشگیرانه یعنی انجام اقدامات مناسب در خصوص علل جرم به روشی کارآمد، اثربخش، پایدار و قابل قبول که نیازهای معین و اولویت‌دار بزه‌دیدگان و جامعه را مورد هدف قرار دهد. (محمدنسل, ۱۳۸۹, ص. ۳۲۵)

۲-۴- نقش علل فردی در هکتیویسم

عوامل فردی مهیاکننده بزهکاری به عواملی گفته می‌شود که آمادگی لازم برای ارتکاب بزه را در فرد فراهم می‌کنند. به همین دلیل می‌توان از آن‌ها به عنوان عوامل تواناساز یاد کرد (امیریان فارسانی, ۱۳۹۹, ص. ۱۹۷)علل فردی مختلفی می‌توانند در ارتکاب هکتیویسم تأثیرگذار باشند که از میان آن‌ها دو عامل جنسیت و سن را مورد بررسی قرار می‌دهیم:

۴-۲-۱-جنسیت در ارتکاب هکتیویسم

در دنیای امروز، گستردگی بزهکاری میان مردان و زنان به شکل برابر نیست. هر چند امروزه با افزایش مشارکت زنان در جامعه، نرخ بزهکاری زنان نیز بیشتر شده است، اما هنوز در بسیاری از جرایم، رقم بزهکاری مردان نسبت به زنان بیشتر است. (محمد کوره پز, ۱۳۹۳, ص. ۱۱۷) اخبار روز دنیا مملو از داستان‌هایی در مورد هک است. از گروه‌های هکتیویستی که اعضای آن ناشناخته است تا افرادی که به تنهایی قدم در این راه نهاده‌اند. گزارش‌هایی درباره « جرمی‌هاموند[1]»، عضو «لولز سکیوریتی»، یا « ادوارد اسنودن[2]»، پیمانکار سابق آژانس امنیت ملی، به این تصور که همه هکرها مردان جوان، سفیدپوست و طبقه متوسط هستند کمک کرده است. این نشان‌دهنده یک تصویر مغرضانه و یک روایت یک طرفه از جامعه است. با اذعان به وجود اکثریت آماری در خصوص هکرهای مرد و تعداد اندک زنان درگیر در هک و فناوری در مقایسه با مردان، پیوندهای بین جنسیت و هکتیویسم مسأله‌ای است که نیاز به بررسی دارد. به نظر می‌رسد صحنه هکتیویسم به دلیل انگیزه اجتماعی

[1]- Jeremy Hammond
[2]- Edward Snowden

و سیاسی‌اش برای یک تحلیل جنسیت محور مناسب می‌باشد. عدم حضور چشمگیر زنان چه در جامعه و چه در ادبیات موجود در خصوص هکتیویسم و نادیده گرفتن سهم زنان در این شکل از کنشگری، سوگیری جنسیتی را مطرح و تقویت می‌کند. لئونی ماریا تانکزر[1]، محقق فوق دکتری امنیت سایبری، در مقاله‌ای در سال ۲۰۱۵ با نمونه‌ای متشکل از پنج زن و پنج مرد، یک تحلیل گفتمانی از جوامع هکتیویست انجام داد. وی معتقد بود که تحلیل جنسیتی به ویژه برای جامعه‌ای که بر ایجاد تغییرات اجتماعی و سیاسی متمرکز است ضروری است. اگرچه حجم نمونه تانکزر کوچک است، اما او اولین کسی است که به مطالعه ارتباط مستقیم بین جنسیت و هکتیویسم پرداخت. او در مصاحبه با سوژه‌هایش، چهار الگوی گفتمان را تشخیص داد. مهم‌تر از همه، او گفتمان غافل مردانه را در میان مردانی که مورد بررسی قرار داد شناسایی کرد؛ به‌این‌ترتیب که در آن مردان به طور کامل، جنسیت را در ارتکاب هکتیویسم نادیده گرفتند. نپذیرفتن جنسیت گرایی و هویت مردانه در جامعه هکتیویست که عمدتاً مرد هستند، به خودی خود نوعی تبعیض جنسیتی است و نشان می‌دهد که به وجود جنس زن در ارتکاب هکتیویسم، به عنوان یک موضوع غیرمعمول نگاه می‌کنند. هکرهای زن این نگرش را از طریق گفتمان‌های مقاومت زنانه رد می‌کنند. آن‌ها در این گفتمان یا به صورت فعالانه بر هویت خود به عنوان زن و هکتیویست تأکید و با تبعیض جنسیتی در جامعه مبارزه می‌کنند، یا هنگامی که با این تبعیض یا نادیده گرفتن زنان مواجه می‌شوند، به صورت منفعل با احساس طرد شدن و توجیه هویت هکتیویستی دست و پنجه نرم می‌کنند که در این حال، مردان با یک گفتمان انتقام‌جویانه از خود دفاع می‌کنند. (Curcelli, 2017, p. 21)

۴-۲-۲- سن در ارتکاب هکتیویسم

گسترش روزافزون استفاده از گوشی‌های تلفن همراهِ مجهز به اینترنت و تمایل افراد از پیر و جوان به ورود در فضای مجازی به دلایل مختلف از جمله جذابیت‌های این فضا و سهل بودن استفاده از آن، باعث شده است که ارتکاب رفتارهای مجرمانه در فضای مجازی، فقط مختص افراد یا گروه‌های خاصی نباشد و افراد مختلف بتوانند با انگیزه‌های متفاوت، به ارتکاب رفتارهای مجرمانه در این فضا بپردازند. توجه به تاریخچه هکتیویسم و مرتکبین آن نشان می‌دهد که حتی در مواردی بزرگترین هک‌های تاریخ، توسط نوجوانان کنجکاو و یا جوانانی که تمایل به خود نمایی و جلب توجه داشته‌اند صورت گرفته است. برای مثال می‌توان به قضیه شبکه‌های رایانه‌ای «تله نت[2]» و «دیتاپک[3]» اشاره کرد. استفاده‌کنندگان از این دو شبکه، ظرف مدت یک هفته شکایت‌هایی به مسئولان شبکه تسلیم کردند و معترض شدند که افرادی به صورت غیرمجاز به سیستم آن‌ها دست یافته و مشکلاتی ایجاد کرده‌اند. چون سوءاستفاده الکترونیکی یاد شده وضع فراملّی یافت، پلیس کانادا با همکاری پلیس آمریکا از طریق خطوط الکترونیکی شبکه‌ها، چهار نوجوان ۱۳ ساله مدرسه دالتون نیویورک را دستگیر کرد. (پاکزاد, ۱۳۸۸, ص. ۱۸) در موارد بسیاری هم افراد میانسال و مسن، رهبری گروه‌های بزرگ هکتیویستی را بر عهده داشته‌اند. در این بین تفاوتی که میان این مرتکبین وجود دارد از جهت دارا بودن مسئولیت کیفری و بحث انگیزه، جلوه گر می‌شود.

۴-۳- علل اجتماعی

معمولاً آنچه که در بررسی علل‌اجتماعی ارتکاب جرایم بیشتر خودنمایی می‌کند فرهنگ، خانواده، گروه همسالان، اقتصاد، رسانه‌های‌جمعی و محیط‌اجتماعی می‌باشد. برابر آموزه‌های جرم‌شناسی، ارتکاب جرم پاسخی به یک نیاز و واکنشی به یک نقص و فقدان است.

[1]- Leonie Maria Tankzer
[2]- Telenet
[3]- Datapack

شرایط نامساعدی که به لحاظ سیاست‌های خاص دولت‌ها از نظر اقتصادی و اجتماعی، بر مردم تحمیل می‌شود، هم می‌تواند منتهی به ارتکاب جرایم سنتی شود و هم می‌تواند زمینه‌ساز اعتراضات هکتیویستی و سایر انواع جرایم‌سایبری باشد.

عصر حاضر، عصر حاکمیت اقتصاد است. به اعتقاد « مرتون[1]»، پول خدای دنیای امروز است. در دنیایی که پول حرف اول را می‌زند و یکی از مظاهر جهانی‌شدن، گشوده شدن مرزهای کشورها به روی سرمایه‌داران است، یکی از نتایج حاکمیت نظام سرمایه‌داری، عقب‌نشینی دولت‌ها از ارائه خدمات اجتماعی است و یکی از نتایج این عقب‌نشینی فقر است. به عقیده رابرت مرتون، همین فقر و تورم اقتصادی فشاری را بر افراد تحمیل می‌کند که با ارتکاب جرم به دنبال راه حلی جهت رهایی از عوامل این فشار هستند.

فقراقتصادی یا جنون‌ثروت، ممکن است فرد را تحریک به استفاده از ابزارهای نامشروع جهت کسب ثروت نماید و در این راستا از فضای مجازی به عنوان محیطی امن استفاده کرده و با نشستن در خانه و استفاده از یک رایانه و مقداری تخصص سیستم‌های اقتصادی را مختل می‌نماید. (وروایی, ۱۳۹۰, ص. ۱۱)

از سوی دیگر، طبق نظریه معاشرت ترجیحی « ساترلند»[2]، افراد در معاشرت با دوستان و آشنایان و بالاخص کسانی که برای وی اهمیت زیادی دارند، یک سری اعمال و اقدامات را فراگرفته و با تجزیه و تحلیل آن‌ها برخی از این اقدامات را ترجیح داده و سعی در تقلید از این الگوها می‌نماید. بنابراین، نوع گروه همسالانی که فرد در آن عضویت دارد و هنجارها و ارزش‌های حاکم بر این گروه، تأثیر بسزایی در افکار و رفتار اعضای خود خواهد گذاشت. (وروایی, ۱۳۹۰, ص. ۱۲)

۵- بررسی امکان پیشگیری از وقوع هکتیویسم

هکتیویسم، پدیده‌ای نسبتاً نوظهور است که از ابزارهای نرم‌افزاری برای تسهیل بیان نمادین اعتراضات سیاسی آنلاین استفاده می‌کند و از اشکال مختلفی از جمله حملات انکار سرویس،تحصن‌های مجازی،تغییر مسیر سایت[3]،دسترسی به کامپیوتر یا شبکه و سرقت داده‌ها،تخریب‌های سایت، تقلیدهای سایت، ویروس‌ها و بدافزارها برای رسیدن به اهداف خود بهره می‌برد. البته با پیشرفت تکنولوژی، این ابزارها نیز روز به روز در حال تجهیز و تغییر هستند. حداقل در ظاهر، ماهیت غیرقانونی هکتیویسم، باعث بروز بحث‌های گسترده در رابطه با مضرات احتمالی آن برای شبکه‌ها و منافع اپراتورها و کاربران شبکه‌ها شده است. تداوم وجود هکتیویسم به عنوان یک رویه سیاسی به موازات توسعه و شکل‌گیری فضای مجازی، بازار بحث و جدل پیرامون نحوه برخورد و نظارت نسبت به این فعالیت‌ها و پیشگیری از ارتکاب آن را داغ نموده است. در این میان قبل از بررسی و جستجو برای یافتن تدابیر پیشگیرانه،ابتدا باید این مطلب روشن شود که آیا امکان اتخاذ تدابیر پیشگیرانه در خصوص هکتیویسم وجود دارد یا خیر؟

درک و توضیح هکتیویسم، به عنوان رفتاری که در فضای‌سایبر ارتکاب می‌یابد، بسیار دشوارتر از جرایم سنتی است. علیرغم اینکه تخمین‌ها از شیوع جرایم‌سایبری و تهدیدی که برای کاربران فضای مجازی ایجاد می‌کند زیاد است، اما به دلیل ماهیت نامشهود عواقب آن، پیچیده بودن فناوری به کار رفته توسط عاملان آن و ناکافی بودن گزارش توسط قربانیان، میزان واقعی جرایم‌سایبری ناشناخته باقی مانده است؛ به این معنی که رقم تاریک جرایم‌سایبری بسیار زیاد است. البته در مورد هکتیویسم این رقم کمتر است. چرا که اغلب هکتیویست‌ها- خصوصاً زمانی که در اعتراض به سیاست‌های اتخاذی دولت دست به این کار می‌زنند- تمایل دارند تا اقدامات خود را به گوش جهانیان برسانند و حتی اگر

[1] -Merton
[2]- Sutherland
[3]- Site redirects

قربانیان در تلاش برای پنهان کردن این موضوع باشند، خود هکتیویست‌ها دست به افشاگری می‌زنند؛کما اینکه، در اصل هدف بسیاری از اقدامات هکتیویستی نیز افشاگری می‌باشد. مثل افشاگری‌هایی که توسط ویکی‌لیکس انجام شده است.

عرصه فضای سایبر، پهنه‌ای است که اشخاص بدون داشتن شناختی از یکدیگر، به‌راحتی و بدون نیاز به تخصص خاصی، از کودک و پیر و جوان در آن می‌تازند و جولان می‌دهند. امروزه از طریق فضای سایبر به راحتی می‌توان با تمام نقاط جهان ارتباط برقرار کرد. به موازات گستردگی این بستر و با توجه به ویژگی‌های بی‌مرز بودن، دسترسی سریع و راحت، غیرقابل‌لمس بودن، تخصصی بودن و پیچیدگی فضای سایبر مشکلات و آسیب‌های بسیاری نیز درترسیم الگوهای خطر جرایم‌سایبری جلوه‌گر می‌شود. بروز پدیده‌ای همچون هکتیویسم معمولاً مرزهای جغرافیایی را درمی‌نوردد و افراد بسیاری درگیر آن می‌شوند. در عصری که تکنولوژی و فناوری هر لحظه در حال پیشرفت است و بشر هیچ حد و مرزی برای خود قائل نیست، به طوری که حتی حاضر است زیر چکمه‌های پیشرفت و تمدن، انسانیت و نوع‌دوستی را لگدمال کند، ترسیم الگوی خطر هکتیویسم و تسلط بر بستر وسیعی که محل حدوث این پدیده است و تدارک تدابیر پیشگیرانه برای آن، به راحتی امکان‌پذیر نیست و این امر بسیار متفاوت با مسأله‌یابی جرایم سنتی می‌باشد.

در دیدگاه مارک آنسل[1]، سیاست‌جنایی، نخست، علاوه بر «جرم» که یک مفهوم قانونی است، به «انحراف» (کژروی)که یک مفهوم اجتماعی است نیز می‌پردازد؛ دوم اینکه، علاوه بر سرکوب و مجازات بزهکاری، به پیشگیری از آن توجه دارد؛ سوم اینکه، علاوه بر اقدام‌های جزایی و نظام کیفری، بر تدبیرها و نظام‌های اجتماعی، فرهنگی، اخلاقی و...و نیز بر همه آنچه که در بهداشت و پیشگیری اجتماعی از بزهکاری مؤثر است، تکیه می‌کند. (صبح خیز, ۱۴۰۰, ص. ۱۳۰)

مستند به ماده ۲ قانون مجازات اسلامی، زمانی می‌توان گفت جرمی ارتکاب یافته است که رفتاری به وقوع بپیوندد که قانونگذار برای آن رفتار چه در قالب فعل باشد چه ترک فعل، مجازات تعیین کرده باشد. از سوی دیگر می‌دانیم که زمانی قانونگذار رفتاری را مستوجب مجازات می‌داند که آن رفتار، ارزشی از ارزش‌های اجتماع را نقض کرده باشد. دورکیم، ارتکاب جرم را معادل جریحه‌دار کردن احساسات جامعه می‌داند و مجازات را واکنش عاطفی و احساسی جامعه در مقابل جرم معرفی می‌کند. به اعتقاد او ارتکاب جرم، نقض اساسی‌ترین ارزش‌ها است. ارزش در اصطلاح جامعه‌شناسی و فلسفه اخلاق، به باورهایی گفته می‌شود که افراد یا گروه‌های انسانی در مورد چیزهای مطلوب و مناسب دارند. ارزش‌های گوناگون، نمایانگر جنبه‌های اساسی تنوع در فرهنگ انسانی است که معمولاً از عادت و هنجار سرچشمه می‌گیرند.(ویکی پدیا). بنابراین وقتی ارزشی درونی شود، فرد در هنگام مواجهه با نقض آن ارزش، دچار فشار درونی می‌شود. با همین منطق به خود نیز اجازه نقض آن ارزش‌ها را نمی‌دهد و در واقع تمایل خود برای ارتکاب جرم راکنترل می‌کند. این روند خودکنترلی، یکی از روش‌هایی است که باعث می‌شود فرد به سمت ارتکاب جرم نرود.

در فضای مجازی، بسیاری از رفتارها وجود دارد که هر چند در شمار رفتارهای آسیب‌رسان هستند، اما هنوز به جایگاه ارزشی نرسیده‌اند و به اندازه کافی در فرهنگ و هنجارهای جامعه نفوذ نکرده‌اند و ارتکاب آن‌ها به اندازه جرایم سنتی، باعث جریحه‌دار شدن احساسات عمومی نمی‌شود.

هکتیویسم، یک پدیده دو بعدی است.از آن منظر که پدیده‌ای نوظهور است، هنوز به اندازه کافی درونی نشده و خودکنترلی در مورد آن نمی‌تواند کارکرد لازم را در راستای پیشگیری از ارتکاب داشته باشد. از منظری دیگر، بسیاری، هکتیویست‌ها را به عنوان افرادی که طرفدار

[1]- Mark Ansel

آزادی و حق هستند می‌شناسند. خود هکتیویست‌ها نیز ارتکاب هکتیویسم را رفتاری اعتراضی و جلوه‌ای از آزادی بیان می‌دانند و لذا نه‌تنها تمایلی به خودکنترلی ندارند، بلکه خود را در ارتکاب آن محق نیز می‌دانند؛ بنابراین از این منظر نیز پیشگیری از طریق خودکنترلی و مکانیسم فشار، معنا و موضوعیت خود را از دست می‌دهد.

ارتکاب جرم همواره جوامع را در معرض خطر و ناامنی قرار داده است. بی‌نظمی‌هایی که ارتکاب جرم به همراه دارد، نیازمند اتخاذ تدابیری است تا منتهی به فروپاشی بنیان‌های اجتماع نشود. زمانی می‌توان نسبت به یک رفتار تدابیر پیشگیرانه در نظر گرفت که ماهیت آن رفتار شناخته شده باشد. پیش‌بینی تدابیر پیشگیرانه برای مقابله با رفتاری که ویژگی‌های آن ناشناخته است، تنها دستاوردش خدشه‌دار کردن حقوق و آزادی‌های فردی و امنیتی ساختن جامعه خواهد بود. چرا که اگر قانونی در قضیه مطروحه وجود نداشته باشد یا قانون در خصوص موضوع ساکت باشد، در این صورت نهاد قدرت خواسته خود را در باب پیشگیری پیاده خواهد کرد و مراجع انتظامی و اجرایی، قدرت بیشتری نسبت به نهادهای تقنینی و قضایی خواهند داشت. در قوانین جزایی کشور ما هر چند واژه هکتیویسم به صراحت مورد توجه قانونگذار نبوده است و بر این اساس، در بحث پیشگیری ایرادات مذکور را دارد، اما اَشکالی از هکتیویسم، به عنوان رفتار مجرمانه مستوجب مجازات پیش‌بینی شده است که در مورد آن‌ها می‌توان تدابیر پیشگیرانه را اتخاذ کرد. این مسأله موضوعی مهم است که بدانیم که آیا می‌توان برای پیشگیری از هکتیویسم اقدامات عملی را در خصوص داده‌ها و رایانه‌ها و امنیت اطلاعات و سازمان‌ها در نظر گرفت یا خیر؟ در فضای‌سایبر برای دستیابی کامل‌تر به اهداف پیشگیری از جرم، در وهله اول، باید وظیفه افراد مسئول امنیت سیستم‌ها و شبکه‌های اطلاعاتی در مهار و رفع مشکلات امنیتی و اتخاذ تدابیری در جهت تقویت سیستم دفاعی، برای جلوگیری از تکرار جرم، به آن‌ها آموزش داده شود. در مرحله دوم، باید مشخص شود که چه چیزی یک پاسخ و واکنش مناسب را تشکیل می‌دهد؟

۵-۱- انواع اصلی پیشگیری در خصوص هکتیویسم

پیشگیری از جرایم‌سایبری، منتفع از بهترین شیوه‌های مربوط به سیستم‌ها و شبکه‌های رایانه‌ای و دانش و تجربه است تا بتواند امنیت سایبری را در بالاترین سطح ممکن فراهم کند. برای تدارک این اقدامات باید نرم‌افزارهایی طراحی شود و امکانات سخت‌افزاری بهبود یابد. این امکانات باید استانداردها و شیوه‌های امنیتی پیشرفته و به روز و ابزارهایی همچون رمزگذاری، امضای دیجیتال و غیره را به همراه داشته باشد تا بتواند موانعی برای مهاجمان بالقوه ایجاد کند. نکته مهم و غیرقابل چشم‌پوشی این است که هکتیویست‌ها نیز افرادی هستند که به همه این ابزارها دسترسی دارند و معمولاً در کنار آن از تخصص بالایی هم برخوردار هستند که از آن در راه شناسایی آسیب پذیری این ابزارها و پیشبرد اهداف خود استفاده می‌کنند.

یکی از عناصر پیشگیری از جرم، پیش‌بینی اقدامات غیر قهرآمیز غیر کیفری در خصوص جرم است. زمانی که عوامل شخصی و وضعی دست به دست هم دهند ارتکاب جرم راتسهیل می‌نمایند. بنابراین برای پیشگیری از ارتکاب جرم انجام یک سری اقدامات فردی و وضعی مؤثر خواهد بود.

۵-۱-۱-پیشگیری وضعیت‌مدار از هکتیویسم

پیشگیری وضعیت‌مدار یا اقدامات وضعی پیشگیرانه، ناظر به شرایط و اوضاع و احوالی است که مجرم را در آستانه ارتکاب جرم قرار می‌دهد. این اوضاع و احوال در جرم‌شناسی «وضعیت‌های پیش از ارتکاب» یا «وضعیت‌های پیش جنایی» نام دارند. این شرایط زمینه‌ساز عمل مجرمانه بوده و ارتکاب جرم را تحریک یا تسهیل می‌نمایند. (صلاحی, ۱۳۸۸, ص. ۲۲۲)

پیشگیری وضعی، معادل بر هم زدن فرصت ارتکاب جرم است. به عبارت بهتر در پیشگیری وضعی بحث بر سر خنثی‌کردن فرصت‌های ارتکاب جرم و هدف، تغییر وضعیتی است که می‌تواند منجر به ارتکاب جرم شود.

در سال ۱۹۷۹، کوهن[1] و فلسون[2] نظریه‌ای را برای توضیح روند نرخ جرم و جنایت بر اساس تغییرات در فعالیت‌های روزمره زندگی مطرح کردند. آن‌ها استدلال کردند که ساختار فعالیت‌های عادی روزانه بر فرصت‌های مجرمانه تأثیر می‌گذارد.گفته می‌شود که حداقل سه عنصر بر نرخ جرم تأثیر می‌گذارد: وجود مجرمان با انگیزه، در دسترس بودن اهداف مناسب و عدم وجود نگهبانان توانمند در برابر تخلف. حدود ۲۰ سال بعد، فلسون و کلارک[3]، ده اصل نظریه فرصت را ترسیم کردند، یکی از این اصول بیان می‌کند که تغییرات اجتماعی و فناوری، فرصت‌های جدید جرم و جنایت را ایجاد می‌کند. (Russell G. Smith, 2015, p. 13)

مؤلفه‌های نظریه فرصت که کاهش انگیزه افراد برای ارتکاب جرم، کاهش اهداف موجود برای ارتکاب جرم و تقویت نقش پلیس در پیشگیری یا کشف جرم است، بر زمانی که جرم و جنایت توسعه جهانی نیافته و بومی است، تمرکز دارند. در فضای مجازی، ما یک محیط جرم‌زای ایده‌آل داریم؛ زیرا اهداف و فرصت‌های فراوان، مجرمان با انگیزه بالا و تا همین اواخر، مقررات و قوانین زیادی برای مقابله با آن‌ها وجود ندارد. با این وصف می‌توان نظریه فرصت را با برخی تغییرات در فضای‌سایبر و در خصوص جرایم‌سایبری از جمله هکتیویسم هم اعمال کرد. از نظر فرصت‌های جرم و جنایت، می‌توان اظهار نظر ویلی ساتون[4]، سارق بدنام بانک آمریکایی دهه ۱۹۵۰ را به یاد آورد که زمانی که از او پرسیده شده چرا در سرقت از بانک‌ها اصرار داشته است؟ پاسخ داده است: «چون پول اینجاست ».در فضای مجازی، فرصت‌ها فراوان است و این فرصت‌ها عمدتاً به دنبال توسعه و معرفی فناوری‌های دیجیتال جدید بوده است. (Russell G. Smith, 2015, p. 15)

به مصداق اینکه علاج واقعه را قبل از وقوع باید کرد، در پیشگیری وضعی این اختیار در دست نهاد قدرت است که از هر علاجی برای جلوگیری از وقوع جرم استفاده کند؛ حتی اگر این علاج، ورود به حریم خصوصی افراد در فضای‌سایبر باشد.از این نظر پیشگیری وضعی می‌تواند به ابزاری در دست خودکامگان بدل شود و مورد سوءاستفاده قرار گیرد. در فضای‌سایبر، در راستای پیشگیری وضعی باید به تدابیر فنی پناه برد تا به کمک آن‌ها امنیت اطلاعات و سیستم‌ها حفظ شود. تدابیر پیشگیری وضعی در فضای‌سایبری تدابیری کلی هستند و اختصاص به جرم‌رایانه‌ای خاصی ندارند.بنابراین با توجه به اینکه برای استفاده از رایانه و ارتکاب جرم در این فضا همیشه لازم نیست که فرد از تخصص و دانش بالایی برخوردار باشد و ابتکار عمل خاصی داشته باشد تا بتواند مرتکب جرم شود، بلکه همین که بتواند از رایانه استفاده کند زمینه برای ارتکاب جرم مساعد خواهد بود، تدابیری که در مورد پیشگیری وضعی از ارتکاب هکتیویسم به کار گرفته می‌شود تفاوتی با دیگر جرایم‌سایبری ندارد.

پیشگیری وضعی می‌تواند در قالب تقویت حمایت از آماج بالقوه جرم یا حمایت از بزه‌دیده مورد توجه قرار گیرد. گاهی اوقات وضعیتی که مجنی‌علیه یا آماج جرم دارد باعث ارتکاب جرم نسبت به او می‌شود و در واقع اگر این اوضاع و احوال در مجنی‌علیه وجود نداشت امکان داشت که بزه‌دیده واقع نشود. بنابراین بزه‌دیده و آماج جرم می‌تواند به عنوان یکی از وضعیت‌های پیش‌جنایی قلمداد شود که مجرم را در آستانه ارتکاب جرم قرار می‌دهد. در مورد هکتیویسم نیز(پیشگیری وضعی می‌تواند در قالب آگاه کردن شهروندان در خصوص نحوه استفاده

[1]- Cohen
[2] -Felson
[3] -Clark
[4]- Willie Sutton

از فضای‌سایبری و خطرات احتمالی که در این فضا می‌تواند آن‌ها را تهدید کند، تدابیر اداری و سازمانی، تدابیر فنی، رمزگذاری رایانه، یافتن روزنه شبکه، استفاده از برنامه‌های مرورگر شبکه، استفاده از برنامه‌های اعلام خطر نفوذ مطرح شود.) (ناصرزاده, ۱۳۹۳, ص. ۲۶۳)

از آنجا که در پیشگیری وضعی به دنبال این هستیم که با ایجاد موانعی مرحله گذار از اندیشه به فعل مجرمانه را مشکل و در صورت امکان غیرممکن سازیم، باید از راهکارهایی استفاده شود که دسترسی به هدف از ارتکاب جرم را برای مرتکب با دشواری مواجه کند تا با استفاده از این روش، افرادی که فکر ارتکاب جرم را در سر می‌پرورانند با دیدن دشواری‌های مسیر ارتکاب جرم و احساس خطر در مورد شناسایی و دستگیرشدن، تمایل به ارتکاب جرم در آن‌ها کاهش یابد یا حتی از این اندیشه خود منصرف شوند.

۵-۱-۲- پیشگیری فردمدار از هکتیویسم

در پیشگیری فرد مدار توجه و تمرکز بر روی خود فرد و تلاش برای پر کردن خلأهای دوران کودکی است. پیشگیری فرد مدار شامل پیشگیری اجتماعی و پیشگیری رشد مدار است.

۵-۱-۲-۱-پیشگیری اجتماعی

پیشگیری ممکن است در سطح جامعه انجام شود. این نوع از پیشگیری که پیشگیری اجتماعی نامیده می‌شود بر تغییر شرایط عمدتاً جرم‌زای محیط اجتماعی و اصلاح ساختارهای فرهنگی، خانوادگی، اقتصادی، اداری و... از طریق از بین بردن عوامل اجتماعی تکوین جرم تأکید می‌کند. (معظمی گودرزی, ۱۴۰۱, ص. ۱۷۱)

در واقع، «پیشگیری اجتماعی»، مجموعه تدابیرآموزشی، فرهنگی، اقتصادی و اجتماعی هستند که برای سالم‌سازی محیط و حذف یا کاهش عوامل اجتماعی جرم مورد استفاده قرار می‌گیرند. (ناصرزاده, ۱۳۹۳, ص. ۲۹۵)در این نوع پیشگیری سالم‌سازی زیرساخت‌های ملی در سطح جامعه و از بین بردن عوامل جرم‌زای اجتماعی به عنوان هدف این نوع پیشگیری مطرح می‌شود.

در خصوص هکتیویسم –با توجه به ویژگی‌های خاص جرایم‌سایبری- پیشگیری اجتماعی با جرایم سنتی متفاوت است. اقداماتی که در قالب پیشگیری اجتماعی از هکتیویسم قابل انجام است می‌تواند به شکلِ دادن آموزش‌های لازم به افرادی که در مشاغل مرتبط با فضای مجازی فعالیت می‌کنند، بهبود اوضاع اقتصادی و معیشت مردم، افزایش فرهنگ استفاده درست از اینترنت و فضای مجازی و...مطرح شود.

یکی دیگر از مواردی که به عنوان عاملی اجتماعی در پیشگیری از ارتکاب جرایم و از جمله هکتیویسم می‌تواند مطرح شود، افزایش میزان تحصیلات و علم و آگاهی افراد جامعه است. البته در برخی از جرایم به خصوص جرایمی که نیاز به تبحر و تخصص خاصی دارند یکی از علت‌های گرایش به رفتار مجرمانه همین وسوسه شدن برای اثبات دانش و تخصص و یا استفاده از آن در ارتکاب جرم و تصور کشف نشدن به لحاظ بهره‌گیری از فنون خاص می‌باشد.

۵-۱-۲-۲-پیشگیری رشدمدار

پیشگیری رشدمدار ناظر به پیشگیری با تأثیرگذاری بر مراحل رشد فرد از کودکی می‌باشد. این نوع پیشگیری هم شامل کودک و هم شامل کسانی می‌شود که در تربیت کودک برای مقاومت در برابر ارتکاب جرم کوتاهی کرده‌اند. پیشگیری رشدمدار در قالب مداخله زودرس از طریق خانواده، مدرسه، نظارت بر ارتباط با گروه همسالان و استفاده از برنامه‌های آموزنده در رسانه‌های جمعی و غیره می‌تواند مطرح شود.

بستر فضای مجازی محلی است که انسان می‌تواند در آن سرشت خود را نشان دهد و یا از روی شرارت، شهوت، کنجکاوی و یا زیاده‌خواهی دست به ارتکاب اعمال و رفتاری بزند که خلاف قانون، اخلاق و هنجارهای اجتماعی باشند. سیستم‌های رایانه‌ای امروزه در دسترس همگان

قرار دارد و به لحاظ داشتن امکانات فراوان و جذابیت این فضا برای کاربران، به جرأت می‌توان گفت بسیاری از نوجوانان و جوانان بیشترین ساعات شبانه‌روز خود را به گشت و گذار در این فضا و کشف ابعاد مختلف این فضای جذاب می‌گذرانند. در مقابل، متولیان امر تدوین تدابیر پیشگیرانه اجتماعی به اندازه جوانان و نوجوانان امروز در پیچ و خم فضای مجازی سیر نکرده‌اند و رابطه عمیقی با این فضا ندارند، این فاصله و شکاف دیجیتال باعث ناکارآمدی و عدم تأثیرگذاری تدابیر پیشگیرانه می‌شود.

در مسیر پیشگیری از ارتکاب جرم، یکی از ابزارهای مهمی که سیاست جنایی از آن بهره می‌برد، اعتقاد به ارزش‌های مورد پذیرش جامعه است که می‌تواند باعث شود فرد در جهت رعایت این ارزش‌ها به سمت ارتکاب جرم نرود و اگر تفکر ارتکاب جرم را داشته ازآن منصرف شود. ممکن است اعتقادات فرد هکتیویست، بر خلاف ارزش‌های مورد پذیرش اجتماع باشد و بنابراین در مورد این پدیده پیشگیری از ارتکاب، با توسل به اعتقاد به ارزش‌های مورد پذیرش جامعه مفهومی نخواهد داشت؛ بر خلاف جرایم سنتی و سایر جرایم‌سایبری که در آن‌ها اعتقاد به این ارزش‌ها می‌تواند عاملی برای پیشگیری از ارتکاب جرم باشد.

۶-تأملات مربوط به بزه دیده در هکتیویسم

قربانی، یک عنصر کلیدی در تولید رویداد مجرمانه به ویژه در اینترنت است؛ جایی که او منطقه خطر خود را با گنجاندن کالاهای خاص در فضای مجازی تعیین می‌کند. تعامل با دیگران، به ویژه غریبه‌ها و عدم استفاده از تمام ابزارهای ممکن برای محافظت از خود.

نقش و تأثیر بزه دیده در ارتباط با ارتکاب هکتیویسم انکارناپذیر است.بزه‌دیده سایبری شخصی است که به علت بی‌احتیاطی و ناآگاهی از تدابیر حفاظتی در برخی مواقع، خود عامل اصلی ارتکاب یک جرم سایبری محسوب می‌گردد. به عبارتی دیگر،(بسیاری از مجرمین سایبری جهت ارتکاب اقدامات خود مترصد غفلت و بی‌احتیاطی کاربر اینترنتی هستند و با تحقق این شرط، اهداف خود را به مرحله اجرا خواهند گذاشت. لذا به منظور جلوگیری از شکل‌گیری اینگونه جرایم، باید تا حد ممکن با آموزش و آگاه‌سازی کاربران و اتخاذ تدابیر امنیتی در فضای سایبر از تبدیل شدن کاربران سایبری به بزه‌دیدگان سایبری جلوگیری کرد. البته صِرف بی‌اطلاعی و ناآگاهی از تدابیر امنیتی، عامل ایجاد بزه‌دیده سایبری نیست؛ بلکه در پاره‌ای موارد عوامل زیست‌شناختی مانند سن، جنس و یا عوامل اجتماعی از قبیل مشاغل خطرناک و آسیب‌پذیر، شیوه زندگی، شرایط اجتماعی- اقتصادی و عوامل روان‌شناختی از جمله سهل‌انگاری و بی‌توجهی می‌تواند موجب شکل‌گیری بزه‌دیدگی به ویژه از نوع سایبری گردد. (وروایی, ۱۳۹۰, ص. ۱۹)

به نظر می‌رسد کشورهایی که زیرساخت اینترنتی خوبی دارند، اغلب هدف هکتیویسم هستند و بیشتر تحت تأثیر آن قرار می‌گیرند.

ایالات متحده ۲۳ درصد از حملات سایبری را به خود اختصاص داده است و پس از آن چین با ۹ درصد در رتبه دوم قرار دارد. شرکت معروف امنیت رایانه «مک‌آفی[1]» با انتشار گزارشی اظهار داشته است که اینترنت سالانه ۲ تا ۳ تریلیون دلار درآمد دارد و جرایم‌سایبری باید به خاطر از بین بردن ۱۵ تا ۲۰ درصد از این رقم پاسخگو باشد. تخمین مجموع ضررها به دلیل عدم گزارش بیشتر هک‌ها به درستی امکان‌پذیر نیست؛ با این حال مرکز مطالعات استراتژیک و بین‌المللی با همکاری مک‌آفی خسارات وارد شده را حداقل بین ۳۷۵ و در بدترین حالت ۵۷۵ میلیارد دلار تخمین می‌زند. بنابراین، جرایم‌سایبری یک مشکل بزرگ است که با همان سرعت دنیای دیجیتال، گسترش می‌یابد. در همین گزارش، مک‌آفی پیشنهاد می‌کند که کشورها تمایل دارند فعالیت‌های مخرب فضای مجازی را نادیده بگیرند؛ زیرا از ۲ درصد تولید ناخالص

[1]-McAfee

داخلی کشورها بالاتر نمی‌رود. چنین برخورد سهل‌انگارانه‌ای با تهدیدی به این خطرناکی، ناشی از این موضوع است که دفاع در برابر آن بسیار پرهزینه است. (C.N.Hampson,Noah, 2012, p. 4)

۷-روش شناسی پژوهش

پژوهش حاضر از منظر هدف در شمار تحقیقات کاربردی است و از نظر راه‌های تجزیه و تحلیل اطلاعات، جنبه توصیفی-تحلیلی دارد و مراحل پیشگیری و انواع آن در کنار امکان سنجی پیشگیری از هکتیویسم مورد بررسی قرار گرفته است. گردآوری اطلاعات به روش کتابخانه‌ای و از میان کتاب‌ها و مجله‌ها و پایان‌نامه‌های مرتبط داخلی و خارجی و ترجمه مقالات و کتاب‌های خارجی صورت گرفته است. در نهایت، تجزیه و تحلیل پژوهش به شیوه استدلالی انجام شده است.

۸-یافته‌های پژوهش

امروزه، هکتیویست‌ها از تعدادی زیرگروه با انگیزه‌های متنوع تشکیل شده‌اند.این افراد، به یک زنجیره خوب و بد متصل نیستند و به طور منظم، در دسته‌های کاملاً تعریف شده قرار نمی‌گیرند. آن‌ها با انگیزه‌ها و موقعیت‌های مختلف، به صورت دایره وار، در کنار یکدیگر قرار می‌گیرند. دسته بندی هکتیویست‌ها می‌تواند بر اساس مذهب، منطقه جهانی، ایدئولوژی سیاسی، وضعیت اجتماعی، ملاحظات اقتصادی و غیره صورت گیرد. از بین بردن و شناسایی راه‌های از بین بردن هکتیویسم به طور کامل امکان‌پذیر نیست و حذف پدیده‌ای که به صورت ارگانیک در جامعه به عنوان بیان نیاز شهروندان به اقدامات سیاسی توسعه یافته است به نظر نمی‌تواند پیامدهای مثبتی به همراه داشته باشد. می‌توان گفت هکتیویسم نیز یک رویه سیاسی است و همچون هر رویه سیاسی دیگر مانند تصمیم‌های مجلس و اعتصابات قانونی و...گاهی اوقات ممکن است مورد سوء استفاده قرار گیرد. بر این اساس بازرسی و نظارت بر این رویه سیاسی و هدایت آن در جهت مثبت و سازنده موضوعی بسیار مهم است.

کاهش فضای عملیاتی می‌تواند در قالب پیشگیری وضعی و سخت کردن ارتکاب جرم مورد توجه قرار گیرد. هکتیویسم، در بستر اینترنت که هیچ حد و مرزی ندارد اتفاق می‌افتد و معلوم نیست که بتوان تدابیر پیشگیرانه سنتی را که در ارتباط مستقیم با فرهنگ مردم و مکان ارتکاب جرم هستند، در فضای‌سایبر هم اعمال نمود.از سوی دیگر در پدیده هکتیویسم، دسترسی به ابزار ارتکاب نیز به راحتی امکان پذیر است و در نهایت همه چیز به دانش هکتیویست و تخصص او در استفاده از رایانه و اینترنت بستگی دارد.

نکته مهم و قابل توجه این است که همانطور که در سراسر جهان، شاهد ابتکارات متعدد دولت‌ها برای محدود کردن استفاده آزادانه از شبکه‌های رایانه‌ای هستیم، دانش و بحث در مورد اقدامات موازی این ابتکارات و مقابله با آن، به طور فزاینده‌ای در حال پیشروی است. طراحی، ساخت و استفاده روزافزون از انواع وی‌پی‌ان‌ها توسط کاربران اینترنت و شبکه‌های اجتماعی خود مصداق بارز هکتیویسمی است که دولت‌ها با ایجاد محدودیت‌های مختلف در دسترسی به شبکه‌ها کاربران را به سمت آن سوق داده‌اند. این مهم ما را به این نتیجه رهنمون می‌سازد که تدابیر پیشگیرانه برای اینکه کارآمدی آن مشخص شود، نیاز به نظارت و ارزیابی دارد. (توصیه شده است که ارزیابی و سنجش برنامه‌های پیشگیری به صورت دوره‌ای انجام شود مخصوصاً در صورتی که برنامه پیشگیری طولانی باشد، طراحان برنامه باید به طور منظم و دوره‌ای نمونه‌برداری کرده و نتایج را ارزیابی کنند). (محمدنسل, ۱۳۸۹, ص. ۳۲۸)

در هکتیویسم، فرد در بستری خلوت و به دور از دیگران بر اساس وسوسه‌های ذهنی که از خواست درونی اش نشأت می‌گیرد دست به ارتکاب جرم می‌زند.تنها راه برای نفوذ به این فضا در راستای پیشگیری از ارتکاب جرم، ورود به حریم خصوصی افراد است و نتیجه ورود

به حریم خصوصی افراد نه تنها نمی‌تواند پیشگیری از وقوع جرم را به همراه داشته باشد، بلکه باعث تجری افراد و نشانگر خودکامگی نهاد قدرت خواهد بود.

بحث و نتیجه گیری

اساسا، هکتیویسم، در عصری که پیشگیری از خطر و دستیابی به حداکثر امنیت، یک منطق غالب است، به عنوان شکل جدیدی از اعتراض که دلیل خود را برای قانون شکنی وجود انگیزه‌های سیاسی بیان می‌کند، مفهوم عدالت اجتماعی را در بستری جدید و چالش برانگیز دوباره چارچوب می‌دهد. رویه هکتیویستی با پیکربندی جدید خود از روش‌های اعتراضی سنتی، ما را وادار می‌کند که بحث‌های قدیمی تر در مورد عدالت و قانون شکنی، که به عنوان تلاشی برای دستیابی به آزادی بیان و حفظ حریم خصوصی و اعتراض‌های سیاسی مطرح می‌شد، را در عصر جدید، در فضای مجازی و با روش‌های نوین بازگو کنیم. ادراک ما باید به منظور در نظر گرفتن ابعاد مختلف اجتماعی، تولد ابزارها و هنجارهای ارتباطی و رفتاری توسط جوامع جدید که از علل اجتماعی و سیاسی قدیم و جدید حمایت می‌کنند، گسترش بیابد و پیکربندی مجدد شود.این یک گام ضروری در چالش پیشگیری از جرایم‌سایبری و پدیده‌های نوظهور در این بستر از جمله هکتیویسم است.

علیرغم خطرات فضای مجازی به عنوان یک میدان نبرد دیجیتالی در آینده، مزایای فضای‌سایبری بر معایب آن برتری دارد و باید به این فضا به عنوان ساختاری نگاه کنیم که جریان آزاد اطلاعات را تسهیل می‌کند و لازم است از مزایای آن برای پیشرفت جامعه از جمله ارتقا و توسعه سرمایه‌گذاری و تسهیل تجارت استفاده کرد. فضای مجازی بستری است که موجب رشد آزادی بیان در جامعه مدنی می‌شود. این همه، نیازمند حمایت و ترویج آزادی دسترسی به اطلاعات و رها شدن آن از دام محدودیت‌ها و سانسور و اجتناب از محروم نمودن شهروندان از انتخاب آزادانه و دسترسی آزاد به اطلاعات به نام امنیت است. دولت با ایجاد اعتماد در فضای مجازی، وظیفه اصلی مهار تهدیدی به نام هکتیویسم را بر عهده دارد.

دولت‌ها نباید به نام پیشگیری، فضای باز اینترنت را با بستن مرزهای دیجیتالی خود به روی سایر نقاط جهان مسدود و محدود کنند. در همه کشورهای توسعه یافته، بزرگترین سرمایه، سرمایه انسانی است. سرمایه انسانی با تولید فکر، امکان اشتغال‌زایی و تولید را فراهم می‌کند. حمایت از سرمایه انسانی مستلزم این است که از یک سو امکانات آموزش رایگان و همگانی شهروندان فراهم شود و از سوی دیگر با فراهم ساختن بسترهای فرهنگی، اجتماعی و اقتصادی راهی به وجود آید تا این سرمایه انسانی از دلگرمی و دلخوشی لازم برخوردار باشد تا در کشور بماند و بحران فرار مغزها پیش نیاید.

با توجه به اینکه در اکثر مواقع، هکتیویست‌ها اقداماتشان را برای جلب توجه، خودنمایی یا رضایت خود انجام می‌دهند لازم است در نگارش و تدوین قانون به این نکته مهم توجه شود که افزایش مجازات راه مناسبی برای پیشگیری از اقدامات هکتیویست‌ها نیست و بهتر است به جای مجازات به آن‌ها در مورد آسیب‌های ناشی از هکتیویسم آموزش‌های لازم داده شود و از ظرفیت هوش و دانش آن‌ها برای ارتقاء سطح امنیتی سیستم‌های رایانه‌ای در کشور و آموزش دادن به افرادی که علاقمند به یادگیری فناوری ارتباطات و اطلاعات هستند استفاده شود.

یکی از مهم‌ترین راه‌های پیشگیری ازهکتیویسم، شناخت توانمندی‌های دانش‌آموزان در مدارس و تقویت ارزش‌های اخلاقی برای آن‌ها در برابر هک و ورود به حریم خصوصی دیگران و هدایت علاقه ایشان به رایانه در جهت مثبت می‌باشد و با توجه به اینکه ویژگی‌های محیطی در احتمال انحراف افراد تأثیر می‌گذارد و سوءاستفاده از محیط سایبر با داشتن کمترین مهارت و دانش فنی امکان‌پذیر است، لذا تدابیر پیشگیرانه در مورد نوجوانان و جوانان، بیش از سایر گروه‌ها باید مورد توجه قرار گیرند.

برگزاری دوره‌های آموزشی در خصوص آموزش اخلاق استفاده از رایانه و دوره‌های دفاع از امنیت رایانه و سازماندهی خدمات امنیت رایانه برای کارکنان دولت، سازمان‌ها و غیره جزء موارد قابل توجه در راستای پیشگیری می‌باشد.

شناسایی علل بروز هر پدیده‌ای برای یافتن تدابیر پیشگیرانه و نظارتی اجرایی در راستای پیشگیری از ارتکاب جرم لازم و ضروری است. در این راستا توجه ویژه به تدابیر پیشگیرانه غیر قهری غیرکیفری از اهمیت بالایی برخوردار است. اجرای اصول پیشگیری غیرکیفری اجتماعی و وضعی از جرایم‌سایبری و نیز هکتیویسم، نیازمند توسعه بازرسی و نظارت در فضای مجازی است. هکتیویسم پدیده‌ای نیست که به راحتی و بلافاصله پس از ارتکاب،قابل تشخیص باشد. فرایند تعقیب و رسیدگی در جرایم سایبری و نیز پیشگیری از آن نیازمند تربیت نیروهای متخصص با استفاده از تخصص و تبحر افراد آشنا به تکنولوژی آخرین فناوری‌های روز دنیا می‌باشد.

هکتیویسم پدیده‌ای است که در فضای فرامرزی سایبر تحقق می‌یابد و بروز آن ابعاد گسترده و جهانی دارد، بنابراین همکاری با دیگر کشورها و برگزاری کنگره‌ها و نشست‌های بین‌المللی و کارگاه‌های آموزشی در راستای تبادل نظر و آموزش آخرین فناوری‌های روز دنیا در زمینه بهبود امکانات سخت‌افزاری و نرم‌افزاری برای پیشگیری از جرایم سایبری و هکتیویسم مفید و حتی ضروری می‌باشد.

تعارض منافع

در انجام مطالعه حاضر، هیچ‌گونه تضاد منافعی وجود ندارد.

مشارکت نویسندگان

در نگارش این مقاله تمامی نویسندگان نقش یکسانی ایفا کردند.

حامی مالی

این پژوهش حامی مالی نداشته است.

فهرست منابع

ارقیلا، د. ر. (۲۰۰۱). شبکه‌ها و جنگ‌های شبکه‌ای: آینده تروریسم، جرم و تندروی. گزارش‌های مونوگراف.

اسمیت، ر. گ.، و سی. -سی.-سی. (۲۰۱۵). ریسک‌ها و پاسخ‌ها به جرایم سایبری: دیدگاه‌های شرق و غرب.

امیریان فارسانی، ف. ح. (۲۰۲۰، پاییز). علت‌شناسی جرایم سایبری و سازوکارهای پیشگیری از آن. فصلنامه علوم خبری، ۹(۳۵)، ۱۹۳-۲۳۰.

باقری‌اصل، ج. ف. (۲۰۰۸). پیشگیری اجتماعی از جرایم و انحرافات سایبری. مجلس و پژوهش، ۱۴(۵۵)، ۱۲۱-۱۵۵.

پاکزاد، ب. (۲۰۰۹). تروریسم سایبری (رساله دکتری). تهران.

جعفری، م. (۲۰۰۸). مختصر جرم‌شناسی (خلاصه مباحث جرم‌شناسی دکتر نجفی ابرندآبادی). تهران.

جوان جعفری بجنوردی، ز. ف. (۲۰۱۷، بهار). نقض آزادی جریان اطلاعات در فرآیند پیشگیری موقعیت‌مدار از جرایم سایبری. پژوهش حقوق کیفری، ۵(۱۸)، ۶۹-۱۰۰.

جوردن، ت. (۲۰۰۱). فعالیت‌گرایی! اقدام مستقیم، هکتیویسم و آینده جامعه (ویرایش: ب. ب. همیلتون). لندن: انتشارات رکسیون.

جیشانکار، ک. (ویرایشگر). (۲۰۱۱). جرم‌شناسی سایبری: بررسی جرایم اینترنتی و رفتار مجرمانه. نیویورک.

حیدری‌نژاد، ن. (۲۰۱۸، تابستان). پیشگیری وضعی در جرایم سایبری از منظر حقوق کیفری ایران و جهان. فصلنامه علمی حقوقی قانون یار، ۲(۶)، ۲۹-۴۳.

دنینگ، د. ای. (۲۰۰۱). فعالیت‌گرایی، هکتیویسم و تروریسم سایبری. در شبکه‌ها و جنگ‌های شبکه‌ای: آینده تروریسم، جرم و تندروی (ص. ۲۳۹–۲۸۸).

سلیمان، ر. (۲۰۱۷). اعتراضات الکترونیکی: هکتیویسم به عنوان یک نوع اعتراض در اوگاندا. مرور حقوق و امنیت کامپیوتر، ۳۳، ۷۱۸—۷۲۸.

صبح‌خیز، ب. پ. (۲۰۲۱). الگوی مفهومی سیاست جنایی جرایم سایبری در ایران. فصلنامه مطالعات راهبردی ناجا، ۶(۲۰)، ۱۲۹–۱۵۴. بازیابی تابستان، سال ششم.

صلاحی، ج. (۲۰۰۹). بزهکار اطفال و نوجوانان (جلد چهارم). تهران: بنیاد حقوقی میزان.

کاراگیانوپولوس، و. (۲۰۱۸). زندگی با هکتیویسم: از تعارض تا هم‌زیستی. در ت. ج. هولت (ویرایشگر)، https://doi.org/10.1007/978-3-319-71758-6

کرسلی، گ. (۲۰۱۷). هکینگ غیرمتعارف: مقابله با جنسیت‌زدگی در جوامع هکتیویستی به منظور گسترش گزینه‌های نافرمانی مدنی الکترونیکی. چپل هیل.

لی، اکس. (۲۰۱۳، پاییز). هکتیویسم و متمم اول: تعیین مرز بین اعتراضات سایبری و جرم. مجله حقوق و فناوری هاروارد، ۲۷، ۳۰۱–۳۳۰.

محمد کوره‌پز، ح. ب. (۲۰۱۴). نیمرخ جرم‌شناسی بزهکاران سایبری. پژوهش حقوق کیفری، ۳(۹)، ۱۱۱–۱۴۶. https://jclr.atu.ac.ir/article_1019.html

محمد نسل، غ. (۲۰۱۰، بهار). فرآیند پیشگیری از جرم. فصلنامه حقوق مجله دانشکده حقوق و علوم سیاسی، ۱(۴۰)، ۳۱۷–۳۳۴. https://jlq.ut.ac.ir/article_20861.html#ar_info_pnl_cite

مسکو، گ. (۲۰۱۸). در برخی جنبه‌های جرایم سایبری و قربانیان سایبری. مجله اروپایی جرم، حقوق کیفری و عدالت کیفری، ۱۸۹–۱۹۹.

معظمی گودرزی، س. (۲۰۲۲، خرداد). پیشگیری از وقوع جرم خودزنی در بین کارکنان وظیفه نیروهای مسلح. فصلنامه علمی نظارت و بازرسی، ۱۶(۵۹)، ۱۶۵–۱۹۰. https://doi.org/10.22034/si.2022.98890

ناصرزاده، ز. ب. (۲۰۱۴). امنیت در فضای سایبری با تأکید بر پیشگیری وضعی و اجتماعی. مجموعه مقالات همایش ملی پدافند غیرعامل و علوم انسانی، ۲۵۷–۲۶۴.

هلد، و. وی.، و ب. (۲۰۱۲). هکتیویسم: تجزیه و تحلیل انگیزه انتشار اطلاعات محرمانه. سان مارکوس.

همپسون، سی. ن. (۲۰۱۲، ۵ ژانویه). هکتیویسم: نوعی اعتراض جدید در دنیای شبکه‌ای (جلد ۳۵).

الهی‌منش، ب. پ. (۲۰۲۲، بهار). کارآمدی ضمانت‌اجراها در قبال پولشویی الکترونیکی: بازدارندگی پیشگیرانه در رویارویی با بازدارندگی کیفری. فصلنامه مطالعات فقه و حقوق اسلامی، ۱۴(۲۶)، ۱۹۳–۲۲۴. https://doi.org/10.22075/feqh.2022.25822.3149

وروایی، ح. م. (۲۰۱۱). جرایم سایبری: از علت‌شناسی تا پیشگیری.

References

Arquilla, D. R. (2001). Networks and netwars: The future of terror, crime, and militancy. Monograph Reports.

Curcelli, G. (2017). Unorthodox hacking: Addressing sexism in hacktivist communities to expand options for electronic civil disobedience. Chapel Hill.

Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism. In Networks and netwars: The future of terror, crime, and militancy (pp. 239-288).

Jordan, T. (2001). Activism! Direct action, hacktivism and the future of society (B. B. Hamilton, Ed.). London: Reaktion Books Ltd.

Jaishankar, K. (Ed.). (2011). Cyber criminology: Exploring internet crimes and criminal behavior. New York.

Karagianopoulos, V. (2018). Living with hacktivism: From conflict to symbiosis. In M.-H. M. Thomas J. Holt (Ed.), https://doi.org/10.1007/978-3-319-71758-6

Li, X. (2013, Fall). Hacktivism and the first amendment: Drawing the line between cyber protests and crime. Harvard Journal of Law & Technology, 27, 301-330.

Mesko, G. (2018). On some aspects of cybercrime and cyber victimization. European Journal of Crime, Criminal Law and Criminal Justice, 189-199.

Smith, R. G. (2015). Cybercrime risks and responses: Eastern and western perspectives.

Solomon, R. (2017). Electronic protests: Hacktivism as a form of protest in Uganda. Computer Law & Security Review, 33, 718–728.

Held, W. V., & B. (2012). Hacktivism: An analysis of the motive to disseminate confidential information. San Marcos.

Elahi Manesh, B. P. (2022, Spring). Effectiveness of sanctions in relation to electronic money laundering: Preventive deterrence in dealing with criminal deterrence. Faslnameh Motaleat Fiqh va Hoquq Islami, 14(26), 193-224. https://doi.org/10.22075/feqh.2022.25822.3149

Amirian Farsani, F. H. (2020, Fall). Causality of cybercrimes and mechanisms for their prevention. Faslnameh Oloum Khobari, 9(35), 193-230.

Bagheri Asal, J. F. (2008). Social prevention of cybercrimes and deviations. Majles va Pazhoohesh, 14(55), 121-155.

Pakzad, B. (2009). Cyber terrorism (Doctoral dissertation). Tehran.

Jafari, M. (2008). A brief criminology (Summary of Dr. Najafi Abrandabadi's criminology discussions). Tehran.

Javan Jafari Bijanoudi, Z. F. (2017, Spring). Violation of freedom of information flow in the process of situational crime prevention. Pazhoohesh Hoquq Keifari, 5(18), 69-100.

Heidari Nejad, N. (2018, Summer). Situational prevention in cybercrimes from the perspective of Iranian and international criminal law. Faslnameh Ilmi Hoquqi Ghanoon Yar, 2(6), 29-43.

Sobh Khiz, B. P. (2021). Conceptual model of criminal policy for cybercrimes in Iran. Faslnameh Motaleat Rahborde Najah, 6(20), 129-154. Retrieved Summer, Year 6.

Salahi, J. (2009). Juvenile delinquency and crimes (4th ed.). Tehran: Mizan Legal Foundation.

Mohammad Koreh Piz, H. B. (2014). Criminal profiling of cybercriminals. Pazhoohesh Hoquq Keifari, 3(9), 111-146. https://jclr.atu.ac.ir/article_1019.html

Mohammad Nasl, G. (2010, Spring). Crime prevention process. Faslnameh Hoquq Majaleh Daneshkadeh Hoquq va Oloum Siyasi, 1(40), 317-334. https://jlq.ut.ac.ir/article_20861.html#ar_info_pnl_cite

Nassirzadeh, Z. B. (2014). Security in cyberspace with emphasis on situational and social prevention. Majmoeh Maqalat Hamayesh Melli Padafand Gheir Amali va Oloum Enshahi, 257-264.

Varoavi, H. M. (2011). Cybercrimes: From causality to prevention.

Hampson, C. N. (2012, January 5). Hacktivism: A new breed of protest in a networked world (Vol. 35).

Moezami Godarzi, S. (2022, June). Prevention of self-harm crimes among conscripted soldiers. Faslnameh Ilmi Nezarat va Bazresi, 16(59), 165-190. https://doi.org/10.22034/si.2022.98890