Iranian Journal of Public Policy
2023, Vol. 9 , No. 2 , 97-114

RESEARCH ARTICLE

Criminal Policy making in Cyber Security Violations and Social Prevention Approaches

Eraj Negahdar[1], Babak Pourghahrmani[2*], Jamal Beigi[3]

1- Ph.D Student in Criminal Law and Criminology, Maragheh Branch, Islamic Azad University, Maragheh, Iran
2- Associate Professor of Criminal Law & Criminology, Maragheh Branch, Islamic Azad University, Maragheh, Iran
3- Associate Professor of Criminal Law & Criminology, Maragheh Branch, Islamic Azad University, Maragheh, Iran

* Corresponding Author's Email: **pourghahramani@iau-maragheh.ac.ir**

https://doi.org/10.22059/jppolicy.2023.93610

Received: 28 November 2022
Accepted: 25 April 2023

ABSTRACT

Security is the most important component in the political authority of governments and the cyber world violates it by acknowledging its valuable achievements. Therefore, developing an effective preventive criminal policy against cyber security violation is so important that neglecting it can cause the criminal system to face irreparable challenges. Despite the approval of the international document on cyber security, this paper, using the method of document analysis and a descriptive analytical method, seeks to read the strategies of Iran's cyber security order in the upstream laws and documents and examine the state of social preventive criminal policy in the laws of other countries. It seems that criminal policymaking in Iran can play a significant role, especially in the field of social preventive measures against cyber security violations. In this way, different countries have adopted several security approaches to prevent cyber security violations. Based on the findings of this research, although Iran has considered different strategies in strengthening the security foundations of cyber encounters, due to the lack of appropriate differential policy, it has not yet succeeded in adopting centralized social preventive mechanisms and efficiency in preventing cyber security violations has not been considered and the measures applied are often non-technical in nature, such as training and promotion of digital Knowledge.

Keywords: Criminal Policymaing, Cyber Security, Social Prevention, Security Violation, Criminal Policy, Cyber Space.

فصلنامه سیاستگذاری عمومی

دوره ۹، شماره ۲، تابستان ۱۴۰۲. صفحات ۱۱۴ - ۹۷

مقاله پژوهشی

سیاستگذاری جنایی در نقض امنیت سایبری و رهیافت‌های پیشگیری اجتماعی

ایرج نگهدار[۱]، بابک پورقهرمانی[۲*]، جمال بیگی[۳]

۱- دانشجوی دکتری حقوق جزا و جرم‌شناسی، دانشگاه آزاد اسلامی واحد مراغه، مراغه، ایران

۲- دانشیار حقوق جزا و جرم‌شناسی، دانشگاه آزاد اسلامی واحد مراغه، مراغه، ایران

۳- دانشیار حقوق جزا و جرم‌شناسی، دانشگاه آزاد اسلامی واحد مراغه، مراغه، ایران

* رایانامهٔ نویسنده مسئول: pourghahramani@iau-maragheh.ac.ir

تاریخ دریافت: ۷ آذر ۱۴۰۱

تاریخ پذیرش: ۵ اردیبهشت ۱۴۰۲

https://doi.org/10.22059/jppolicy.2023.93610

چکیده

امنیت، مهم‌ترین مؤلفه در اقتدار سیاسی دولت‌هاست و دنیای سایبری با اذعان به دست‌آوردهای ارزش‌مندش؛ ناقض آن است. لذا سیاستگذاری جنایی پیشگیرانه کارآمد در قبال نقض امنیت سایبری دارای آنچنان اهمیتی است که غفلت از آن، می‌تواند نظام کیفری را با چالش‌های غیرقابل جبرانی روبرو سازد. این نگاشته با استفاده از روش تحلیل اسناد و به روش توصیفی تحلیلی در پی خوانش وضعیت سیاستگذاری جنایی پیشگیرانه اجتماعی ایران در قوانین و اسناد بالادستی در قبال نقض امنیت سایبری و بررسی راهبردهای نظم امنیت سایبری در قوانین دیگر کشور می‌باشد. به‌نظر می‌رسد سیاستگذاری جنایی در ایران میتواند نقش قابل توجهی به ویژه در حوزه اقدامات پیشگیرانه اجتماعی در قبال نقض امنیت سایبری ایفا نماید و در این رهگذر کشورهای مختلف رویکردهای امنیتی متعددی را در قبال پیشگیری از نقض امنیت سایبری اتخاذ نموده‌اند. براساس یافته‌های این پژوهش، هرچند ایران در تقویت بنیان‌های امنیتی مقابلات سایبری راهبردهای مختلفی را درنظر داشته، اما به جهت نبود سیاستگذاری افتراقی مناسب تا به‌حال موفق به اتخاذ سازوکارهای پیشگیرانه اجتماعی متمرکز و کارآمدی در قبال پیشگیری از نقض امنیت سایبری نگردیده و تدابیر اعمال‌شده، غالباً دارای ماهیت غیرفنی نظیر آموزش و ارتقاء دانش دیجیتالی می‌باشند.

واژگان کلیدی: سیاستگذاری جنایی پیشگیرانه، امنیت سایبری، پیشگیری اجتماعی.

مقدمه

در پرتو تأمین امنیت، امکان تحقق ارزش‌های مورد حمایت دولت در تحقق عدالت و آزادی نیز میسر می‌شود. سیاستگذاری‌های جنایی به عنوان شاخه‌ای از سیاستگذاری‌های عمومی به برنامه‌ریزی‌ها و راهبردگذاری برای تحقق امنیت مورد نظر دولت می‌پردازد (shiri,2018:161). سیاستگذاری عمومی[1] برخاسته از علم سیاست است. دانشمندان علوم سیاسی، برای افزایش کارآمدی دولت، رشته سیاستگذاری عمومی را بنیان نهاده و « تصمیم‌های دولتی که با هدف حل یک مسأله عمومی طراحی شده‌اند، سیاستگذاری عمومی نامیده می‌شوند» (Malekmohammadi,2018:20). در این ارتباط سیاستگذاری جنایی، شاخه‌ای از سیاستگذاری عمومی و دارای ویژگی‌های آن است. «سیاستگذاری عمومی مبتنی بر قانون بوده و اقتدارآمیز است» (Ashtarian,2017:28) به نقل از: (shiri,2018:165). گفتمان سیاستگذاری جنایی در پی فراخوان نگاهی همه جانبه به مبارزه با پدیده‌های آسیب‌زای اجتماعی و به عنوان الگوی نوین در تحلیل پدیده‌های جنایی جایگاه بسیار مهمی را در عرصهٔ حقوق کیفری کسب نموده است(Najafi Abrandabadi,2018:554). لازرژ سیاست جنایی را «کلیه اقدامات کیفری و غیرکیفری و پیشگیرانه با ماهیت‌های مختلف که دولت و جامعه مدنی هر یک به نحو مستقل و یا با مشارکت سازمان‌یافته یکدیگر در قالب روش‌های مختلف و به منظور سرکوبی بزهکاران و نیز پیشگیری از جرم و انحراف استفاده می‌کنند» تعریف می‌نماید. با این حال سیاست جنایی در رویکرد فرانوگرایانه در حقیقت تلفیقی از سیاستگذاری عمومی و سیاست جنایی است که براساس داده‌های نوین دانش بشری در پی پیشگیری وقایع برمی‌آید تا از طریق، اصلاح روش‌ها و حذف عوامل مؤثر از وقوع پدیده‌های که ظرفیت تبدیل به پدیدهٔ جنایی را دارند، جلوگیری نماید. در سیاست جنایی، برای پیشگیری از جرم مبارزه با آن از وسایل مختلف دولتی و غیردولتی کمک گرفته می‌شود (Watani, Amir and Asadi,2016:99). پیشگیری از نقض امنیت ملی در فضای سایبر از آن‌رو اهمیت مضاعف دارد که تهدیدها علیه امنیت ملی در این فضا با فناوری اطلاعات یا فناوری هسته‌ای به نسبت تهدیدات گذشته متنوع‌تر شده و دولت‌ها را در مسیر پرمخاطره‌ای قرار داده است(Bahremand & Davoudi, 2017:28). این پژوهش بر این فرض اولیه استوار است که نقض امنیت سایبری نه یک جرم خاص بلکه پدیده‌ای فراحقوقی و بین‌رشته‌ای و مشتمل بر ویژگی‌های فنی، اجتماعی و امنیتی است. بدین ترتیب این مفهوم در ادبیات حقوقی سایبری آنچنان که باید مورد بررسی قرار نگرفته و نتیجه آن نبود نظام واحد پیشگیری با تعریف خاص قانونی از نقض امنیت و اتخاذ راهکارهای پیشگیرانه است. با اعتقاد به اینکه در سیاستگذاری جنایی کارآمد، اقدامات پیشگیرانه صرفاً نه در قبال جرایم بلکه در قبال تمامی آسیب‌های پیدا و پنهان پدیده‌های اجتماعی است و نظر به تأثیرگذاری تهدیدات سایبری بر حاکمیت و استقلال کشورها، این نگاشته سیاستگذاری جنایی در حوزه امنیت سایبری را نه تنها به راهبردی در مقابل جرم؛ بلکه رهیافتی در قبال آسیب‌های مختلف در عرصه‌های امنیتی–اجتماعی و نیازمند اقدامات پیشگیرانه خاص می‌داند؛ چراکه فقدان عنوان نقض امنیت سایبری وعدم اقدام در قبال مصادیق آن، اثرات غیرقابل جبرانی را بدنبال خواهد داشت. از منظر حقوق بین‌الملل برای مقابله با نقض امنیت سایبری و تعیین تکالیف اعضای جامعه بین‌المللی در برخورد با این پدیده چالش‌های متعددی وجود دارد. نه کنوانسیون خاصی و نه عرف بین‌المللی واحدی که دولت‌های قربانی حملات سایبری بدانند در برابر آن به چه اقداماتی متوسل شوند، وجود ندارد و آن چه مسلم است، حملات سایبری نیازمند قانون‌مندشدن و ایجاد رویه واحد در عرصه بین‌المللی است (Joner & Lotrent ,2001:864) به نقل از (Katanchi & Zakeri,2018:617). در کشور ما هرچند تا حدودی ماهیت پیشگیری از نقض امنیت سایبری و موانع و موجود روشن است؛ لکن سیاستگذاری پیشگیرانه با محدودیت همراه است و بخاطر شفاف‌نبودن مقررات موجود، نحوه به کارگیری این ابزارهای پیشگیرانه نیز مشخص نمی‌باشد (Jazayeri& Nematollahi& AmirianFarsani,2018:13). با این اوصاف، فقدان راهبرد مشخص در زمینه توسعه الکترونیک و امنیت فضای مجازی، فقدان متولی مشخص در حفاظت از داده‌های موجود در سامانه‌های نظامی و امنیتی کشور، فقدان سیاستگذاری مشخص ملی در آموزش، اطلاع‌رسانی و افزایش جرائم پنهانی در فضای مجازی و حرفه‌ای‌شدن بزه‌کاران با افزایش استفاده از شبکه‌های مجازی در دستگاه‌ها و نهادهای دولتی و خصوصی و فقدان سیاستگذاری نظارتی و امنیتی کارآمد در کشور

۱– سیاستگذاری عمومی و جنایی در ایران لزوماً محدود به الزام‌های قانونی نیست. فرمان‌های رهبری، مصوّبات مجمع تشخیص مصلحت نظام، قوانین بالادستی، نظیر برنامه‌های پنج ساله، قانون بودجه، مصوّبات شوراهای عالی مانند شورایعالی امنیّت ملّی، مبنای سیاستگذاری عمومی جنایی در ایران را تشکیل می‌دهند.

از چالش‌های پیشرو است (Hatef, 2007:14) به نقل از: (Zafari, et al, 2020:19). با توجه به این چالش‌ها، انتظار از سیاستگذاری پیشگیرانه این است که فرصت نقض امنیت را از طریق دشوار ساختن ارتکاب و افزایش خطرپذیری و کاهش آماج و قربانیان کاهش دهند. در این تعریف از سیاستگذاری جنایی، یک ساختار اعم از قانون‌گذاری و نظارت و اعمال و اجرا مدنظر قرار می‌گیرد. نکته مهم، توجه اندک محققان به شناسایی سیاستگذاری جنایی پیشگیرانه ملی و فراملی و نبود نظام مشترک بین‌المللی در قبال نقض امنیت سایبری و چالش‌های سیاستگذاری در ایران در پیشگیری از نقض امنیت سایبری است. از این‌رو با روش مطالعه تحلیلی-اسنادی[1] برآنیم تا با مراجعه به نوشتگان حقوق امنیت سایبری، اسناد موجود را شناسایی و تحلیل و پس از آن نمودهای سیاستگذاری پیشگیرانه اجتماعی، آثار و تبعات این رهیافت در ایران و سایر کشورها مورد بحث قرار گیرند. همچنین، از آنجاکه کشورهای چون آمریکا و روسیه و کشورهای اروپایی در حوزه امنیت سایبری پیشرو هستند، مطالعه این نظام‌های حقوقی و تطبیق با نظام حقوقی ایران، در جای خود نواندیشی این نگارش بوده است. سؤال اصلی تحقیق این است که رهیافت‌های پیشگیری اجتماعی در قبال نقض امنیت سایبری در ایران کدامند و این تدابیر در مقایسه با رهیافت‌های جهانی چگونه ارزیابی می‌گردند؟ به‌نظر می‌رسد سیاستگذاری کلان پیشگیری از نقض امنیتی سایبری در سیاستگذاری جنایی ایران فاقد رویکرد افتراقی[2] پیشگیرانه سایبری بوده و لذا مهم‌ترین سازوکارهای حمایت از امنیت سایبری در ایران، همسوکردن مقررات ناظر با قوانین و مقررات جهانی و یکدست‌نمودن قوانین و مقررات حوزه امنیت سایبر است.

مفهوم شناسی

مفاهیم مندرج در این نگارش خوانشی از عناوین حقوق سایبر با ابتناء بر رویکردهای امنیتی آن است. این موضوع هر چند دامنه پرتکراری از عناوین حقوقی و فنی را در برمی‌گیرد اما ماحصل آفرینش ترکیبی نوین و از جمله مباحث بسیار جدی جهان جدید مجازی است که به ترتیب مورد بحث قرار می‌گیرد.

فضای سایبر و امنیت سایبری

شورایعالی فضای مجازی در مصوبه «توسعه فضای مجازی سالم، مفید و امن» این فضا را این‌گونه تعریف می‌کند: «فضایی[3] است متشکل از شبکه‌های ارتباطی که در آن محتوا و خدمات مفید در چارچوب مبانی و ارزش‌های اسلامی و قوانین و مقررات کشور ارائه می‌شود و کاربران می‌توانند بر اساس ویژگی‌های جمعیتی از محتوا و خدمات مورد نیاز بهره‌مند شوند»[4] و هدف از این امر را تولید و توزیع محتوا و خدمات سالم مفید و امن مورد نیاز و ممانعت از نشر محتوا و خدمات مضر و ناسالم و ناایمن ذکر می نماید[5]. با این وصف حرکت کشورها به سمت نوگرایی باعث ایجاد انقلاب صنعتی چهارم[6] است، لذا امنیت در عصر جهانی‌شدن را باید در تعامل و تقابل با موضوعاتی چون «رژیم‌های بین‌المللی»، «هنجارها»، «توسعه»، «وابستگی متقابل»، «بازیگران بین‌المللی»، «سازمان‌های غیردولتی» تفسیر کرد (Alaei,2012:121). امنیت سایبری را می‌توان به عنوان راه‌حل‌های پیشنهادی (شامل قوانین، دستورالعمل‌ها، حراست‌های فناوری و غیره) برای تهدیدات ناشی از هک و به خطر انداختن

۱- روش اسنادی را تحلیل آن دسته از اسنادی می‌داند که شامل اطلاعات دربارهٔ پدیده‌هایی است که قصد مطالعهٔ آ نها را داریم. روش اسنادی مستلزم جستجویی توصیفی و تفسیری است و علاقهٔ پژوهش‌گر این است که از فهم مقاصد و انگیزه‌های اسناد و متون یا تحلیل‌های تأویلی یک متن خارج شود و آن را به‌عنوان زبان مکتوب و گفتمان نوشتاری نویسنده، پذیرفته و مورد استناد قرار دهد (صادقی و عرفان‌منش، ۱۳۹٤:٦٥).

۲- منظور از سیاستگذاری جنایی افتراقی تفکیک مبانی نظری، ماهوی، راهکارهای علمی و مقررات کلی درباره جرم و آسیب‌ها براساس معیارهای سن، شخصیت، سابقه کیفری و موقعیت بزه‌کاران و بزه‌دیدگان است. بدین ترتیب براساس هرکدام از معیارهای مذکور، محتوای متفاوتی در حوزه سیاستگذاری جنایی ایجاد می‌شود (شیری،۱٤۰۱:۹۵)

۳- از نگاه دیوید بل، فضای سایبر۳ یک شبکه گسترده جهانی امنیت سایبری است ۳ که شبکه‌های مختلف رایانه‌ای در اندازه‌های متعدد و حتی رایانه‌های شخصی را با استفاده از سخت‌افزارها و نرم‌افزارهای گوناگون و با قراردادهای ارتباطی به یکدیگر وصل می‌کند(Sharifi Holasu,2008:52). به نقل از Pourghahremani& Azimi,2018:410).

٤- کمیته دائمی پدافند غیر عامل در «سند راهبردی پدافند سایبری کشور» در ذیل ماده یک این سند، فضای سایبری را « شبکه‌های وابسته به یگدیگر از زیرساخت‌های فناوری اطلاعات، شبکه‌های ارتباطی سامانه‌های رایانه‌ای، پردازنده‌های تعبیه‌شده، کنترل‌کننده‌های صنایع حیاتی، محیط مجازی اطلاعات و اثر متقابل بین این محیط و انسان به منظور تولید، پردازش، ذخیره‌سازی، مبادله، بازیابی و بهره‌برداری از اطلاعات »٤ تعریف نموده است.

۵-مصوبه دوم جلسه ۲۲ مورخ ۱۳۹۳/۱۲/۱۰ شورای عالی فضای مجازی

6-Industrial Revolution (IR4.0)

سیستم‌های رایانه‌ای تعریف کرد (Bruno 2018:3). این نشان می‌دهد که امنیت سایبری به دلیل رشد سریع فناوری دیجیتال در کشورهای مدرن در سطح جهان به عنوان موضوع تحقیقاتی انتخاب می‌شود (Katanchi&pourghahremani ,2021:14). امنیت[1] سایبری نیز یکی از دسته‌بندی‌های امنیت بر پایه فضای سایبری است که در چهره درون سایبری بر دو دسته امنیت اطلاعات و امنیت سامانه تقسیم و ناظر بر سه دسته امنیت کاربران، امنیت زیرساخت‌های نهادهای عمومی و امنیت ملی است (Mahmoudzade & Ebrahim,2018:215). در سند راهبردی امنیت فضای تولید و تبادل اطلاعات کشور اشاره شده است که «فضای تبادل اطلاعات در معرض چالش‌ها، آسیب‌ها و تهدیدهای گوناگونی نظیر ارتکاب جرایم سازمان‌یافته، تخریب بانک‌های اطلاعاتی، حملات مختل‌کننده خدمات، جاسوسی، خرابکاری، نقض حریم خصوصی و نقض حقوق مالکیت معنوی قراردارد».

پیشگیری از نقض امنیت سایبری

صیانت امنیتی فضای سایبر موضوع بسیار مهمی است و بسیار جلوتر از امنیت فضای سایبر است، زیرا در امنیت فضای سایبر به دنبال یک سری از الزامات برای ایمنی و امنیت این فضا است، درحالی که صیانت امنیتی به دنبال موضوعاتی شامل ارزش‌ها، حریم خصوصی، سرمایه‌های مادی و معنوی، اسرار و اطلاعات، تخلفات و جرائم، خدمات و سرویس‌ها، قوانین و مقررات، پیاده‌سازی مراکز عملیات امنیت می‌باشد (Hossieni,2016:286). با این نگاه، نقض امنیت سایبری را می‌توان «تجاوز یا هنجارشکنی یا تهدید نسبت به یکی از پنج موضوع داده‌ها و اطلاعات، شبکه‌ها و سیستم‌های رایانه‌ای و مخابراتی، کاربران و مشترکان اینترنتی و نهایتاً موضوعات بیرون از دنیای سایبر که مرتکب به واسطه محیط سایبر درصدد تجاوز به آن برمی‌آید» (Aalipour,2013:72). امنیت سایبری، بازخوردی گسترده در تمامیت نظام سایبری و مختص به ماهیت این فضاست که نقض آن سبب بروز تهدیدات گسترده در زیرساخت‌ها و استقلال سایبری و تمامیت ساختار امن آن و فراتر از مفاهیمی چون جنگ سایبری و تروریسم و جاسوسی سایبری است[2].

سندشناسی سیاست جنایی سایبری

شناخت مفاهیم مرتبط و بررسی رویکردهای قانونی و انسجام‌بخش نظام سیاستگذاری جنایی در قبال نقض آن نیازمند احصاء اسناد داخلی و جهانی در این عرصه است؛ لذا مراجع دخیل و اسناد مهم را بازخوانی خواهیم نمود.

اسناد سایبری داخلی

رهیافت‌های سیاستگذای نقض امنیت سایبری در ایران در اسنادی از جمله سند چشم انداز ایران ۱۴۰۴ ، سیاست کلی شبکه اطلاع‌رسانی، سیاست کلی نظام برای رشد و توسعه فناوری در کشور[3] ، نظام جامع توسعه فناوری اطلاعات کشور[4]، سند راهبردی امنیت فضای تولید و تبادل اطلاعات کشور[5] ، قانون برنامه پنجم و ششم توسعه جمهوری اسلامی ایران، شرح وظایف پلیس فضای تولید و تبادل اطلاعات، قانون جرایم رایانه‌ای، نظام جامع توسعه فناوری اطلاعات کشور، سند تبیین الزامات شبکه ملی اطلاعات، مصوبات سازمان تنظیم مقررات و ارتباطات رادیویی، سند سیاست‌ها و اقدامات ساماندهی پیام‌رسان‌های

۱- در زمینه تأثیر فناوری اطلاعات و ارتباطات بر مفهوم امنیت دو دسته از نظریه پردازان وجود دارند. گروهی بر این عقیده‌اند که این ابزار به بهترین وجه می‌تواند مفهوم امنیت را کمرنگ و مفهوم صلح را جایگزین آن کند. گروه دوم که همان نظریه‌پردازان رئالیسم کلاسیک هستند؛ معتقدند که هرچند فناوری اطلاعات و ارتباطات گسترش یافته است اما مفهوم کلاسیک امنیت به معنای امنیت دولت در قالب نظامی و جریان اطلاعات رسمی همچنان جایگاه خود را حفظ کرده است (Eriksson and Giacomello,2006:222-223)

۲- توجه به این نکته ضروری است که سیاست جنایی بین‌المللی رفتارهای منجر به نقض امنیت سایبری را ناقض حقوق بین‌الملل عمومی می‌داند و ناتو طی توافقی در زمینه خط مشی مشترک سایبری اعلام نمود که هرگاه حمله سایبری علیه یکی از دولت‌های عضو ناتو به وقوع بپیوندد مطابق ماده ٤ معاهده سازمان پیمان اتلانتیک با آن برخورد خواهد شد.

۳- در ٤ ماده و ۲۵ بند در ۱۳۸٦ به تصویب هیات وزیران رسید.

٤- در جلسه ۸٦/۸/۱۹ کمیسیون راهبردی شورای عالی فناوری اطلاعات کشور مدنظر قرار گرفته است.

۵- معاونت فناوری اطلاعات دفتر امور زیربنایی فناوری اطلاعات در سال ۱۳۸٦ به استناد بند "ج" ماده ٤٤ قانون برنامه چهارم توسعه اقتصادی، اجتماعی و فرهنگی جمهوری اسلامی ایران، سند راهبردی امنیت فضای تبادل اطلاعات را به منظور تضمین هم‌گرایی و نظام‌بندی برنامه‌های کشور در زمینه امنیت فضای تبادل اطلاعات را به عنوان سند بالادستی برای کلیه برنامه‌های بخشی و فرابخشی تدوین نمود.

اجتماعی[۱]، سند راهبردی پدافند سایبری کشور[۲]، سند نظام هویت معتبر در فضای مجازی کشور مصوب شورایعالی فضای مجازی و طرح امن‌سازی زیرساخت‌های حیاتی در قبال حملات سایبری سال ۱۳۹۷ مرکز مدیریت راهبردی افتا نهاد ریاست جمهوری به چشم می‌خورند که هریک به نوعی موضوعاتی را بیان اما تاکنون علی‌رغم این تکثر، سیاستگذاری جنایی جامعی در قبال نقض امنیت سایبری اتخاذ نشده است و شیوه حکمرانی کنونی فضای مجازی از رویکردی غیرمشارکتی واز بالا به پایین پیروی می کند (Khoshnevis,2018:37).

اسناد سایبری خارجی

نقض امنیت سایبری مستلزم صیانت از داده‌ها و اطلاعات سایبری است. از این‌رو، کشورهای پیشرو سیاست صیانت از داده‌های شخصی را در دستور کار خود قرارداده و ضمانت اجراهای حقوقی و کیفری متعددی را وضع کرده‌اند. نخستین دستورالعمل شورای اروپا درباره حمایت از داده در سال ۱۹۹۵، با عنوان «حمایت از اشخاص در جریان پردازش داده‌های شخصی و جریان آزاد اطلاعات» به تصویب رسید[۳]. در قبال نقض امنیت سایبری اسناد و مقاوله‌نامه‌های بین‌المللی و قوانین داخلی متعددی وضع شده است. به‌عنوان مثال سازمان‌ها و مجامع جهانی که ناظر بر«هنجارهای رفتار مسئولانه دولت‌ها در فضای سایبری» می‌باشند؛ شامل کنوانسیون بوداپست (۲۰۰٤)، تلاش‌های علمی گروه خبرگان حکمرانی سازمان ملل متحد[٤]، سند راهبرد بین‌المللی ایالات‌متحده برای فضای سایبری (۲۰۱۱)، یافته‌های موسسه مطالعات امنیتی شرق و غرب[٥] (۲۰۱۱)، مطالعات تطبیقی کنوانسیون‌های لاهه و ژنو در حوزه مورد بحث، دستورالعمل تدوین‌شده در سازمان پیمان آتلانتیک شمالی (ناتو) تحت عنوان «تالین (۲۰۱۳)»، طرح بلوک چین و روسیه با عنوان «کدهای رفتاری بین‌المللی برای امنیت اطلاعات» (۲۰۱۵)، استراتژی وزارت امور خارجه امریکا در حوزه سیاست‌های بین‌المللی (۲۰۱٦)، اعلامیه گروه۷ در خصوص«رفتار مسئولانه دولت‌ها در فضای سایبری» در ایتالیا (۲۰۱۷) ، فرمان اجرایی ترامپ در حوزه تقویت امنیت سایبری شبکه‌ها و زیرساخت‌های فدرال (۲۰۱۷) برخی از اسناد قابل توجه می‌باشند[٦]. در اسناد بین‌المللی در حوزه امنیت سایبری، سندی که در اجلاس سران ناتو در ۲۰ نوامبر ۲۰۱۰ در لیسبون پرتغال به تصویب رسید از جمله موارد حائز اهمیت است و فعالیت‌های موثری را در سه زمینه دفاع دسته جمعی، مدیریت بحران و همکاری امنیتی متمرکز ساخته است (Ahmadian& Bloki& Searmifar, 2019:1). اتحادیه بین المللی مخابرات[۷] از جمله نهادهای بین‌المللی دیگر در زمینه امنیت سایبری است. اجلاس جهانی سران درباره جامعه اطلاعاتی[۸] در سال ۲۰۱۹ که در آن فرم چند ذینفعی اجلاس سالانه جامعه اطلاعاتی، پیاده‌سازی خطوط اقدامات را برای اهداف توسعه پایدار تسهیل و موضوعات مهمی مانند حذف شکاف دیجیتالی، امنیت سایبری و اخلاق و همچنین فناوری‌های نوین نظیر هوش مصنوعی، اینترنت اشیاء، بلاکچین، G۵ مطرح شد[۹](Vamala,2017:12). در همین راستا، اتحادیه بین‌المللی ارتباطات از راه دور (IUT) سازمان ملل متحد شاخص امنیت سایبری جهانی (GCI) را در اوریل ۲۰۱٤ برای سنجش وضعیت

۱- اهمیت پیام‌رسان‌های اجتماعی و توان در نقض امنیت سبب شد شورایعالی فضای مجازی سند « سیاست‌ها واقدامات ساماندهی پیام‌رسان‌های اجتماعی» را در تاریخ ۱۳۹٦/۳/۱۳ تصویب نماید. که هدف از آن، تعیین سیاست‌ها و اقدامات لازم برای ساماندهی فعالیت پیام‌رسان‌های اجتماعی، با هدف فراگیری پیام‌رسان‌های اجتماعی داخلی و ساماندهی پیام‌رسان‌های خارجی عنوان شده است.

۲- کمیته دائمی شورای عالی پدافند غیر عامل کشور در جلسه مورخ ۱۳۹٤/۲/۲۹ به استناد ماده ۸ اساسنامه سازمان پدافند غیرعامل کشور مصوب رهبری «سند راهبردی پدافند سایبری کشور» را تصویب نمود.

3- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data

4- UNGGE2010

5- East West Institute (EWI)

٦- به نقل از سایت مرکز ملی فضای مجازی،۱۳۹۹

۷- این اتحادیه از زمان شکل‌گیری در سال ۱۸٦۵، نقش مهمی در زمینه ارتباطات راه دور، امنیت اطلاعات و تعیین استانداردهای جهانی با ظرفیت‌های مختلف ایفا کرده است. فعالیت‌های زیر از جمله اقدامات این اتحادیه قلمداد می‌شود: اجلاس جهانی در مورد جامعه اطلاعاتی و دستور کار امنیت سایبری جهانی (GCA) و اقدام سطر C5در اجلاس جهانی جامعه اطلاعاتی و ابتکار عمل حفاظت از "کودکان برخط". این سند مسائلی را مورد توجه قرار می‌دهد که کشورها در بازنگری یا فرآیند پربارکردن و غنی‌سازی راهبردهای امنیت ملی سایبری، باید به آن بپردازد (وامالا، ۱۳۹٦:۱٦).

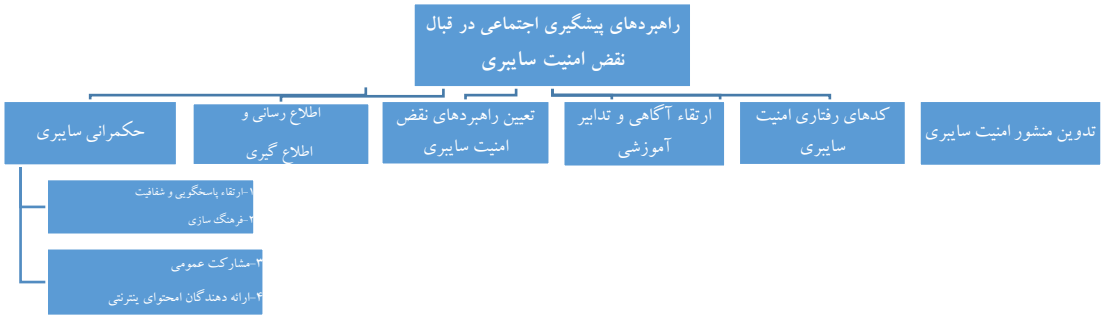
8- Information Society

۹- همچنین در نتیجه نشست‌های عمومی سازمان ملل نیز این نهاد در پنج قطعنامه مهم، به بازتاب نظر خود در باره امنیت سایبری پرداخته است که شامل A/RES/55/63: مبارزه با استفاده مجرمانه از فناوری ارتباطات و اطلاعات و A/RES/56/121: مبارزه با استفاده مجرمانه از فناوری ارتباطات و اطلاعات و A/RES/57/239: فرهنگ امنیت سایبری و A/RES/ 57/239: زیرساخت‌های حیاتی و A/RES/57/239: فرهنگ جهانی امنیت سایبری می‌باشند.

امنیت سایبری در سراسر جهان راه‌اندازی کرده است. شاخص‌های توسعه امنیت سایبری در هر کشور می‌تواند در موارد ذیل خلاصه شود: اقدامات قانونی مانند تصویب مقررات کیفری متناسب؛ اقدامات فنی مانند اعطای گواهینامه‌ها و تعیین استانداردها؛ اقدامات سازمانی مانند طراحی سیاست نقشه راه و سازمان‌های ناظر؛ ظرفیت‌سازی در زمینه توسعه نیروی انسانی و همکاری درون سازمانی یا برون‌مرزی (Sak& Chaisari ,2021:40).

راهبردهای پیشگیرانه سایبری در نظام‌های حقوقی ایران و جهان

گرچه سیاستگذاری جنایی پیشگیرانه مبتنی بر رویکردهای مختلفی از جمله تقنینی و قضائی و اجرایی و وضعی و اجتماعی است لکن در این مقاله از میان تدابیر گوناگون، الگوی پیشگیری اجتماعی به سبب بعد کاربردی و رهیافت‌های مندرج در ارتباط با پیشگیری از نقض امنیت سایبری بررسی و جهت تشحیذ ذهن مخاطبین؛ تقسیم‌بندی مطالبی که به نظر نگارندگان، نمودهای از پیشگیری اجتماعی است، ترسیم می‌گردد.



نمودار ۱ – راهبردهای پیشگیری اجتماعی در قبال نقض امنیت سایبری.

راهبردهای پیشگیرانه اجتماعی در قبال نقض امنیت سایبری

در پیشگیری اجتماعی، هدف زدودن انگیزه‌های مجرمانه از طریق آموزش و فرهنگ‌سازی است. تدابیری که در راستای پیشگیری اجتماعی به اجرا در می‌آید، می‌کوشد زمینه‌های فردی یا اجتماعی را که سبب بروز انگیزه‌های مجرمانه می‌شود، برطرف کند. لذا این نوع پیشگیری شامل آن گروه از تدابیری است که با مداخله در فرایند بهبود شرایط افراد و سالم‌سازی محیط اجتماعی از وقوع بزه ممانعت می‌نماید و شامل مجموعه اقدامات پیشگیرانه‌ای است که به‌دنبال حذف یا خنثی‌کردن عواملی مؤثر در نقض امنیت باشد. به عبارت دیگر، پیشگیری راهبردی است که برخورد با علل ریشه‌ای اقدامات مجرمانه و بزه‌دیدگی را مدنظر قرار می‌دهد (Javan-Jaafari&Sodomandrad,2014:37), (Grant, 2015: 5). توضیح اینکه پیشگیری اجتماعی به رشدمدار و اجتماع‌مدار منقسم است. مورد نظر ما پیشگیری اجتماعی در قبال نقض امنیت سایبری است که در آن به تعریف کدهای رفتار اجتماعی و فردی، اطلاع‌رسانی و اطلاع‌گیری، حکمرانی سایبری، پاسخگویی و شفافیت و... توجه شده است و هدف نگارنده بررسی و تبیین این رویکردهاست. باید اشاره داشت بسیاری از طرح‌ها و برنامه‌های پیشگیری بدون ارزیابی اجرا و پس از اجرا نیز میزان اثربخشی آن‌ها سنجیده نمی‌شود. همچنین استفاده بیش از اندازه از فیلترینگ و معرفی آن به عنوان یکی از راهکارهای درست برای پیشگیری از نقض امنیت سایبری، نه تنها ممکن است موفقیت آمیز نباشد، بلکه پیامدهای ناخواسته‌ای نیز به بارخواهد آورد که اثربخشی این اقدامات را دچار تردید می‌کند(Shamlou, Baqi&Kazhni-Joibari,2018:13). افزون براین که ضعف ارتباط میان بخش خصوصی و دولتی به همراه سهم ناچیز مردم و انجمن‌های مردم نهاد، از دیگر موانع اثربخشی مداخله‌های پیشگیرانه در این حوزه به شمار می‌روند. لازم بذکر است که اعمال بدون شرایط و ضوابط فیلترینگ توسط حاکمیت‌ها سبب کاهش محسوس اثربخشی پیشگیری مشارکتی در قبال جرایم و آسیب‌های اجتماعی می‌گردد. فیلترینگ و سانسور دولتی به معنای خلع سلاح کارگزاران پیشگیری و عموم مردم در فضای مجازی است و دولت‌های که به زعم خود در راستای صیانت از امنیت درصدد استفاده بیش از حد از فیلترینگ برآیند، ضمن افزایش هزینه کاربران، اعتماد آن‌ها را ضعیف و استفاده از فیلترشکن‌ها را ترویج می‌نمایند که خود موجب دسترسی غیر مجاز به حریم خصوصی افراد و کاهش امنیت آن‌ها می‌گردد.

حتی اگر براین باور باشیم که نقض امنیت سایبری و پیشگیری از آن در ابعاد امنیتی- اجتماعی- فرامرزی- اقتصادی- نظامی دارای اهمیت است، نمی‌توان و نباید با حذف شهروندان، هوشمندی مجازی و هوش دیجیتال آنان در دنیای مبتنی بر اینترنت اشیاء را خدشه‌دار نمود.

تدوین منشور امنیت سایبری: به فراخور تغییرات بنیادین فناوری، طبعاً حقوق‌دانان نیز باید برای هماهنگی با این فناوری و عقب نماندن از آن، به ارائه ضوابط حقوقی جهت پیشگیری از این تغییرات اقدام نمایند(Javan jafari,2010:179). اما ایرادی که به عنوان مانعی در اتخاذ سیاستگذاری‌های یکدست قابل توجه و نیازمند چاره‌اندیشی است وجود نهادهای موازی تصمیم‌ساز در عرصه فناوری اطلاعات بوده که در مصوبه شماره ۱ جلسه ۵۳ مورخ ۱۳۹۷/۷/۳۰ شورایعالی فضای مجازی با عنوان تعیین تکلیف وظایف اجرایی شورای عالی انفوزماتیک مورد رایانه‌ای، کمیته حق اختراع، صلاحیت نظارت بر نظام صنفی رایانه‌ای و... به وزارت ارتباطات و فناوری اطلاعات محول شده است. در سند سیاست و الزامات توسعه امنیت فضای مجازی کشور خدمات امنیتی را «هرگونه خدماتی که موجب تأمین امنیت در فضای مجازی گردد از جمله؛ خدمات فنی مهندسی، مدیریت امنیت اطلاعات، احراز هویت، رصد و پایش، پالایش، بررسی و ارزیابی براساس استانداردها و دستورالعمل‌ها در حوزه امنیت فضای مجازی را تعریف و زیرساخت‌های مدنظر سیاستگذاری سایبری از جمله؛ مراکز ویژه، مراکز حیاتی، مراکز حساس، مراکز مهم را بیان می‌نماید. اتحادیه بین‌المللی مخابرات در سطح جهانی، اولین نسخه از راهنمای راهبرد امنیت سایبر را در سال ۲۰۱۸ و نسخه اصلاحی این شاخص را برای اندازه‌گیری کمّی سطح پیشرفت امنیت سایبری در کشورها با هدف نهایی تقویت فرهنگ جهانی این امنیت طراحی کرده است. این شاخص شامل پنج مؤلفه قوانین و مقررات[1]، اقدامات فنی[2]، ساختارهای اجرایی و سازمانی[3]، ظرفیت‌سازی[4]، همکاری ملی و بین‌المللی[5] می باشد. اشاره به موارد مذکور بیانگر نوعی تطابق در منشورهای اعلامی سیاستگذاری جنایی ایران و سطح بین‌الملل آن در بعد فنی و اجرایی است.

کدهای رفتاری امنیت سایبری: تحولات دنیای سایبر نقض اصولی از جمله؛ نقض حریم خصوصی، نقض حقوق مالکیت و معنوی را موجب شده است و قوانین کیفری در اغلب کشورها نتوانسته آن‌طور که باید از ارتکاب این نقض پیشگیری نمایند (Pourghahremani,2017:24). اما توسعه و گسترش اینترنت و نیز بهره‌مندی از امکانات و ابزار نوین همچون شبکه‌های اجتماعی نیازمند یک نظام حقوقی مدون و منسجم است که در آن کدهای رفتاری و عمل مشخص با وجود تأمین آزادی بیان در این شبکه‌ها، مانع از سوء استفاده احتمالی از آزادی بیان شده و از آن طریق امنیت ملی را نیز حفظ کند (Bidarvand & Pourghahreman & beigi,2020:43). بنابراین برای مقابله با نقض گزارشات امنیت سایبری، نیازمند تعریف کدهای رفتاری برای اشخاص حقیقی و حقوقی هستیم. این کدها صرف‌نظر از حوزه و محیطی که برای آن تدوین می‌شوند، در مقام تبیین رهنمودهای مورد نظر فهرستی از بایدها و نبایدها را به عنوان الگوهای لازم بیان می‌دارند و با ارائه آگاهی مطلوب در توانمندی کاربران در حفاظت از خود و برنامه‌ریزی برای بکارگیری ابزارهای امنیتی نقش شایان توجهی را بازی می‌کنند (Monfared,2012:158). به‌نظر می‌رسد ایجاد تعاریف برای کاربران تحت عنوان کدهای رفتای در تمامی اسناد بالادستی و مصوبات ابلاغی نمونه‌های از پیشگیری اجتماعی است. در واقع مهم‌ترین هدفی که از تدوین این کدها دنبال می‌شود، تعریف رفتار صحیح، از بین بردن انگیزه‌های سودجویانه مادی در نقض امنیت سایبری است. شورایعالی فضای مجازی، در هشتمین جلسه مورخ ۱۳۹۱/۶/۲۵، براساس ماده ۹ اساسنامه مرکز ملی فضای مجازی، شرح وظایف و اختیارات و اعضای «کمیسیون عالی تنظیم مقررات فضای مجازی کشور» به بیان کدهای مهمی پرداخته که بعد امنیت سایبری در آن‌ها نمایان است از جمله:

۱ـ تصویب معیارها، سیاست‌ها و نظام‌های کنترل کیفی و فنی در همه زمینه‌های فضای مجازی از جمله امنیتی و محتوایی و همچنین سیاست‌ها و معیارهای ارائه محتوا، خدمات، توسعه و بهره‌برداری در فضای مجازی کشور در چارچوب مصوبات شورایعالی.

1- Legal Measures
2- Technical Measures
3- Organizational Measures
4- Capacity Building
5- Cooperation

۲ـ سیاستگذاری، هماهنگی، تصویب ضوابط کلی صدور مجوز فعالیت و بهره‌برداری در چارچوب مصوبات شورایعالی برای ارائه هرگونه فعالیت در فضای مجازی شامل محتوا، خدمات و زیرساخت‌های فنی و ارتباطی. هم‌چنین سند چشم انداز بیست ساله جمهوری اسلامی ایران تعیین‌کننده محورهای پیشرفت ایران و راهبرد امنیتی و سیاست خارجی کشور برای رسیدن به جایگاه اول منطقه‌ای در سال ۱۴۰۴ است. در این سند بر تعامل سازنده و متوازن در روابط بین‌الملل و در سیاست‌های کلی نظام در فضای تولید و تبادل اطلاعات کشور و ارتقای سطح همکاری‌های بین‌المللی در زمینه امنیت فضای مجازی تأکید شده است (Alaei, 2012:121) که نوعی کد رفتار دولتی سایبری قلمداد می‌گردد. گروه خبرگان حکمرانی در حوزه اطلاعات و مخابرات در زمینه امنیت بین‌المللی (۲۰۱۳) که توسط مجمع عمومی سازمان ملل تشکیل شده است، در گزارش خود بیان می‌کند که حاکمیت دولت‌ها و هنجارها و اصول بین‌المللی ناشی از آن با کدهای رفتاری دولت‌ها در حوزه فن‌آوری‌های اطلاعاتی و ارتباطاتی و صلاحیت قضایی آن‌ها در خصوص زیرساخت‌های ICT درون سرزمین‌ها، قابل‌اعمال می‌باشد. آن‌ها در گزارش اجماعی نهایی خود در سال (2013) این‌گونه بیان می‌کنند که «قوانین بین‌المللی، به‌ویژه منشور سازمان ملل، به منظور حفظ صلح و ثبات و ترویج محیط فن‌آوری اطلاعات و ارتباطات باز، امن، صلح‌آمیز و در دسترس، قابل اعمال و ضروری است». در عرصه جهانی، طرح بلوک چین و روسیه سال(۲۰۱۵) با عنوان «کدهای رفتاری بین‌المللی برای امنیت اطلاعات» رفتار مسئولانه دولت‌ها را بر محور «انتشار اطلاعات» و «حق کنترل مستقل فن‌آوری‌های اطلاعاتی و ارتباطاتی» در شرایطی که امنیت ملی یک کشور به خطر می‌افتد را تعریف کرده است. به عنوان نمونه در کنفرانس امنیتی RSA [1] در سال ۲۰۱۸؛ هدف، حفاظت از امنیت فضای سایبری در برابر حملات نقض‌کننده امنیت سایبری توسط دولت‌ها و مدیریت رفتار دولت‌ها در این فضا از طریق ایجاد قواعد و هنجارهای ناظر بر رفتار مسئولانه دولت‌ها در فضای سایبری و نیز ایجاد هنجارهای ناظر بر مسئولیت‌های مشترک شرکت‌های فن‌آوری در برابر مشتریان و شهروندان در هرکجای جهان اعلام گردیده است (Vamala, 2017:40).

ارتقای آگاهی و تدابیر آموزشی: کارآمدی اقدامات پیشگیری اجتماعی انعکاس مستقیم آموزش مفاهیم امنیت سایبر است و رویکرد انفعالی در این‌باره سایر اقدامات کنشی را ناکارآمد می‌نماید. ماده ۱۰۹ قانون برنامه ششم توسعه کشور و نظام ملی پیشگیری و مقابله با حوادث فضای مجازی مصوب شورایعالی فضای مجازی در سال ۱۳۹۶ در سیاستگذاری کلی پیشگیرانه به اهمیت آموزش توجه نموده و از جمله «ارتقاء سطح دانش و ظرفیت‌های علمی، پژوهشی، آموزشی و صنعتی کشور برای تولید علم و فناوری مربوط به امنیت اطلاعاتی ارتباطی» را مبنا قرار می‌دهد. همچنین در راستای ارتقاء امنیت سایبری، دولت را مکلف به افزایش سطح آموزش سایبری مدیران و کارکنان دستگاه‌های اجرایی به منظور جلوگیری از نفوذ و مختل‌نمودن سامانه نرم‌افزاری دستگاه ذی‌ربط و توسعه آمادگی‌ها نموده است. بر اساس بند «ب» ماده ۱۰ قانون برنامه پنج ساله پنجم توسعه جمهوری اسلامی ایران، دولت موظف است سازوکارهای اجرایی لازم برای ارتقای آگاهی، دانش و مهارت همگانی به منظور سازمان‌دهی فضای رسانه‌ای کشور، مقابله با تهاجم فرهنگی بیگانه و جرایم و ناهنجاری‌های رسانه‌ای را فراهم و اجرایی کند. در ایران، رویکرد عملی در طرح «آپا[2]» به منظور ارتقای دانش فنی کشور و توسعه دانش مدیریتی حوادث امنیتی از سال ۱۳۸٤ در پژوهشکده امنیت ارتباطات و فناوری اطلاعات مرکز تحقیقات مخابرات ایران شروع و بهره‌برداری از آن از آواخر سال ۱۳۸٦ آغاز شده است[3]. در این طرح آگاهی‌های امنیتی برای مقابله با اختلالات و حوادث فضای رایانه‌ای به‌عنوان الگوی مبتنی بر دانش‌افزایی ارائه می‌شود (Bahremand&Davoudi,2018:40).

در این راستا قطعنامه ۱۳۰، کنفرانس عالی ۲۰۱۰ اتحادیه بین‌المللی مخابرات کشورهای عضو را به توسعه بیشتر برنامه‌های تحصیلی و آموزشی برای بهبود آگاهی کاربران از خطرات موجود در فضای سایبر دعوت می‌کند. نیازمندی آموزش و مهارت

۱- Rivest Shamir Adleman در بحث رمزنگاری، آر.اس.ای (RSA) شیوه‌ای برای رمزنگاری به روش کلید عمومی (Public Key) است. این روش نخستین روش مورد اعتماد در بین روش‌های رمزنگاری دیگر است و یکی از بزرگ‌ترین پیشرفت‌ها در زمینه رمزنگاری به حساب می‌آید. آر.اس.ای همچنان به صورت وسیعی در تبادلات الکترونیکی استفاده می‌شود و در صورت استفاده درست با کلیدهای طولانی کاملاً امن به نظر می‌رسد.این روش نخستین بار در سال ۱۹۷۷ توسط رونالد ریوست، آدی شامیر و لئونارد آدلمن در دانشگاه ام آی تی مطرح شد. اصطلاح آر.اس.ای نیز از حروف ابتدای نام آن‌ها گرفته شده است. دانشگاه MIT حق اختراع این روش را به نام خود ثبت کرد. این حق اختراع در ۲۱ سپتامبر سال ۲۰۰۰ میلادی منقضی شد.

۲- مخفف «آگاهی‌رسانی، پشتیبانی، امداد رایانه‌ای» و نامی بومی معادل CERT.

3- Https://esfahan.ict.gov.i

به هدف ششم اهداف راهبردی «دستور کار امنیت سایبری جهانی» می‌پردازد که توسعه راهبرد «آسان‌نمودن و ظرفیت‌سازی انسانی و سازمانی» برای بالابردن سطح دانش در بخش‌ها را ایجاب می‌نماید(Vamala,2017:142). شاید بتوان گفت اقدام تعدادی از کشورها ازجمله (نیوزیلند، هلند، کره، چین، ایالات متحده آمریکا) در تأسیس مراکز ملی امنیت سایبری و یا کشورهای دیگری همچون (استرالیا، آلمان[1]، فنلاند[2]) که در حال ایجاد این مراکز به عنوان ایجاد همکاری میان بخش دولتی و خصوصی هستند، می‌تواند در جهت ایجاد همکاری و هماهنگی لازم در میان بخش‌های عمومی و خصوصی جهت ارتقاء دانش و افزایش آگاهی بوده که به دفاع در برابر تهدیدات ناقض امنیت سایبری و بالا بردن سطح آگاهی‌ها نسبت به اقدامات پیشگیرانه سایبری کمک نمایند(Jahanshiri&Taghipour& Pourmanafi, 2015:177).

تعیین راهبردهای نقض امنیت سایبری: آنچه مسلم است، حملات سایبری منجر به نقض امنیت سایبری نیازمند قانون‌مند شدن ایجاد رویه واحد در عرصه بین‌المللی است چراکه؛ هر دولتی که متوسل به اقدامات دفاعی یا تهاجمی در این حوزه می‌شود، لازم است که حدود و ثغور خطرات و حقوق و تکالیف ناشی از اقدام خود را بازشناسد(Lotrionte, 2001: 863-86). در سند «سیاست‌ها و اقدامات ساماندهی پیام‌رسان‌های اجتماعی» در ماده ۱ تحت عنوان سیاست‌ها به «شش» موضوع از جمله در بند «ب» و «ج» به راهبردهای چون «قابلیت پیشگیری از جرایم و مدیریت و اعمال قوانین و مقررات کشور» و «اعتمادسازی و صیانت از حقوق شهروندی، حریم خصوصی، امنیت ملی و عمومی» و «ذخیره‌سازی و پردازش داده‌های عظیم مرتبط با فعالیت پیام‌رسان‌های اجتماعی در داخل کشور و ممانعت از دسترسی غیرمجاز به آن‌ها» اشاره شده است. در سند نظام هویت معتبر در فضای مجازی کشور مصوب شورایعالی فضای مجازی در ماده ۲ الزامات زیست‌بوم هویت معتبر در فضای مجازی در ۱۱ بند مورد توجه واضعان قرار گرفته‌است که مهم‌ترین موارد تبیین‌کننده امنیت سایبری در آن عبارتند از «تأمین سطوح اعتبار و اعتماد در تأمین اطلاعات هویت دیجیتالی به تناسب نوع تعامل و صیانت از حریم خصوصی اشخاص و حقوق عمومی جامعه و رعایت امنیت اطلاعات هویت دیجیتالی و تناسب آن با نوع تعامل از طریق ایجاد چارچوب مبادله قابل اعتماد، اعطای گواهی موثق و مرتبط بودن اطلاعات هویتی پایه فضای مجازی با فضای فیزیکی و تضمین صحت، تمامیت، اعتبار، انکارپذیری و استنادپذیری هویت موجودیت‌های فضای مجازی به تناسب نوع تعامل و افزایش شفافیت و کاهش گمنامی در فضای مجازی و ارتقاء و استمرار فرآیندها احراز هویت در فضای مجازی به‌عنوان راهبردهای اساسی نظام مقابله با نقض امنیت سایبری» توجه گردیده و ماده ۱۰۹ قانون برنامه ششم توسعه کشور و نظام ملی پیشگیری و مقابله با حوادث فضای مجازی مصوب شورای عالی فضای مجازی در سال ۱۳۹۶ در بند «۱»، ایجاد نظام جامع و فراگیر در سطح ملی و سازوکار مناسب برای ایمن‌سازی ساختارهای حیاتی و حساس و مهم در حوزه فناوری اطلاعات و ارتباطات و ارتقاء مداوم امنیت شبکه‌های الکترونیکی و سامانه‌های اطلاعاتی و ارتباطی در قانون‌گذاری حفاظتی از امنیت سایبری را پایه‌ریزی کرده‌است. سازمان ملل متحد به اهمیت امنیت سایبری توجه داشته و قطعنامه «مبارزه با سوء استفاده کیفری از فناوری اطلاعات» را تصویب[3] و همچنین در دوم دسامبر سال‌های ۲۰۰۸ و ۲۰۰۹ دو قطعنامه دیگر با نام‌های مشابه «توسعه‌ها در زمینه اطلاعات و ارتباطات الکترونیک در بستر امنیت بین‌المللی» را به تصویب رسانید. در حوزه سیاستگذاری جنایی بین‌الملل، اولین قطعنامه در ارتباط با امنیت سایبری را روسیه در سال ۱۹۹۸، به کمیته اول مجمع عمومی سازمان ملل ارائه کرد. آمریکا نیز در مقام مقابله، قطعنامه‌هایی در کمیته های دوم و سوم طرح نمود. پیش نویس اولین کنوانسیون در مورد امنیت سایبری را روس‌ها در اجلاس ایکاترین بورگ در سال ۲۰۱۱ رونمایی کردند که غرب با آن مقابله کرد. اولین کردارنامه در مورد امنیت سایبری از طرف شانگ‌های صادر شد که غربی‌ها از آن استقبال نکردند. روس‌ها در سال ۲۰۱۷ از اولین پیش‌نویس بین‌المللی در زمینه جرایم سایبری رونمایی کردند که بررسی این پیش‌نویس، همچنان در دستور کار دولت‌ها می‌باشد. مقررات حفاظت از داده اروپا در راستای ارائه تعریفی از حریم خصوصی و جهت پیشگیری از نقض این حریم به عنوان یکی از مصادیق امنیت سایبری مقرره‌های خاصی را پیش‌بینی نموده است. قانون حفاظت از اطلاعات اشخاص و شرکت‌ها GDPR[4] از ماه می ۲۰۱۸ در تمامی کشورهای اروپایی اجباری و لازم‌الاجرا شده است. تدوین این قانون ٤ سال زمان برده است و بر اساس این قانون، حفاظت از اطلاعات شخصی افراد و

1- Cyber Security Strategy for Germany – February 2011
2- Finland's Cyber Security Strategy 2013.
3- UN General Assembly Resolution A/RES/56/121, "Combating the criminal misuse of information technologies" (19 December 2001)
4- General Data Protection Regulation

شرکت‌ها (اعم از اطلاعات دیجیتال یا اسناد پرینت شده و همچنین اعم از مشتریان شرکت‌ها یا حتی خود کارمندان شرکت‌ها) تعریف و قانون‌مند و راهبری شده است (Ghannad&Aligholi, 2019:1).

اطلاع رسانی و اطلاع‌گیری: به‌نظر می‌رسد اطلاع‌رسانی، مبتنی بر نگاه پیشگیرانه اجتماع‌مدار است. پیشگیری اطلاعی در خصوص امنیت سایبری در فضای مجازی می‌تواند تأثیر بسزایی در این مقابله داشته باشد. امنیت در فضای سایبری دامنه‌های گسترده‌ای دارد که ضرورت اطلاع‌رسانی را آشکار می‌کند(Bahremand & Davoudi,2018:39). اهمیت اطلاع‌رسانی، دولت را به حفاظت از اطلاع‌رسانی واداشته در بند۱۱ از سیاست های کلی نظام در امور پدافند غیرعامل ابلاغی ۱۳۸۹، به کارگیری اصول و ضوابط پدافند غیرعامل در مقابله با تهدیدات نرم افزاری و الکترونیکی و سایر تهدیدات جدید دشمن به منظور حفظ و صیانت شبکه‌های اطلاع‌رسانی، مخابراتی و رایانه‌ای تأکید شده است. ابلاغیه رهبری در سال ۱۳۸۰ راجع به شبکه‌های اطلاع‌رسانی رایانه‌ای نشان از فاصله میان اهداف کلان و اقدامات لازم‌الاجرا و زمینه اطلاع‌رسانی دارد. در این ابلاغیه مواردی از جمله ایجاد، ساماندهی و تقویت نظام ملی اطلاع‌رسانی رایانه‌ای و اعمال تدابیر و نظارت‌های لازم به منظور صیانت از امنیت سیاسی، فرهنگی، اقتصادی، اجتماعی و جلوگیری از جنبه‌ها و پیامدهای منفی شبکه اطلاع‌رسانی، توسعه کمی و کیفی شبکه اطلاع‌رسانی ملی و تأمین سطوح انواع مختلف خدمات و امکانات این شبکه برای کلیه متقاضیان به تناسب نیاز آنان و با رعایت اولویت‌ها و مصالح ملی، ایجاد دسترسی به شبکه‌های اطلاع‌رسانی جهانی صرفاً از طریق نهادها و موسسات مجاز، حضور فعال و اثرگذار در شبکه‌های جهانی، ایجاد و تقویت نظام حقوقی و قضائی متناسب با توسعه شبکه‌های اطلاع‌رسانی، اقدام مناسب برای دستیابی به میثاق‌ها و مقررات بین‌المللی و ایجاد اتحادیه‌های اطلاع‌رسانی با سایر کشورها، به ویژه کشورهای اسلامی به منظورایجاد توازون در عرصه اطلاع‌رسانی بین‌المللی آمده است.[1] اطلاع‌گیری یکی دیگر از تدابیر در این باره است که مبتنی بر تدارک برنامه‌ای جامع در جهت اخذ اطلاعات و جمع‌آوری اخبار نقض‌کننده و تهدیدات امنیت سایبری باشد. در این پیشگیری، بار اصلی بر دوش دولت است که باید هم در راستای اصلاح ساختار خویش و هم آگاهانیدن کارمندان و شهروندان برنامه و پیشنهاد ارائه نماید (Bahremand & Davoudi,2018:36). در این خصوص به موجب قانون آیین دادرسی کیفری، ارایه‌دهندگان خدمات دسترسی مکلف شده‌اند داده ترافیک را حداقل تا شش ماه پس از ایجاد و اطلاعات کاربران را حداقل تا شش ماه پس از خاتمه اشتراک نگهداری کنند. هم‌چنین به موجب ماده ٦٦٩ این قانون، «هرگاه حفظ داده‌های رایانه‌ای ذخیره‌شده برای تحقیق یا دادرسی لازم باشد، مقام قضائی می‌تواند دستور حفاظت از آن‌ها را برای اشخاصی که به نحوی تحت تصرف یا کنترل دارند صادر کند. در شرایط فوری، نظیر خطر آسیب دیدن و یا تغییر یا از بین رفتن داده‌ها، ضابطان قضائی می‌توانند دستور حفاظت را صادر کنند و مراتب را حداکثر تا بیست و چهار ساعت به اطلاع مقام قضائی برسانند...». در همین خصوص ماده ١٦ کنوانسیون جرایم سایبری مقرر می‌دارد: «هر یک از اعضاء باید به گونه‌ای اقدام به وضع قوانین و سایر تدابیر نمایند که در صورت لزوم جهت حفظ فوری داده‌های رایانه‌ای خاص، نظیر داده ترافیک، که در یک سامانه رایانه‌ای ذخیره شده است، به ویژه در جایی که زمینه‌های این باور وجود دارد که داده‌های رایانه‌ای در برابر از بین رفتن یا تغییریافتن آسیب‌پذیرند، این اختیار را به مقام ذیصلاح خود بدهند که دستوراتی صادر کرده یا اقدامات مشابهی به عمل آورند». این شرایط نگاه و سیاست‌های امنیتی را مبتنی بر ایجاد مقررات با هدف امکان اطلاع‌گیری از اقدامات بازیگران عرصه مبادلات عمومی اطلاعاتی نموده است.

حکمرانی سایبری امنیتی: نگاه کاملاً نوین به پدیده امنیت سایبری و یا بازشناختی حقوقی از این عناصر مستلزم شناخت یکی از مهم‌ترین پارامترها در نظم نوین سایبری جهانی در بعد حکمرانی سایبری و نقش آفرینی قواعد حقوقی بازی در دنیای سایبر بوده و اصولاً وجه حکمرانی خوب در فضای سایبر از پارمترهای مهم در مقابله با نقض امنیت سایبری است. در ماده ٣٤ دستور کار تونس برای جامعه اطلاعاتی مفهوم حاکمیت بر اینترنت، این‌گونه تعریف شده است: «توسعه و کاربرد نقش‌های مربوطه، اصول مشترک، هنجارها، قواعد، رویه‌های تصمیم‌سازی و برنامه‌های است که توسط دولت‌ها، بخش خصوصی و جامعه مدنی به منظور شکل‌دهی به تکامل و استفاده از اینترنت صورت می‌گیرد» (Soltani, 2017:156). واقعیت موجود نقض گسترده امنیت سایبری در ابعاد گوناگون آن است و جامعه جهانی و حتی حکمران این عرصه با این معضل دست به گریبانند. بنابراین

۱- ابلاغیه رهبری به شماره ۱/۱۰۳۳ موضوع سیاست‌های کلی شبکه‌های اطلاع‌رسانی رایانه‌ای. برای ملاحظه محوه پیاده‌سازی این تدابیر در پرتو راهبرد کلان «سالم سازی فضای سایبر»، ر. ک: جلالی فراهانی، امیرحسین و باقری اصل، رضا، تأملی بر فیلترینگ: برنامه اقدام برای سالم‌سازی فضای سایبر، مرکز پژوهش‌های مجلس شورای اسلامی، شماره ۸۹٤۷، اردیبهشت ماه ۱۳۸۷.

توسعه راهبردها و رهنامه‌هایی به منظور مواجه فعال و پیش‌دستانه با این رخدادها با هدف آماده‌سازی زیرساخت‌ها و ایجاد هماهنگی به منظور حفظ امنیت ملی و در صورت نیاز، واکنش در برابر این گونه تهدیدات ضروری است(Katrina, Lewis,2011). از آنجا که ریشه‌های نقض امنیت سایبری در وضعیت سیاسی، اقتصادی، اجتماعی و فرهنگی جوامع نهفته است و بدون توجه به این علل و تلاش برای از بین بردن نابرابری‌ها در سطح ملی و جهانی نباید امیدی به پیروزی در مبارزه با نقض امنیتی داشت، از این رو توجه به معیارهای حکمرانی حائز اهمیت است(Bahremand & Davoudi ,2018:41). توجه به این امر ضروری است که رویکرد ایران در حیطه مدیریت داخلی اینترنت، مبتنی بر سیاستگذاری ملی است. پیرو ابلاغ «سیاست‌های کلی شبکه‌های اطلاع‌رسان‌های رایانه‌ای» از سوی رهبری [1]شورای عالی انقلاب فرهنگی، «مقررات و ضوابط شبکه‌های اطلاع‌رسانی رایانه‌ای» را در سال ۱۳۸۰ تصویب کرد. طبق این قانون به موازات حق دسترسی آزاد به اطلاعات، بر رعایت حقوق داخلی در موضوعات اجتماعی، فرهنگی و فنی کشور تأکید گردیده است. 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 پنج ساله توسعه و قانون تجارت الکترونیک نیز وجود دارد که به‌نوعی رویکردهای حکمرانی در فضای سایبر را دنبال می‌کنند، لیکن نخستین قانون جامع و متمرکز در ایران، قانون جرایم رایانه‌ای، مصوب ۱۳۸۸ و قوانین اصلاحی آن، مندرج در قانون آیین دادرسی کیفری و قانون مجازات اسلامی مصوب ۱۳۹۲ با اصلاحات بعدی است که درصدد اتخاذ رویکردهای حکمرانی مقابله‌ای است. با این‌حال 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)[2] مبیّن پذیرش روش بین‌المللی در این عرصه از سوی ایران است. در حال حاضر حاکمیت[3] غالب نظام جهانی اینترنت در اختیار آمریکا و شرکت‌های فراملی تحت نظر این کشور است و لذا حکمرانی چند ذیربطی رویکردی نسبتاً جدید برای حکمرانی در حوزه عمومی است که طی دو دهه اخیر مورد توجه قرار گرفته است. در سند نهایی اجلاس جهانی جامعه اطلاعاتی در سال ۲۰۰۵ در تونس که به دستور کار تونس شهرت یافت، پیشنهاد شده است که حکمرانی بین‌المللی اینترنت به شکلی چند ذیربطی پی‌گرفته شود(Khoshnevis,2019). بنظر می‌رسد حکمرانی سایبری در اسناد کشوری به نحو مطلوبی مورد شناسائی واقع شده چنانچه در اسناد مربوطه برای رسیدن به ایرانی هوشمند در تراز انقلاب اسلامی در افق ۱٤۰٤ با رویکردهای چون ایجاد شفافیت، مبارزه با فساد، ارتقاء کارآمدی و بسط عدالت ازطریق ارائه خدمات هوشمند، تأمین و تسهیل ارتباطات فراگیر، ارائه سرویس‌های محتوای داخلی، ایجاد و توسعه زیرساخت امن و پایدار در تمامی ارکان دولت و جامعه، تمدن‌سازی در فضای مجازی، ارتقاء جایگاه اقتصاد دیجیتال مواجه می‌شویم. مبتنی بر بیانیه گام دوم انقلاب اسلامی، ۲۰ هدف کلان در حوزه حکمرانی مطلوب امنیت‌محور سایبری احصاء گردیده از جمله؛ پیشتازی نظام حکمرانی فضای مجازی ناظر به خودکفایی جمهوری اسلامی ایران در خدمات پایه کاربردی و حفظ امنیت و سلامت فضای مجازی کشور، تبدیل جمهوری اسلامی ایران به یکی از بازیگران اصلی حوزه امنیت فضای مجازی و ایجاد پیمان‌ها و معاهدات همکاری با کشورهای دوست. در ادامه و در برنامه راهبردی فضای مجازی جمهوری اسلامی ایران و در راستای چشم‌انداز فضای مجازی در افق ۱٤۰۰، بیست هدف کلان تبیین که از جمله مصادیق دست‌یابی به قدرت اول سایبری در منطقه غرب آسیا و کسب مقام نخست خدمات فضای مجازی مبتنی بر پیشرفت پایدار و پیش‌تازی نظام حکمرانی فضای مجازی ناظر به شاخص‌های همسویی، هم‌راستایی و وحدت رویه به منظور تقویت حاکمیت ملی، عدالت، تأمین منافع ملی و اشراف و توانایی اعمال سیاست و صیانت از حقوق ملت؛ خودکفایی جمهوری اسلامی ایران در خدمات پایه کاربردی و حفظ امنیت و سلامت فضای مجازی کشور در بالاترین سطح در بین کشورهای منطقه؛ تبدیل جمهوری اسلامی ایران به یکی از بازیگران اصلی حوزه امنیت فضای قابل ذکرند. در برنامه راهبردی ارائه شده توسط «سازمان ارتباطات

۱- نامه شماره ۱۰۷۲/۱ مورخ ۱۳۸۰/۳/۱۳ دفتر رهبری.

2- Internet Corporation for Assigned and Numbers (ICANN)

آیکان طبق قانون شرکت‌های غیرانتفاعی و منفعت عمومی برای اهداف خیریه و عمومی ایالت کالیفرنیا تشکیل شد و وظیفه مدیریت تارنماهای اینترنتی و شناسه پروتکل‌ها (ISP) را در فضای سایبر بر عهده دارد.

۳- حاکمیت بر اینترنت شامل مدیریت و هماهنگی زیرساخت‌های فنی اینترنت است. مثل نام‌های دامنه، آدرس‌ها، استانداردها پروتکل‌هایی که اینترنت را قادر به انجام وظایفش می‌کند. در تعریف موسعی از حاکمیت بر اینترنت ارائه شده است: «عوامل مختلفی که موضوعات مرتبط با سیاست‌گذاری اینترنت را شکل می‌دهند، مثل مالکیت فکری،حریم خصوصی، آزادی اینترنت، تجارت الکترونیک، امنیت سایبری و....» (Kruger,2016:1) ذکر شده‌اند.

کشورهای مشترک المنافع» برای سال‌های ۲۰۱۲ تا ۲۰۱۶، امنیت و جرایم سایبری جزء۶ محور اصلی توسط این سازمان مورد شناسایی قرار گرفته است. همچنین در اکتبر سال ۲۰۱۳، سازمان مذکور «مدل حکمرانی سایبری کشورهای مشترک المنافع» که به وسیله اعلامیه «آبوجا» که در سال ۲۰۱۴ در لندن برگزار شده بود را اجرایی نمود. در واقع این مدل شامل فهرستی از اصولی می‌باشد که هدف آن‌ها راهنمایی کشورهای عضو در راستای برنامه‌ریزی و اجرای برنامه‌های عملیاتی در توسعه سیاستگذاری، قاعده‌مندسازی، همکاری‌های فرامرزی، ظرفیت‌سازی، اقدامات فنی و سایر فعالیت‌های مربوط به فضای سایبری می‌باشد. نکته قابل ذکر پایانی در باب سیاست جنایی کلان جهانی حکمرانی خوب یا حکمرانی چند ضلعی است که از جمله توسط بانک جهانی مطرح و تأکید آن بر تصمیماتی است که امکان تأثیرگذاری بر عملکرد اقتصادی کشورها را فراهم می‌سازد و سپس بعد سیاسی هم به آن افزود شد که شامل ویژگی‌های مشروعیت دولتی، پاسخگویی دولتی، تحقق حقوق بشر از طریق حاکمیت قانون و شایستگی دولتی است (Dabbagh & Nafari,2009:5).

ارتقاء پاسخ‌گویی و شفافیت: شورایعالی فضای مجازی در اجرای ماده ۱۱ آیین‌نامه داخلی خود، مصوبه ۶۸ مورخ ۱۳۹۹/۱۰/۱۶ با موضوع «الزامات پیشگیری و مقابله با نشر اطلاعات، اخبار و محتوای خبری خلاف واقع در فضای مجازی» را به دستگاه‌های ذیربط ابلاغ نمود که هدف از آن صیانت از سلامت و امنیت روانی جامعه و کاهش آسیب‌های موصوف از طریق تعریف و تعیین اقدامات پیشگیرانه و واکنشی و ارتقاء سطح مسئولیت‌پذیری و پاسخ‌گویی هماهنگ و به‌هنگام برای مقابله با ناهنجاری‌ها و پیامدهای تولید و نشر اطلاعات، اخبار و محتوای خبری خلاف واقع است. در اجلاس هفتادم مجمع عمومی سازمان ملل متحد در ۲۲ جولالی ۲۰۱۵ قطعنامه شماره A/۷۰/۱۷۴ در در بند ح چهارمین گروه کارشناسان دولتی موضوع در مقدمه گزارش خود به این مسئله پرداخته است که «دولت‌ها باید به درخواست‌های کمک متعارف از سوی دولتی دیگر که زیرساخت‌های حیاتی آن مورد تهدیدات مخرب در حوزه فناوری اطلاعات و ارتباطات قرار گرفته شفاف پاسخ دهند و دولت‌ها هم‌چنین باید به درخواست‌های مناسب برای کاهش فعالیت‌های مخرب در حوزه فناوری اطلاعات و ارتباطات با هدف زیرساخت‌های حیاتی دولت دیگری که از سرزمین آن‌ها نشأت گرفته است، با توجه به حق حاکمیت پاسخ‌دهند» در بند «ط» نیز تأکید شده است که دولت‌ها باید گام‌های مسئولانه برای اطمینان از یکپارچگی زنجیره تأمین انجام دهند تا کاربران نهایی بتوانند به امنیت محصولات حوزه فناوری اطلاعات و ارتباطات اطمینان داشته باشند. سند راهبرد امنیت سایبری آلمان بر روی چند محور اساسی تمرکز دارد از جمله موارد مهم در این سند، ایجاد شورای ملی امنیت سایبر، مرکز ملی پاسخ سایبری و مرکز دفاع سایبری و تقویت ساختارها و تعاملات سازمان‌ها با یکدیگر است(Hosseini&Zarif-Manesh,2013:52). شفافیت عملکرد نهادهای تولیدکننده ابزارهای اینترنت اشیا یکی از مبانی حفاظت از داده پیام‌های الکترونیکی برای دولت‌های متبوع آن‌هاست (Singh&Etc,2019,4-5). مطابق با مفاد ماده ۱۲ مقررات عمومی حفاظت از داده پیام‌های الکترونیکی[1] اتحادیه اروپا سال ۲۰۱۸، شرکت‌های بیان‌شده تنها در صورتی قابلیت پردازش داده پیام‌های شخصی افراد را خواهند داشت که برای اهداف مشخصی با جلب رضایت مالک این ابزارها، این پردازش صورت گیرد. از این رو پردازش داده پیام‌های مذکور جز در مواردی که این اهداف از ضرورت کافی برخوردار نباشد می تواند منجر به مسئولیت مدنی شرکت مزبور گردد. ماده ۱۲ مقررات ۲۰۱۸ در هیچ کدام از قوانین مصوب کشور ایران مورد تصریح قرار نگرفته است. از این رو اگر این مقررات به عنوان قانون آمره در کشور ایران تصویب نشده یا مقررات آنها در قوانین مصوب گنجانده نشود، نمی توان این تشریفات را به صرف صدور آیین نامه‌ها یا بخشنامه‌های دولتی برای اشخاص حقیقی یا حقوقی خارج از دولت حاکم دانست و برای آنها ایجاد مسئولیت نمود. از این رو عدم وجود این مقررات به عنوان یکی از خلاءهای قانونی در نظام حقوقی ایران شناخته می‌شود که حل آن نیازمند سیاستگذاری صحیح تقنینی می‌باشند (Sadeqi & Mahdavi,2020:92)

فرهنگ‌سازی: امروزه به دلیل مشکلات و بحران‌های مالی و افزایش هزینه‌های روی‌آوردن به نظام‌های رفاهی در دل نظام عدالت کیفری، تمایل به جرم‌انگاری، سایه خود را بر سر سیاست‌های اجتماعی گسترانیده و در قلب نظام رفاهی جای گرفته است (Malekmohammadi,2017:183). با این حال بسیاری از نقض‌های امنیت در فضای سایبر را می‌توان با فرهنگ‌سازی در بعد داخلی و با تقویت فرهنگ قانون‌مداری، ایجاد اعتماد به ظرفیت‌های اجتماعی و حمایت از ارزش‌ها و پذیرش عمومی برنامه‌های

1- General Data Protection Regulation

پیشگیرانه و در بعد بین‌المللی با تقویت فرهنگ و هنجارهای سایبری جهانی و ایجاد فرهنگ مطلوب و صحیح بین‌المللی خنثی نمود. چنانچه قطعنامه ۵۸/۱۹۹ مجمع عمومی سازمان ملل، امنیت سایبری را در گرو یک فرهنگ جهانی[۱] دانسته است (109 Pakzad, 2008:). ماده ۱۰۹ قانون برنامه ششم توسعه کشور رهبردهایی را بیان و فرهنگ‌سازی، آموزش و افزایش آگاهی و مهارت‌های عمومی در حوزه افتا را لحاظ نموده و این چنین مقرر شده است: «ایجاد نظام جامع و فراگیر در سطح ملی و ساز وکار مناسب برای ایمن‌سازی ساختارهای حیاتی و حساس و مهم در حوزه فناوری اطلاعات و ارتباطات و ارتقاء مداوم امنیت شبکه‌های الکترونیکی و سامانه‌های اطلاعاتی و ارتباطی در کشور به منظور استمرار در خدمات عمومی؛ پایداری زیرساخت‌های ملی؛ صیانت از اسرار کشور؛ حفظ فرهنگ و هویت اسلامی- ایرانی و ارزش‌های اخلاقی؛ حراست از حریم خصوصی و آزادی‌های مشروع و سرمایه‌های مادی و معنوی» و در بند ۸ آن باز به فرهنگ‌سازی، آموزش و افزایش آگاهی و مهارت‌های عمومی در حوزه افتا توجه شده است. در بند ۳۳ از سیاست‌های کلی برنامه ششم توسعه کشور به امنیت فضای سایبری نیز به توسعه محتوی در فضای مجازی بر اساس نقشه مهندسی فرهنگی کشور تا حداقل پنج برابر وضعیت کنونی و بومی‌سازی شبکه‌های اجتماعی اشاره شده است. همچنین بر اساس بند «ب» ماده ۱۰ قانون برنامه پنج ساله پنجم توسعه جمهوری اسلامی ایران دولت موظف است سازوکارهای اجرایی لازم برای ارتقای آگاهی، دانش و مهارت همگانی به منظور سازماندهی فضای رسانه‌ای کشور، مقابله با تهاجم فرهنگی بیگانه و جرایم و ناهنجاری‌های رسانه‌ای را فراهم و اجرایی کند. در پیش‌نویس نقشه مهندسی فرهنگی شرکت خدمات ارتباطی رایتل، اپراتور رایتل به عنوان یکی از فراهم‌کننده خدمات، هیأت متخصصی را برای تیین محتوا و پایش آن تشکیل داده است که از جمله وظایف این هیأت تدوین سازوکار نظارتی بر محتوا، تبلیغات و خدمات تعیین ضوابط فرهنگی انتخاب و همکاری با شرکت‌های همکار در موضوعات محتوا، خدمات و تبلیغات، پایش فرهنگی مطبوعات و....) محتوای چند رسانه‌ای، پایش فرهنگی خدمات ارزش افزوده، پایش فرهنگی تبلیغات تلویزیونی، چاپ، پایش فرهنگی فروشگاه‌های عرضه خدمات رایتل، پایش اخبار مرتبط با تبلیغات، خدمات و محتوا، رصد اخبار مرتبط با تبلیغات، خدمات و محتوا می‌باشد. در این خصوص و در نتیجه نشست‌های عمومی سازمان ملل؛ پنج قطعنامه مهم، به بازتاب نظر خود در باره امنیت سایبری پرداخته است که در سند A/RES/57/239: فرهنگ امنیت سایبری قطعنامه بالا، توسعه و ترویج فرهنگ جهانی امنیت سایبری را مورد تأکید قرار می‌دهد. این قطعنامه در ۲۰۲دسامبر ۲۰۰۲ صادر شده و وابستگی روزافزون دولت‌ها و شرکت‌ها و سایر سازمان‌ها و کاربران شخصی به فناوری اطلاعات را مورد توجه قرار می‌دهد. این قطعنامه همچنین به این نکته توجه می‌کند که افزایش مشارکت کشورها در جوامع اطلاعاتی، نیاز به امنیت سایبری را افزایش می‌دهد(Vamala,2017:36). اتحادیه بین‌المللی مخابرات، اولین نسخه از راهنمای راهبرد امنیت سایبر را در سال ۲۰۱۸ و نسخه اصلاحی این شاخص را برای اندازه‌گیری کمّی سطح پیشرفت امنیت سایبری در کشورها طراحی کرده‌است. هدف نهایی اتحادیه بین‌المللی مخابرات از تهیه این شاخص، تقویت فرهنگ جهانی امنیت سایبری است. این شاخص شامل پنج مؤلفه «قوانین و مقررات[۲]، اقدامات فنی[۳]، ساختارهای اجرایی و سازمانی[۴]، ظرفیت‌سازی[۵]، همکاری ملی و بین‌المللی[۶] »می‌باشد. فرهنگ امنیتی همچنین با هدف راهبرد ششم «دستور کار امنیت سایبری جهانی» همسو می‌باشد که با سازوکار ظرفیت‌سازی برای افزایش آگاهی، انتقال دانش و تقویت امنیت سایبری در دستور کار سیاست ملی، سروکار دارد. مجمع عمومی سازمان ملل متحد همچنین ارتقاء، توسعه و پیاده‌سازی فرهنگ قوی جهانی امنیت سایبری را مورد تشویق قرار داده است(UN2010). به نقل از (Vamala,2017:142).

۱- شاخص جهانی امنیت سایبری۱ یک مرجع ارزیابی امنیت سایبری در سطح جهانی است که توانمندی و تعهد کشورها به موضوع امنیت سایبری را در سطح جهانی مورد ارزیابی قرار می‌دهد. شاخص جهانی امنیت سایبری توسط اتحادیه بین‌المللی مخابرات با هدف اصلی ایجاد و تقویت فرهنگ جهانی امنیت سایبری و ادغام ا ین فرهنگ در فناوری‌های اطلاعاتی و ارتباطاتی توسعه داده شده است چارچوب اتحادیه بین‌المللی مخابرات برای همکاری چند ذینفعی بین‌المللی در زمینه امنیت سایبری با هدف ایجاد هم‌افزایی بین ابتکارها و اقدامات فعلی و آینده می‌باشد (Global Cybersecurity Index۲۰۲۰).

2- Legal Measures
3- Technical Measures
4- Organizational Measures
5- Capacity Building
6- Cooperation

مشارکت عمومی: موضوع مهم دیگر در برنامه راهبردی فضای مجازی جمهوری اسلامی ایران است که در حوزه گوناگون راهبردی مانند فرهنگ و سبک زندگی، منابع انسانی، حاکمیت و مدیریت و امنیت شکل گرفته است و ذیل هر حوزه راهبردهای آن آورده شده است. در حوزه امنیت فضای مجازی راهبردهای چون جلب مشارکت شهروندان، سازمان‌ها، کسب وکارها و تمام بخش‌ها در تامین امنیت فضای مجازی، ذاتی و زمینه‌ای‌شدن امنیت در کلیه مراحل طراحی معماری تا اجرای حوزه‌های مختلف فضای مجازی، امن‌سازی زیرساخت‌های حیاتی کشور در قبال حملات الکترونیکی، تسلط کامل بر دروازه‌های ورودی و خروجی فضای مجازی و ارتقاء توان مقابله با هرگونه حمله، واکنش فعال و پیش‌نگر در مدیریت بحران مدنظر قرار گرفته است. از مصادیق نظارت مشارکتی در فضای سایبر استفاده از پتانسیل فراهم‌کنندگان خدمات در حوزه ارتباطات آنلاین است که بیشترین نقش را این زمینه ایفا می‌کنند. استفاده از پتانسیل این فراهم‌کنندگان خدمات در واقع مشارکت‌دادن بخش خصوصی در امر حاکمیتی نظارت است. این مشارکت با بخش خصوصی در ایران نیز به خوبی اجرا شده است(Nazari,et al,2021:165). اعلامیه گروه ۷ در خصوص «رفتار مسئولانه دولت‌ها در فضای سایبری» در ایتالیا ۲۰۱۷ با اشاره به گسترش مخاطرات ناشی از تشدید منازعات و اقدامات تلافی‌جویانه در فضای سایبری و تهدیدات متوجه زیرساخت‌های حیاتی و مداخله سایبری در فرآیندهای انتخاباتی آمریکا و فرانسه، بر ضرورت افزایش فوری همکاری‌های بین‌المللی برای ارتقای امنیت و ثبات در فضای سایبری و بر اعمال قوانین بین‌المللی بر رفتار دولت‌ها در فضای سایبری تأکید نموده و بیان می‌دارد که افراد می‌بایست از حقوقی که در محیط آفلاین برخوردار هستند، در محیط آنلاین نیز برخوردار باشند. کشور آلمان نیز با توسعه سند ملی راهبردی امنیت سایبر به موضوعات راهبردی از قبیل تضمین امنیت سایبر، اعمال حقوق و حفاظت از زیرساخت‌های اطلاعات حیاتی ملی با مشارکت دولت، صنعت و جامعه بر اساس یک رویکرد جامع و عمدتاً متمرکز بر رویکردها و اقدامات پیشگیرانه، تقویت امنیت سایبر با اعمال قواعد بین‌المللی رفتار، استانداردها و هنجارها با همکاری شرکای بین‌المللی و مقابل با رشد سریع جرائم اینترنتی با همکاری نزدیک بین مقامات اعمال قانون در سراسر جهان و اطمینان از امنیت سایبر پرداخته است (German Government,2011). در سال ۲۰۰۰ کنوانسیون امنیت سایبری و محافظت از اطلاعات شخصی اتحادیه آفریقا با هدف ایجاد هماهنگی در قوانین مرتبط با امنت سایبری و مبارزه با نقض حریم خصوصی ایجاد و مقررات کیفری پیشگیری از نقص امنیت سایبری، امنیت شبکه‌های رایانه‌ای و توسعه جامعه اطلاعاتی آفریقا را لحاظ و دستورالعمل گسترده‌ای ارائه و در سال ۲۰۱۲، قانون سایبری آفریقا را مشتمل بر چهار فصل معاملات الکترونیکی، حفاظت از اطلاعات شخصی، ارتقاء امنیت سایبری و مبارزه با جرایم سایبری و مقررات نهایی بازخوانی و در ماده ۲۸، همکاری بین‌المللی را لازمه تحقق امنیت سایبری دانسته و چهار شاخص هماهنگی، کمک حقوقی متقابل، تبادل اطلاعات و ابزار همکاری را برای آن پیش‌بینی کرد (AFRICAN UNION, 2014).

تعیین ارائه‌دهندگان محتوای اینترنتی: به یقین می‌توان معتقد بود سرویس‌های ارائه محتوا و مدیریت آن‌ها یکی دیگر از سیاست‌های پیشگیری اجتماعی مبتنی بر فرهنگ سایبری به شمار می‌رود که به دنبال ارائه محتواهای مطلوب و غیرمجرمانه است تا شهروندان به واسطه دریافت این محتواها، از جست‌وجوی محتواهای مجرمانه منصرف شده و اشتیاقی برای توجه به آن‌ها نداشته باشند. براین اساس، کنش‌گران دولتی در کنار فیلترینگ[1] محتوای مجرمانه، توجه ویژه‌ای به ارائه محتواهای مناسب برای کاربران در این فضا دارند(Nazari,et al,2021:160). بند هفتم از ماده ٤ از دستورالعمل اجرایی سال ۲۰۱۸ اتحادیه اروپا در تعریف کنترل‌کننده بیان می‌دارد: «شخص حقیقی یا حقوقی، مرجع عمومی، نمایندگی یا هر نهاد دیگری است که به تنهایی یا به طور مشترک با دیگران اهداف و وسایل پردازش داده‌های شخصی را تعیین می‌کند». به عبارت دیگر؛ ابزارهای اینترنت اشیا دارای سازندگانی می‌باشند که قابلیت دسترسی به اطلاعات این ابزارها را برخوردار بوده و از امکان کنترل آن‌ها نیز بهره‌مند هستند. این اشخاص حقیقی یا حقوقی که کنترل‌کننده نامیده می‌شوند، مطابق با نقش خود در عملکرد یک ابزار، می‌توانند شناسایی شوند(Sadeqi & Mahdavi,2020:86). با این‌حال قانون‌گذار ایران در هیچ یک از قوانین جرایم رایانه‌ای مصوب

۱- مسئول فیلترینگ وبگاه‌های اینترنتی در ایران، کارگروه تعیین مصادیق محتوای مجرمانه است که طبق ماده 22 قانون جرائم رایانه‌ای از 13 عضو حقوقی و حقیقی تشکیل شده است و حوزه عملکرد این کارگروه به دلیل فعالیت‌های غیرمجاز در حوزه‌های اخلاقی، سیاسی، اعتقادی و مانند آن، به دو روش استفاده از فهرست سیاه و فیلترینگ بر اساس کلیدواژه‌ها بوده که وبگاه‌های مدنظر را غیر قابل دسترس می‌کند(Saad,2014) به نقل از:
Bidarvand & Pourghahreman & beigi,2020:43.

۱۳۸۸ و قانون آیین دادرسی کیفری مصوب ۱۳۹۲ با اصلاحات و الحاقات بعدی، تعریفی از ارائه‌دهندگان خدمات اینترنتی ارائه نکرده است که البته بهتر آن بود تدوین‌کنندگان قانون با ارائه تعریفی در این مورد مطابق دیدگاه خود اقدام می‌کردند. لکن در مورد ارائه‌دهندگان خدمات اینترنتی در متون و منابع مختلف، تعاریف متعددی بیان شده است. بند (پ) ماده (۱) کنوانسیون جرایم سایبری ارائه‌دهندگان خدمات را به این شرح تعریف می‌نماید که «ارائه‌دهندگان خدمات: ۱.هر مجموعه خصوصی یا عمومی است که برای کاربران خود، امکان برقراری ارتباط به وسیله سیستم‌های رایانه‌ای را فراهم می‌آورد؛ ۲. هر مجموعه دیگری است که داده رایانه‌ای را به جای ارائه‌دهندگان خدمات ارتباطی یا کاربران این‌گونه خدمات، پردازش یا ذخیره می کند»(Jalali Farahani,2010:20).

نتیجه‌گیری

آنچه در دوران کنونی به عنوان مهم‌ترین موضوع و چالش غیرقابل انکار از آن می‌توان یاد کرد ابهام و چندگانگی در تعریف روشن از فضای سایبر و امنیت سایبر و شناسایی چالش‌های گوناگون موجود در این عرصه است. هنگامی‌که سخن از سیاست جنایی است، می‌بایست در یابیم که ما در کجای جهان سایبریم و آیا آنچه تعریف ما از سایبر است و آنچه در مفاهیم این پدیده در نظام قانونی و حقوقی جهان سایبر وجود دارد به همان صورت در نظام حقوقی و اجتماعی ما قابل تسری است. در بعد داخلی و بین الملل تلاقی این مفاهیم و تطبیق نظام واژگان موجود خود چالش مهمی است که به سبب تنوع قوانین بعضاً ضعیف موجود در داخل، گریبان‌گیر نظام حقوقی ماست.با مداقه در راهبردهای پدافند سایبری کشور، رویکردهای متنوعی در رهیافت‌های مدنظر کارگزاران سایبری کشور با ابتناء بر آموزه‌های سیاستگذاری جنایی پیشگیرانه به چشم می‌خورد از جمله: توسعه آمادگی دفاعی، توسعه زیست‌بوم سایبری بومی، امن و پایدار، توسعه مفاهیم دفاع سایبری، توسعه نظام حقوقی و تعاملات بین‌المللی در حوزه دفاع سایبری، تدوین قوانین و مقررات، دستورالعمل‌ها، درک هوشمندانه و پیش‌دستانه تهدیدات، عدم بکارگیری غیرهوشمندانه سامانه‌های خارجی در مراکز دارای اهمیت بالا. تدقیق در مجموعه قوانین و مقررات مربوطه، حاکیت ازاین دارد که سیاستگذاری جنایی ایران در قبال نقض امنیت سایبری، سیاست‌گذاری غیرافتراقی و مبهم و فاقد مبنای منسجم حقوقی است. سیاستگذاری مناسب در حوزه حکمرانی دیجیتال می‌تواند باعث افزایش اعتماد عمومی، افزایش سطح کیفیت خدمات دولت، افزایش رفاه و آسایش عمومی در جهت نیل به آرمان‌های بیانیه گام دوم انقلاب اسلامی گردد. تحقق حکمرانی منوط به هم‌گرایی نهادهای سیاستگذار و وزارت ارتباطات و فناوری اطلاعات به عنوان مجری و تنظیم‌گر و ارائه واقع بینانه نیازمندی‌ها و مطالبات حاکمیت در جهت تحقق مدل حکمرانی مطلوب می‌باشد. از سویی دیگر همگرایی ایران با کشورهای منطقه، کشورهای اسلامی، جنبش عدم تعهد و قدرت‌های همسو می‌تواند باعث برون رفت کشور از مواجهه منفرد با سیاستگذاری‌های یک‌جانبه‌گرایانه، ایجاد ظرفیت‌های اقتصاد دیجیتال در منطقه، پیگیری تصویب معاهدات و قوانین پیشنهادی توسط ایران در مجامع و نهادهای قانون‌گذار بین‌المللی و ...گردد. علاوه بر این، امکان پیگیری حقوقی حملات سایبری به زیرساخت‌های کشور(نظیر استاکسنت و سامانه سوخت)، نقض حریم خصوصی شهروندان ایرانی، مسدودسازی صفحات کاربران ایرانی توسط سکو(پلتفرم)های خارجی و تحریم زیرساخت‌ها و ابزارهای توسعه فناوری اطلاعات، از طریق پویایی بیشتر حوزه روابط بین‌الملل وزارت ارتباطات مقدور خواهد بود.

References

1- Aalipour, Hassan, (2013), cyber security crimes, Master's specific partial rights booklet (study of computer crimes), Isfahan University (in Persian)

2- African Union. 2014. African Union Convention on Cyber Security and Personal data Protection. African Union

3- Ahmadian, Qidrat and Bloki, saleh and Searmifar, Maryam (2019). "New Strategic Concept of NATO 2010 and its Security Implication in NATO-Russia Relations", Central Asia and Caucasus Quarterly, No.8, pp.1-30 (in Persian)

4- Alaei, Hossien (۲۰۱۲), Sustainable security in the twenty-year vision document of the Islamic Republic of Iran, Afaq Security Quarterly, number15, page 119-148 (in Persian)

5- Approvals of the High Security Commission of the National Center for Cyberspace in the policy document and requirements for the development of cyberspace security in the country in (2017)

6- Ashtarian, Kyomarth (2016), Public policy making in Iran, second edition, Tehran, Mizan publication n(in Persian)

7- Bahremand, Hamid & Davoudi, Zulfaqar (2018), Social prevention of cyber security crimes, Studies in criminal law and criminology, number 1, page 27-46 (in Persian)

8- Bidarvand, Mokhtar & Pourghahremani, Babak & beigi, Jamal (2019), Instagram filtering from the necessity of national security to the violation of freedom of expression as a human right from the perspective of students, The crime prevention approach quarterly, volume3, number 3, page 41-65 (in Persian)
9- Brunot, R. (2018). United Nations Security Council Background Guide, at:
10- Christopher C. Joyner &Catherine Lotrionte, "information warfare as international coercion: Elements of a legal framework?" European Journal of international law, Vol.12 2001: 863-864
11- Commonwealth of Australia. (2009). National Cyber Security Strategy Australian Government.
12- Dabbagh, soroush & Nafari, Neda (2009), Explaining the concept of good in good governance, Public Administration Journal, volume1, number 3 (in Persian)
13- DHS. (2011). Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise
14- German Government. (2011). National cyber security strategy, Cyber Securit Strategy for Germany Federal Ministry of interior.
15- Ghannad, Fateme, Aligholi, Amireh (2019), Protection of privacy on the web in the light of the European law on the protection of personal data and Iran's legal system, International Web Research Conference, page 1-9 (in Persian)
16- Grant, H. (2015). Social crime prevention in the developing world: exploring the role of police in crime prevention. Switzerland: Springer.
17- Hasani, hasan (2018), Data Localization, Research Institute of the National Center of Virtual Space - Department of Advanced Cyberspace Sciences and Technologies, number 7 (in Persian)
18- Hosseini, Parviz and Zarif-Manesh, Hossein (2013), comparative study of the structure of cyber defense of countries, Security Research Quarterly of Imam Hossein University, second year, number 5, pp. 41-68 (in Persian)
19- Hossieni, Parviz (2016), Presenting a strategic model in the field of political security through compiling the experiences of the holy system of J.A. Iran based on the discourse of Velayat Faqih and the Constitution, Supreme National Defense University, Faculty of National Security, Tehran (in Persian)
20- http://www.ccwa.org/wp-content/uploads/2018/09/UNSC-Final.pdf:1-11
21- ITU. "Global Cybersecurity Index." https://www.itu.int/en/ITU-D/Cybersecurity /Pages/ global-cybersecurityindex. aspx (accessed .08 /05/2020)
22- Jahanshiri, Javad, Taghipour, Reza, Pourmanafi, Abolfazl (2015), Translation of research entitled: International comparison of cyber crimes, International Police Studies Quarterly, number21, page 147-185 (in Persian)
23- Jalali Farahani, amirhossien (2010), Cybercrime Convention and its Additional Protocol, Khorsandi publication, Tehran (in Persian)
24- James A. Lewis Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization. Center forStrategic and International Studies
25- Jatinder Singh, Christopher Millard, Chris Reed, Jennifer Cobbe, Jon Crowcroft. (2019), Accountability in the Internet of Things (IoT): Systems, law & ways forward, Social Science Research Network.
26- Javan jafari, abdolreza (2010), Cyber crimes and the differential approach of criminal law (looking at the Islamic Penal Code section of computer crimes, journal of knowledge and development, 17th year, number34, page 177-201 (in Persian)
27- Javan-Jaafari, Abdolreza and Sodomandrad, Amir (2014), Preventing the situation of violation of trade secrets in the cyberspace, two-quarter volume of Economic Law Encyclopedia (Former Knowledge and Development), New Volume, Year 21, Number 6, pp. 31-50 (in Persian)
28- Jazayeri, Seyyed Abbas, Nematollahi, Maesam, Amirian Farsani, Amin (2018), Prevention of cybercrimes and its governing restrictions, Ghanoonyar publication, volume3, number 11, page 9-24 (in Persian)
29- Katanchi, Elnaz, Pourghahremani, Babak (2021), Cyber security challenges in "ASEAN" countries, international studies publication, year 18, number 1, page 69 (in Persian)
30- Katanchi, Elnaz, Zakeri, Reza (2018), Methods of legal confrontation with cyber attacks in international law, Bushehr Police Knowledge Quarterly, 11th year, number41, page 80-106 (in Persian)
31- Khoshnevis, Yaser (2019), Multi-stakeholder Governan of Cyber Space, cyberspace research instirute, number 3, Tehran (in Persian)
32- Kriang, Sak, Kiti, Chaisari, translator: Translator: Sadeghi, Hossein et al (2021), General International Law of Cyberspace, Hoghoghyar publication, Tehran (in Persian)
33- Lennard G. Kruger Internet Governance and the Domain Name System: Issuse for Congress November 18, 2016. P.1
34- Mahmoudzade, Ebrahim, Esmaeili, Keyvan (2017), The strategic model of security protection of the cyberspace of the armed forces, nationalsecurity publication,8th year, number 30, page 203-237 (in Persian)
35- Malekmohammadi, Hamidreza (2016), Investigating the effects of social policy on the phenomenon of crime, journal of public policy, volume3, number 3, page 179-186(in Persian)
36- Malekomohammadi, Hamidreza (2017), public policy, Mizan publication, Tehran (in Persian)
37- Manuel Valls. (2015). French National Digital Security Strategy. French Government
38- Monfared, Mahboube, Jalalifarahani, Amirhossien (2012), Codes of conduct and crime prevention, criminal law research journal, year3, number2, page 105-134 (in Persian)
39- Najafi Abrandabadi, Ali-Hossein (2012), Criminology (Prevention), produced by Mohammad Ali Babaei, in the collection of essays, by Shahram Ebrahimi, 6th edition (in Persian)
40- Najafi Abrandabadi, Ali-Hossein (2016), Criminal policy, entry in: Encyclopaedia of economic criminal sciences, by Amirhassan Niazpour, Tehran, Mizan publication, first edition (in Persian)
41- Nazari, Seyedghani and Jafarzadeh, Siamak and Nikkhah Sarnaghi, Reza (2021), The Role of Participatory Criminal Policy in the Prevention of Cybercrimes in Iran, Political Studies of the Islamic World, Islamic World Studies Association, 11th year, 4th issue, page 151-174 (in Persian)
42- Pakzad, Betol (2008), cyber terrorism, doctoral dissertation in criminal law and criminology, Shahid Beheshti University, Tehran (in Persian)
43- Pourghahremani, Babak (2017), Iran's criminal policy regarding computer crimes (Comparative study with international documents), Shahr Danesh Legal Research Institute (in Persian)
44- Pourghahremani, Babak and Azimi, Fahima, (2018), The role of cyberspace in the development of tourism security, Proceedings of the Second National Cyber Defense Conference, East Adarbaijan, Islamic Azad University, Maragheh Branch, pp. 423-408 (in Persian)
45- Saad, Ali (2014), An income on filtering policies of internet sites, The journal of modern media studies, volume1, number 2, page 143-159 (in Persian)
46- Sadeqi, Hossien & Mahdavi, Naser (2020), Providing the legal framework of accountability in the operation of Internet of Things tools in the context of electronic government; Explaining the effective policy model, journal of public policy, volume 6, number 3, page 103 (in Persian)

47- Shamlou, Baqer (2019), Rereading preventive crime policy in light of the Covid-19 pandemic and chaos theory, Journal of legal research, special letter on law and corona, page 111-142 (in Persian)
48- Shamlou, Baqir and Kazhni-Joibari, Mehdi, (2018), obstacles to the effectiveness of strategies to prevent crimes against moral security in cyberspace, Rihafat Prevention Quarterly, second period, first issue, pp. 13-35 (in Persian)
49- Shiri, Abbas (2017), Criminal policy making about the rights of victims, journal of public policy, volume 4, number1, page 161-175 (in Persian)
50- Soltani, Nasrollah (2017), Towards a Cyber Convention: Streamology of Norms and Monitoring of Trends, volume1, Sepand Qalam publication (in Persian)
51- Soltani, Nasrollah (2021), Cyber and the United Nations, cyber space research institute publication, Tehran (in Persian)
52- Vamala, Frederik (2017), International Telecommunication Union's Guide Document in the Field of National Cyber Security Strategy, translated by: Morteza Vahedi and Ali Asghar Haghiri, Defense Industries Educational and Research Institute Publications, Tehran (in Persian)
53- Watani, Amir and Asadi, Hamid (2016), Criminal policy of the Islamic Republic of Iran in cyber crimes with an emphasis on the special features of these crimes, Islamic Law Research Journal, 17th year, number 1, page 99-126 (in Persian)
54- Zafari, Ayoub and Forughinia, Saeed and Bavand, Musa, 2019, the effect of cyber space on the national interests of the Islamic Republic of Iran from the point of view of soft war, Bushehr Police Science Quarterly, year 11, number 41, pp. 80-106 (in Persian)