

<http://doi.org/10.22133/MTLJ.2022.363418.1125>

## Legal-Criminological Pathology of Cyberspace Refinement in Iran

Mohammad Ali Haji Deh Abadi<sup>1</sup>, Ehsan Salimi Ghleh<sup>2\*</sup>, Parviz Dehghani<sup>3</sup>

<sup>1</sup> Educational Department of Criminal Law and Criminology, Faculty of Law, Qom University, Qom, Iran

<sup>2</sup> Assistant Professor. Department of Law, Faculty of Humanities, Maragheh University, Maragheh, Iran

<sup>3</sup> Assistant Professor. Department of Law, Faculty of Humanities, Maragheh University, Maragheh, Iran

### Article Info

### Abstract

#### Original Article

#### Received:

24-09-2022

#### Accepted:

11-11-2022

#### Keywords:

Filtering

Fair Prevention

Theoretical Prevention

Crime Generalization

Cultural Participation

Participatory Prevention

The most common strategy to prevent cybercrime in Iran is to refine content. However, filtering is not consistent with criminological knowledge approaches and contradicts the natural rights of citizens, including the right to liberty, equality and the right to security. The findings of this research show that the high use of filtering results in "civil disobedience," "society laziness in protecting morality," "generalization of crime," and "juvenile delinquency and victimization". The findings of this research show that the high use of filtering results in "civil disobedience," "society laziness in protecting morality," "generalization of crime," and "juvenile delinquency and victimization". There are already some levels of these unfavorable outcomes in Iran's cyberspace. The conclusion and theory of this article is that sustainable prevention of crime in cyberspace is realized when crime prevention is planned in a "right-wing paradigm" through "community measures" and with respect for individual rights and freedoms. Therefore, it is suggested that by moderating the policy of filtering in the current way, a participatory prevention pattern is implemented so that citizens of cyberspace follow the issue of prevention as a right (the right to cultural participation).

#### \*Corresponding author

e-mail: [e.salimi@maragheh.ac.ir](mailto:e.salimi@maragheh.ac.ir)

#### How to Cite:

Haji Deh Abadi, M. A., Salimi Ghleh, E., & Dehghani, P. (2022). Legal-Criminological Pathology of Cyberspace Refinement in Iran. *Modern Technologies Law*, 3(6), 77-94.

Published by University of Science and Culture <https://www.usc.ac.ir>

Online ISSN: 2783-3836



## پالایش محتوا در سنجۀ حق‌های بنیادین و رهیافت‌های جرم‌شناختی؛ نقد وضع موجود و درآمدی بر وضعیت مطلوب

محمدعلی حاجی ده‌آبادی<sup>۱</sup>، احسان سلیمی قلعه<sup>۲\*</sup>، پرویز دهقانی

<sup>۱</sup> دانشیار گروه آموزشی حقوق جزا و جرم‌شناسی، دانشکده حقوق دانشگاه قم، قم، ایران

<sup>۲</sup> استادیار گروه حقوق دانشکده علوم انسانی، دانشگاه مراغه، مراغه، ایران

<sup>۳</sup> استادیار گروه حقوق دانشکده علوم انسانی، دانشگاه مراغه، مراغه، ایران

اطلاعات مقاله	چکیده
<b>مقاله پژوهشی</b>	پالایش محتوا یا فیلترینگ رایج‌ترین راهبرد پیشگیری از جرم در فضای مجازی ایران شناخته می‌شود. کارآمدی این راهبرد پیشگیرانه، همچون دیگر راهبردهای پیشگیری از جرم، در گرو عادلانه و علمی بودن آن است. در این نوشتار، کمیت و کیفیت پالایش محتوا در پرتو حق‌های بنیادین و رهیافت‌های دانش جرم‌شناختی بررسی شده است. بنابر یافته‌های این پژوهش، پالایش محتوا به شیوۀ جاری «نافرمانی مدنی» و «عمومی‌شدن جرم» در فضای سایبر را در پی داشته است. در این مقاله پیشنهاد می‌شود که در راستای دستیابی به پیشگیری عادلانه و نظریه‌مند در فضای سایبر، با تعدیل سیاست فیلترینگ به شیوۀ جاری، «الگوی پیشگیری مشارکتی حق‌بنیاد» در دستور کار قرار گیرد تا شهروندان فضای مجازی رأساً موضوع پیشگیری را به‌مثابه یک حق (حق مشارکت فرهنگی) دنبال کنند؛ چه آن‌که اگر پیشگیری از جرم در «الگوی حق‌مدار» و از گذر «تدابیر جامعوی» و به‌صورت ریزومی طرح‌ریزی شود، کارآمدی بیشتری خواهد داشت.
<b>تاریخ دریافت:</b> ۱۴۰۱/۷/۲	
<b>تاریخ پذیرش:</b> ۱۴۰۱/۸/۲۰	
<b>واژگان کلیدی:</b> پالایش محتوا پیشگیری عادلانه پیشگیری نظریه‌مند عمومی‌شدن جرم مشارکت فرهنگی پیشگیری مشارکتی *نویسنده مسئول	
رایانامه: <a href="mailto:e.salimi@maragheh.ac.ir">e.salimi@maragheh.ac.ir</a>	

نحوه استناددهی:

حاجی ده‌آبادی، محمدعلی، سلیمی قلعه، احسان و دهقانی، پرویز (۱۴۰۱). پالایش محتوا در سنجۀ حق‌های بنیادین و رهیافت‌های جرم‌شناختی؛ نقد وضع موجود و درآمدی بر وضعیت مطلوب. حقوق فناوری‌های نوین، ۳(۶)، ۷۷-۹۵.

ناشر: دانشگاه علم و فرهنگ <https://www.usc.ac.ir>

شاپای الکترونیکی: ۲۷۸۳-۳۸۳۶

برحسب اعلام مؤسسه «ترویج اینترنت آزاد»<sup>۱</sup> که هدفش نظارت و گزارش فیلترینگ اینترنت در کشورها است، تقریباً در همه کشورهای جهان از پالایش محتوا یا فیلترینگ<sup>۲</sup> برای کنترل فضاهای سایبر بهره‌برداری می‌شود. با این حال، کمیت و کیفیت اجرای برنامه‌های پالایش محتوا در کشورها متفاوت است. در حالی که در کشورهای اروپایی و امریکا کاربست فیلترینگ به صورت حداقلی و با ملاحظات حقوق بشری و دانش جرم‌شناختی و تحلیل اقتصادی صورت می‌گیرد، در اغلب کشورهای دیگر، بدون بررسی تبعات فیلترینگ، استفاده گسترده‌ای از آن می‌شود (سعد، ۱۳۹۴، ص ۱۹۲-۱۹۳). در ایران، پالایش محتوا در زمره معدود برنامه‌های پیشگیری از جرایم سایبری است که مقنن درصدد برآمده است تا شیوه و کیفیت اجرای آن را مشخص سازد. اعمال فیلترینگ یا پالایش محتوا در ایران معمولاً به وسیله ارائه‌دهندگان خدمات دسترسی و میزبانی در اینترنت انجام می‌شود؛ ولی تعیین سطح و مصادیق و سیاست‌های فیلترینگ با کمیته تعیین مصادیق محتوای مجرمانه است. مستند قانونی پالایش فضای مجازی در ایران مواد ۷۴۹ و ۷۵۰ و ۷۵۱ از قانون مجازات اسلامی بخش جرایم رایانه‌ای است. مطابق با ماده ۷۵۰ از قانون مذکور، کارگروه تعیین محتوای مصادیق مجرمانه، که دارای دوازده عضو حقیقی و حقوقی است و با حضور دست‌کم هفت عضو رسمیت می‌یابد، به ریاست دادستان کل کشور تشکیل جلسه می‌دهد. این کارگروه دو دسته از محتواهای ناشی از جرایم رایانه‌ای و محتواهایی که برای جرایم رایانه‌ای به کار می‌روند را شناسایی می‌کند. ماده ۷۴۹ ارائه‌دهندگان خدمات دسترسی و ماده ۷۵۱ ارائه‌دهندگان خدمات میزبانی را متصدیان اجرایی اعمال فیلترینگ معرفی می‌کند که موظف‌اند فهرست تهیه‌شده توسط کارگروه تعیین مصادیق محتوای مجرمانه را پالایش کنند. به این ترتیب، قانونگذار درصدد است که اولاً با سلب دسترسی و ثانیاً با سلب میزبانی پالایش فضای مجازی را به طور کامل محقق سازد. مطابق با تبصره ۲ از ماده ۷۵۰، شکایت و اعتراض درباره مصادیق پالایش‌شده توسط کارگروه مذکور رسیدگی می‌شود. همچنین، مطابق با تبصره ۲ از ماده ۷۴۹، برخی پالایش‌های موردی که در راستای حمایت از شاکی خصوصی صورت می‌گیرد به دستور مقام قضایی رسیدگی کننده به پرونده و پس از احراز مجرمیت یا حداقل محکومیت (اعم از حقوقی یا جزایی) صورت می‌گیرد.

درخصوص شیوه‌های پالایش محتوا در فضای مجازی، به طور کلی در ایران چند شیوه خاص به کار گرفته شده است. در روش اول، فیلترینگ از طریق آدرس آی پی (IP) انجام می‌شود. در این روش، آدرس آی پی چهاربخشی مربوط به سروری که سایت ممنوعه در آن قرار دارد فیلتر می‌شود. اشکال اصلی این روش آن است که بیشتر سایت‌های اینترنتی از سرویس میزبانی اشتراکی استفاده می‌کنند. در این حالت، اگر هزار سایت روی یک سرور قرار داشته باشد و فقط یک سایت جزو سایت‌های ممنوعه باشد، با فیلتر شدن آی پی دسترسی به هر هزار سایت غیرممکن خواهد شد. این روش در سال‌های اول فیلترینگ در ایران انجام می‌شد و بعضاً موجب فیلتر شدن صفحه‌های دولتی نیز شده است. روش دوم، فیلترینگ از طریق فهرست سیاه است. فیلترینگ مرکزی‌ای که هم‌اکنون در ایران استفاده می‌شود از نوع فیلترینگ سیاه است. در فیلترینگ بر اساس فهرست سیاه، فهرستی شامل نشانی وبگاه‌هایی که دسترسی به آن‌ها مجاز نیست وجود دارد. در روش سوم، که فیلترینگ از طریق کلیدواژه‌ها است، فهرستی از کلمات کلیدی ممنوعه تهیه می‌شود و شناسایی کلیدواژه‌های مجرمانه به وسیله نرم‌افزارهای فیلترینگ انجام می‌شود. نرم‌افزار فیلترینگ بر این اساس عمل می‌کند که اگر واژه ممنوعه در آدرس لینک صفحه درخواستی کاربر باشد یا توسط کاربر در موتورهای جست‌وجو وارد شود با پیغام خطا مواجه می‌شود.<sup>۳</sup>

۱. open net initiative: این مؤسسه از شماری امکانات فنی و همچنین شبکه‌ای جهانی از محققان برای تشخیص گستره و نوع فیلترینگ‌های دولتی اینترنت بهره می‌برد. برای اطلاعات بیشتر درباره این مؤسسه ر.ک: <http://opennet.net/about-oni>

۲. فیلتر (الرقابه/ filter): مفهوم لغوی filtering، غربال کردن و تصفیه نمودن است. در ادبیات سایبری، مفهوم اصطلاحی آن به معنای مسدودسازی و پالایش برخی محتواها در فضای سایبر است. فرهنگستان زبان و ادب پارسی پالایه‌سازی و قانون جرایم رایانه‌ای پالایش محتوا را به فارسی برگزیده‌اند.

۳. برای مطالعه بیشتر درخصوص موضوع فیلترینگ رجوع کنید به: قیاسی، رضا و شاه‌محمدی، غلامرضا (۱۳۹۶). جرایم نو ظهور سایبری و روش‌های پیشگیری از آن. تهران: انتشارات دانشگاه علوم انتظامی امین، ۱۹۵-۲۰۱.

تعیین عادلانه بودن پیشگیری از جرم اقتضا می‌کند که هر برنامه پیشگیرانه با سنجۀ حق‌های بنیادین و رهیافت‌های دانش جرم‌شناسی ارزیابی شود؛ چه آن‌که رعایت حق‌های بنیادین مانع از آن است که افراد جامعه، در نتیجۀ برنامه‌های پیشگیری از جرم، از حقوق اساسی خود محروم شوند و تعیین پشتوانۀ علمی یا نظریه‌مند بودن هر برنامه پیشگیرانه نیازمند ارزیابی آن با آموزه‌های دانش جرم‌شناسی است؛ زیرا دانش جرم‌شناسی، به‌منزله دانشی که از پیشگیری از جرم تا علت‌شناسی بزهکاری گسترده است، در هر دو قسمت نظری و کاربردی خود، رهیافت‌های ارزشمندی دارد که کاربست آن‌ها در درجه اول مانع از جرم‌زایی برنامه‌های پیشگیری می‌شود و در درجه بعدی اثربخشی و موفقیت برنامه‌های پیشگیری را تضمین می‌کند.

پژوهشگر در این نوشتار به ارزیابی پالایش محتوا در فضای سایبر در پرتو حق‌های بنیادین و دانش جرم‌شناسی پرداخته است. به این ترتیب، درصد برآمده است که به پاسخ چهار پرسش پیش‌رو دست یابد: اول، پالایش محتوا یا فیلترینگ در ایران چقدر مطابق با حقوق بنیادین یا حق‌های طبیعی است؟ دوم، دانش جرم‌شناسی فیلترینگ به شیوۀ رایج را که سیاست پیشگیری از جرم است چقدر تأیید می‌کند؟ سوم، کارآمدی پالایش محتوا در ایران چقدر است؟ چهارم، چه راهبرد جایگزینی برای پیشگیری از جرم در فضای سایبر متصور است؟

## ۱. پالایش محتوا در سنجۀ حق‌های بنیادین

«پیشگیری غیرکیفری به‌منظور عادلانه‌شدن مستلزم رعایت همان اصول و حقوق و آزادی‌های فردی است که باید به هنگام پیشگیری کیفری رعایت شود» (نجفی ابرندآبادی، ۱۳۹۰، ص ۵۸۴). بر این مبنا، یکی از معیارها برای سنجش عادلانه بودن پیشگیری از جرم انطباق آن با حقوق بنیادین است. حق‌های بنیادین یا حق‌های طبیعی حقوقی مسلم‌اند که هیچ قاعده‌ای نمی‌تواند آن‌ها را از انسان جدا کند؛ حق‌هایی برتر و والاتر از اراده قانونگذار که غیرقابل نفی و انکار است و از ذات انسانی جدایی‌ناپذیر است، تا آن حد که هیچ‌کس نمی‌تواند از آن‌ها صرف‌نظر کند یا آن‌ها را به دیگری انتقال دهد؛ دسته‌ای از حق‌های ازلی، ابدی و تغییرناپذیر که مشمول مرور زمان نمی‌شود و عموم افراد بشر از هر نژاد و جنس را دربر می‌گیرد. «این حقوق طبق قانون و ناموس طبیعت مقرر شده‌اند و هیچ قاعده وضعی و قراردادی نمی‌تواند آن‌ها را از انسان سلب کند» (قربان‌نیا، ۱۳۹۲، ص ۴۴). به‌طور مشخص، این حق‌ها را می‌شود شامل حق بر آزادی و حق بر امنیت دانست.

### ۱-۱. نقد پالایش محتوا در پرتو حق بر آزادی

سیاست‌های پیشگیری، برخلاف سیاست‌های کیفری که فقط علیه بزهکاران به‌کار گرفته می‌شود، تمامی افراد جامعه را دربر می‌گیرد؛ زیرا شناسایی مجرمان بالقوه و آینده ممکن نیست. از این‌رو «اقدامات پیشگیرانه باید به نحوی اجرا شود که افراد جامعه از حقوق اساسیشان محروم نشوند» (نجفی ابرندآبادی، ۱۳۹۰، ص ۵۵۹) و افراد متعارف جامعه که پیشگیری از جرم برای تأمین امنیت و منافع آن‌ها صورت گرفته است تا آنجا که ممکن است در نقش قربانی اقدامات پیشگیرانه ظاهر نشوند. در واقع «تأمین امنیت نباید جز بر مبنای آزادی، برابری، عدالت و رعایت حقوق بنیادین انسان در مراحل مختلف و پیشگیری از جرم صورت گیرد» (نجفی ابرندآبادی و رضوانی، ۱۳۹۴، ص ۳۸). پیش از هر سخن، باید مشخص شود که مبنا و مستند حق بر دسترسی به فضای مجازی و اینترنت چیست؟

«از منظر فلسفۀ حق، هر ادعایی را نمی‌شود «حق» دانست، چه، حق تکلیف است و تکلیف را نمی‌شود بی‌علت بر دیگران تحمیل کرد. از این‌رو برای این‌که هر ادعایی حق شناخته شود توجیحات قوی لازم است» (Wenar, 2005). شناسایی حق بر فناوری‌های بشری مانند فناوری اطلاعات و ارتباطات، به‌علت نوپدید و بشری بودن آن، موضوعی چالشی و بحث‌برانگیز است، چه آن‌که از یک سو، مطابق با برخی دیدگاه‌ها، حقوق انسان منحصر به موارد خدادادی و طبیعی است<sup>۱</sup> و از سوی دیگر شناسایی نشدن حقی مشابه برای دسترسی به فناوری‌های نوین دیگر مانند فناوری نانو یا فناوری هسته‌ای و همین‌طور نوپدید بودن فناوری اطلاعات و ارتباطات و احتمال زوال آن با ظهور فناوری‌های برتر دیگر

۱. در همین راستا، برخی اندیشمندان اسلامی نیز منشأ ایجاد حق و تکلیف را منحصر به اراده پروردگار تعالی می‌دانند. (خلیلی و جوادی آملی، ۱۳۸۴)

شناسایی حق برای دسترسی به این فناوری را با تردید مواجه ساخته است.<sup>۱</sup> با این همه، باید اذعان داشت که حتی اگر حق بر دسترسی به فضای مجازی قابلیت شناخته‌شدن به‌عنوان یک حق مستقل را نداشته باشد، شناسایی آن در سایه «حق آزادی» و به‌منزله شقی از شقوق آن دشوار نیست. توضیح آن‌که، همان‌گونه که امروز در اعلامیه جهانی حقوق بشر و میثاق بین‌المللی مدنی و سیاسی و قوانین اساسی بسیاری از کشورها، از جمله ایران، در پرتو حق آزادی، آزادی انتشار اطلاعات و رسانه پذیرفته شده است، می‌توان آزادی دسترسی به فضای مجازی را نیز پذیرفت. ماده ۲۱، ۳۲، ۳، ۴۳، ۱۹، ۲۷ و... از اعلامیه جهانی حقوق بشر و ماده ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی به‌صراحت به حق آزادی پرداخته است. برای نمونه، ماده ۱۹ اعلامیه جهانی حقوق بشر در این زمینه مقرر می‌دارد:

«هر انسانی محق به آزادی عقیده و بیان است؛ و این حق شامل آزادی داشتن باور و عقیده‌ای بدون [نگرانی] از مداخله [و مزاحمت] و حق جست‌وجو، دریافت و انتشار اطلاعات و افکار از طریق هر رسانه‌ای بدون ملاحظات مرزی است.»

مستند حق آزادی در فضای سایبر جدای از مستند این حق در فضای واقعی نیست. با این حال، فضای سایبر حق آزادی<sup>۲</sup> را با چشم‌اندازهای جدید و افق‌های نامحدود مواجه ساخته است. این موضوع به‌عنوان آرمان فضای سایبر به‌صراحت در «اعلامیه استقلال فضای سایبر»<sup>۳</sup> بیان شده است.<sup>۴</sup> علاوه‌براین، کنوانسیون جرائم سایبری بوداپست مصوب ۲۰۰۱ که درصدد رویه‌سازی و قانونمندکردن کنش‌ها و واکنش‌ها درخصوص جرایم سایبری بوده است، در ماده ۱۵ خود با عنوان شروط و تضمین‌ها، دولت‌های عضو را موظف کرده است که هنگام وضع قوانین و مقررات، حقوق و آزادی‌های فردی از جمله حق آزادی بیان و حریم خصوصی افراد را مطابق با قوانین و مقررات بین‌المللی دقیقاً رعایت کنند. در بخشی از این ماده آمده است:

دولت‌ها باید اطمینان دهند که حمایت شایسته‌ای از حقوق و آزادی‌های بشری به عمل می‌آورند که شامل حقوق برخاسته از تعهداتی است که آن‌ها در کنوانسیون شورای اروپا راجع به حمایت از حقوق و آزادی‌های اساسی بشر (۱۹۵۰) و سایر اسناد لازم‌الاجرای حقوق بشری که پذیرفته‌اند (جلالی‌فراهانی، ۱۳۸۹، ص ۵۸).

با عنایت به نوع فعالیت کاربران فضای سایبر می‌شود دو شعبه فرعی از حق آزادی را استخراج و از یکدیگر تفکیک کرد. شعبه اول، آزادی فعالیت برای آن‌دسته از کاربران فضای سایبر است که از ابزار سایبر به‌صورت فعال بهره‌برداری می‌کنند و به بارگذاری اطلاعات در این فضا

۱. برای مطالعه بیشتر در این زمینه ر.ک:

انصاری، باقر (۱۳۹۹). حق دسترسی به اینترنت، مبانی و محتوا. مجله حقوقی دادگستری، ۸۴(۱۱۲)، ۵۱-۷۹.

۲. تمامی افراد بشر آزاد زاده می‌شوند و از لحاظ حیثیت و کرامت و حقوق با هم برابرند.

۳. همه افراد بشر حق دارند، بی هیچ‌گونه تمایزی، از تمامی حقوق و آزادی‌های ذکرشده در این اعلامیه برخوردار شوند و...

۴. هر فردی حق زندگی، آزادی و امنیت شخصی دارد.

۵. هر فردی حق آزادی عقیده و بیان دارد.

۶. هر فردی حق دارد آزادانه در زندگی فرهنگی اجتماع شریک و سهم‌گردد.

۷. آزادی به‌مثابه یک حق قلمرو بسیار گسترده‌ای دارد و حق‌های دیگری و از جمله حق‌های شهروندی از آن انشعب می‌یابد. ماده یکم، دوم، سوم، نوزدهم، بیست‌وهفتم و... از اعلامیه جهانی حقوق بشر و ماده ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی که مقرر می‌دارد «هیچ‌کس نباید در زندگی خصوصی و خانواده و اقامتگاه یا مکاتبات مورد مداخلات خودسرانه (بدون مجوز) یا خلاف قانون قرار گیرد» و ده‌ها مقررۀ جهانی و منطقه‌ای دیگر ترجمان و بازتاب این حق طبیعی بنیادین به‌شمار می‌آیند.

۸. این توضیح لازم است که این اعلامیه جنبه نمادین دارد و فاقد ضمانت اجرا است.

۹. در این اعلامیه آمده است:

ای دولت‌های جهان صنعتی، ای غول‌های کسل‌کننده‌ای که از فلز و شهوانیت ساخته شده‌اند، من از اهالی فضای سایبرم... در جایی که ما گرد هم می‌آییم، شما از هیچ حاکمیتی برخوردار نیستید... ما هیچ دولت منتخبی نداریم و امیدواریم هیچ حکومتی در اینجا پدیدار نشود (بارلو، اعلامیه استقلال فضای سایبر، ۱۹۹۶).

می‌پردازند. شعبه دوم، آزادی دسترسی به اطلاعات برای آن دسته از کاربرانی است که به صورت منفعل از فضای سایبر استفاده می‌کنند و به بارگیری اطلاعات از این فضا می‌پردازند.

حال باید دید که آیا فیلترینگ می‌تواند محدودیتی در قبال دو حق یاد شده فراهم آورد؟

به نظر می‌رسد پالایش مستقیم و غیرمستقیم محتوا این دو شعبه از حق آزادی را با مخاطره مواجه ساخته است؛ گاه کاربران منفعل فضای سایبر، به علت مسدودبودن یا پالایش محتوای موردنیازشان، از دسترسی آزاد به اطلاعات منع می‌شوند و از فیلترینگ برای سانسور استفاده می‌شود. گاهی از فیلترینگ به عنوان ضمانت اجرا بهره‌برداری می‌شود و کاربران فعال فضای سایبر، به علت نداشتن مجوز، با مسدودشدن فضای فعالیت از ادامه فعالیت منع می‌شوند.

### ۱-۱-۱. فیلترینگ به مثابه ضمانت اجرای دریافت نکردن مجوز

«سازمان بین‌المللی یونسکو در گزارش شاخص‌های مربوط به توسعه رسانه‌ها که در مارس ۲۰۰۸ به تصویب رساند، ضمن تکیه بر ضرورت مقابله دولت‌ها با محدودیت‌های مربوط به تأسیس و انتشار رسانه‌ها، به آن‌ها توصیه کرده است که پایگاه‌های اینترنتی (وبگاه‌ها)، وبلاگ‌ها و پخش‌کنندگان برنامه‌های اینترنتی الزام به ثبت نام نزد مقامات عمومی نداشته باشند و نباید برای فعالیت‌های خود از این مقامات اجازه بگیرند» (رضایی و بابازاده مقدم، ۱۳۹۳، ص ۶۳). هرچند ظاهراً دریافت مجوز و ثبت نام برای تأسیس رسانه، پایگاه‌های اینترنتی، اجتماعات مجازی و... غیرموجه به نظر نمی‌رسد، بیم آن می‌رود که دریافت مجوز تأسیس حقوق و آزادی‌های بنیادین را به خطر اندازد. چه، آن‌که در فرض دریافت نکردن مجوز دولت محق به فیلترکردن و مسدودسازی است. توضیح آن‌که «در کشورهای دارای نظام اقتدارگرا که عموماً حکومت‌ها از آزادی‌های سیاسی مردم ترس دارند و می‌کوشند به هر شکل این آزادی‌ها را محدود و به نوعی کانالیزه کنند، تأسیس و فعالیت رسانه، تابع نظام پیشگیری یا نظام تأمینی است. در این کشورها، برای کنترل افشاگری و فعالیت‌های روشنگرانه گروه‌های مخالف و منتقد، اشخاص برای تأسیس رسانه باید مجوز بگیرند. اتخاذ این سیاست به مرور موجب می‌شود که فقط اشخاص مورداعتماد حکومت بتوانند مطبوعات و سایر رسانه‌ها را تأسیس کنند و به این ترتیب تمامی تریبون‌های خبری و اطلاع‌رسانی در دست حکومت باقی می‌ماند» (رضایی و بابازاده مقدم، ۱۳۹۳، ص ۶۲).

خوشبختانه، در نظام حقوقی ایران، اصل نهم قانون اساسی<sup>۱</sup> از حق آزادی ملت حمایت همه‌جانبه کرده است، تا آنجا که حتی با وضع قانون نیز نمی‌توان آزادی افراد ملت را سلب نمود کرد؛ از این رو، هرگونه استفاده از ابزارهای سلبی یا تنبیهی برای تحدید آزادی‌های افراد ملت ولو با وضع قانون مخالف قانون اساسی است. بنابراین، آنچه در مواد ۲ و ۲۹ طرح «سامان‌دهی پیام‌رسان‌های اجتماعی» آمده است، به این کیفیت که ماده ۲ طرح مذکور عرضه و ارائه خدمات پیام‌رسان‌های اجتماعی را منوط به ثبت نام و دریافت مجوزهای لازم دانسته است و ضمانت اجرای این امر را مسدودسازی دسترسی به آن قرار داده است و ماده ۲۹ این طرح برای ایجاد یا اداره کانال و گروه‌هایی که با نقض غیرقانونی تدابیر مسدودسازی تشکیل شده‌اند به حربه مجازات متوسل شده است، نمی‌تواند مورد حمایت قانون اساسی شناخته شود.

### ۱-۱-۲. فیلترینگ به مثابه ابزار سانسور

«بی‌گمان افراط در پیشگیری نژادهای حقوق بشر را که جامعه جهانی برای دستیابی به آن بهای بسیاری پرداخته است» (سواری و پورحسن، ۱۳۹۲، ص ۸۰) نقض می‌کند و حتی ممکن است آثار نامطلوب‌تری از جرم بر جامعه تحمیل کند. رصد فضای سایبر در ایران نشان می‌دهد که از محتواهای منافی عفت تا تارنماهای سیاسی و شبکه‌های اجتماعی را دربر گرفته است. قطع نظر از محتواهای منافی عفت و مستقیماً مجرمانه مانند تارنماهای اشاعه خشونت و نفرت و خریدوفروش مواد مخدر و برخی موارد این چنینی که پالایش فضای مجازی از آن‌ها مورد

۱. در جمهوری اسلامی ایران آزادی و استقلال و وحدت و تمامیت ارضی کشور از یکدیگر تفکیک‌ناپذیرند و حفظ آن‌ها وظیفه دولت و آحاد ملت است. هیچ فرد یا گروه یا مقامی حق ندارد به نام استفاده از آزادی به استقلال سیاسی، فرهنگی، اقتصادی، نظامی و تمامیت ارضی ایران کمترین خدشه‌ای وارد کند و هیچ مقامی حق ندارد به نام حفظ استقلال و تمامیت ارضی کشور آزادی‌های مشروع را، هرچند با وضع قوانین و مقررات، سلب کند.

وفاق نسبی جامعه است، برخی شبکه‌های اجتماعی مانند فیس‌بوک، تلگرام و یوتیوب نیز بدون استفاده از ابزارهای فیلترشکن غیرقابل دسترسی است؛ بر اساس پژوهشی جامع، در دامنه فضای مجازی «ایران بیش از ۴۸ درصد از پانصد وبگاه برتر در رتبه‌بندی جامع الکسا فیلتر است» (Aryan et al., 2013). حتی در پژوهشی داخلی اعلام شده است که «ایران در خصوص مسدودسازی و فیلترینگ رسانه‌های اجتماعی مجازی در جهان در جایگاه اول قرار گرفته است» (بصیریان جهرمی و خانیکی، ۱۳۹۳، ص ۶۱). همچنین، بنابر آمار ارائه شده از سوی متصدیان پالایش محتوا، تا آبان‌ماه ۱۳۸۷ «بیش از ۵ میلیون وبگاه اینترنتی در ایران فیلتر شده است» (خرم‌آبادی، ۱۳۸۷). پژوهش‌ها و آمار مذکور حکایت از آن دارد که در حال حاضر بعضاً از روش فیلترینگ به‌عنوان ابزار سانسور استفاده نامطلوبی می‌شود. برای نمونه، فیلترینگ محتوای خبری برخی از خبرگزاری‌های بین‌المللی یا برخی وبگاه‌های فرهنگی-اجتماعی با آموزش محور مانند یوتیوب که در محافل عملی دانشگاهی کاربرد بسیاری دارد از این دست است. نباید نادیده گرفت که استفاده از ابزار فیلترینگ برای سانسور در بسیاری از کشورهای مدعی حقوق بشر نیز وجود دارد. برای نمونه، وبگاه ویکی‌لیکس، که با هدف ایجاد شفافیت در عملکرد دولت‌ها فعالیت دارد، در بازه‌های زمانی مشخص که به انتشار اطلاعات علیه دولت‌های خاصی پرداخته است از سوی آن دولت مسدود شده و مورد تعقیب قضایی نیز قرار گرفته است.<sup>۲</sup>

## ۱-۲. نقد پالایش محتوا در پرتو حق بر امنیت

از مهم‌ترین حق‌هایی که در تمامی نظام‌های دنیا برای شهروندان به رسمیت شناخته شده است حق بر امنیت است. در پرتو تأمین حق بر امنیت است که انسان می‌تواند از دیگر حقوق خود و از جمله حق بر آزادی بهره‌مند شود. برخی حق بر امنیت را چنین تعریف کرده‌اند: «اطمینان خاطری که بر اساس آن افراد در جامعه‌ای که زندگی می‌کنند نسبت به حقوق مادی و معنوی خود بیم و هراسی نداشته باشند.» (اسماعیل‌پور و شریعت‌باقری، ۱۳۹۳، ص ۲۰) برخی دیگر امنیت را وضعیتی می‌دانند که در آن، «انسان به عدم تعرض به حقوق فردی خود اطمینان دارد» (علیزاده و کاویانی، ۱۳۹۰، ص ۲۵۷). باید توجه داشت که این حق بسان شمشیر دولبه‌ای است که دولت‌مردان نیز فعالیت‌های خویش را در راستای تأمین آن توجیه می‌کنند. در هر حال، شناخت برخی مستندات این حق ضروری است، چه ممکن است افرادی از اصل منکر چنین حقی در فضای سایبر شوند.

### ۱-۲-۱. مستندات و مصادیق حق بر امنیت در فضای سایبر

بی‌گمان حق شهروندان بر امنیت به دنیای خاکی محدود نمی‌شود و با توجه به گسترش زیست سایبری شهروندان، حق امنیت شهروندان در فضای سایبر موضوعی مهم و در خور توجه است. مبانی و مستندات حق امنیت در فضای سایبر متفاوت با مبانی و مستندات این حق در فضای واقعی نیست. به عبارت دیگر، همان مبناها و مقرره‌هایی که این حق را برای افراد در جامعه به رسمیت شناخته است قابلیت تعمیم به فضای سایبر را دارد و می‌توان حق بر امنیت شهروندان در فضای سایبر را در قالب همان مبناها و مستندات شناسایی کرد. در قانون اساسی ایران، برای به رسمیت شناختن امنیت شهروندان، هم در برابر افراد جامعه و هم در برابر هیئت حاکمه، اصول عدیده‌ای طراحی و تدوین شده است که مهم‌ترین آن‌ها اصل ۲۲ قانون اساسی است. این اصل مقرر می‌دارد: «حیثیت، جان، مال، حقوق، مسکن و شغل اشخاص از تعرض مصون است مگر در مواردی که قانون تجویز کند.»

۱. الکسا (Alexa) عنوان سامانه‌ای وابسته به سایت آمازون (Amazon.com) است که خدمات آن در آدرس Alexa.com ارائه می‌شود. هدف از این سامانه جمع‌آوری اطلاعات ترافیک وب و رتبه‌بندی پایگاه‌های اینترنتی از نظر تعداد بازدیدها است که با در نظر گرفتن یکسری معیارهای محاسباتی و الگوریتم‌های خاص، نهایتاً سایت‌های شبکه جهانی وب را به لحاظ میزان دیده‌شدن صفحات آن‌ها رتبه‌بندی می‌کند.

۲. برای مطالعه بیشتر در این زمینه ر.ک: Jones, A. (2010). Pentagon Papers II? On WikiLeaks and the First Amendment. The Wall Street Journal. Retrieved, 6.

این اصل، به‌منزله اصلی عام، مصادیق و گستره فراوانی را دربر می‌گیرد و به دنبال تضمین مصونیت حیثیت، جان، مال، حقوق، مسکن و شغل اشخاص هم در برابر دولت و هم در برابر شهروندان است. در اصل ۲۵ قانون اساسی نیز مصونیت ارتباطاتی شهروندان از هر نوع تجسس و سانسور محافظت شده است:

«بازرسی و نرساندن نامه‌ها، ضبط و فاش کردن مکالمات تلفنی، افشای مخبرات تلگرافی و تلکس، سانسور،

عدم‌مخابره و نرساندن آن‌ها، استراق‌سمع و هر گونه تجسس ممنوع است مگر به حکم قانون.»

کاربرد حق امنیت و مصادیق آن در فضای سایبر به‌علت ویژگی‌های خاص داده‌ها و اطلاعات مانند تکثیرپذیری، غیرملموس بودن و آسیب‌پذیری قدری متفاوت است. «مصادیق حق مذکور در فضای سایبر را می‌شود به «امنیت محرمانگی داده‌ها» و «امنیت تمامیت داده‌ها» بسط داد» (فضلی، ۱۳۸۹، ص ۱۹۷). همچنین می‌شود از «امنیت بر دسترسی به داده» به‌عنوان شق سوم امنیت سایبری یاد کرد. امنیت بر محرمانگی ارتباط مستقیمی با موضوع فیلترینگ پیدا نمی‌کند، اما دو دسته دیگر به‌علت پالایش غیراصولی فضای مجازی در معرض تضییع قرار گرفته‌اند.

### ۱-۲-۲. فیلترینگ و نقض حق امنیت بر تمامیت داده‌ها

امنیت بر «تمامیت داده‌ها» متضمن این مهم است که اصل اطلاعات مصونیت داشته باشد و در معرض نابودی یا مخاطره قرار نگیرد. اجرای پالایش محتوا به شیوه رایج حق شهروندان فضای مجازی بر امنیت بر تمامیت اطلاعات را نادیده گرفته است. توضیح آن‌که، قانونگذار در سه ماده‌ای که به بحث فیلترینگ پرداخته است، یعنی مواد ۷۴۹، ۷۵۰ و ۷۵۱ قانون مجازات اسلامی، به «پالایش محتواهای مجرمانه» تصریح نموده است. این نکته مهم باید مورد توجه قرار گیرد که عبارت محتوای مجرمانه که به‌عنوان موضوع پالایش در مواد قانونی مذکور آمده است به معنای مظروف فضای مجازی و آن چیزی است که در داخل یک وبگاه یا در یک شبکه اجتماعی وجود دارد و نمی‌شود به‌منظور پالایش محتوای مجرمانه وبگاه یا شبکه اجتماعی را کاملاً مسدود ساخت. این درحالی است که مجریان پالایش محتوا، به‌جای تکلیف مقرر در مواد ۷۴۹ تا ۷۵۰ مبنی بر پالایش محتوا و حذف محتواهای ناسالم، به مسدودسازی دسترسی به کلیه فضایی که محتوای ناسالم در آن قرار دارد و به تعبیر دقیق‌تر به بلوکه کردن آدرس اینترنتی مبادرت می‌ورزند؛ بدیهی است که مسدودسازی ناگهانی دسترسی به یک وبگاه باعث ازبین‌رفتن حجم زیادی از داده‌ها و اطلاعاتی می‌شود که سابقاً توسط مدیران وبگاه بارگذاری شده است.

این درحالی است که در بسیاری از کشورها سازوکارهای حمایت از داده‌ها درحال تکامل و توسعه است و مقرره‌گذاری‌های نوین و کارآمدی در این خصوص انجام می‌شود. برای نمونه، در سال ۲۰۱۶، با هدف حمایت از این حق، کنوانسیون حفاظت از داده‌های اتحادیه اروپا مقرراتی درخصوص حفاظت از داده و محرمانگی با عنوان «مقررات عمومی حفاظت از داده اتحادیه اروپا»<sup>۱</sup> وضع کرد. مطابق با ماده ۱ این قانون، حمایت از اشخاص حقیقی در رابطه با پردازش داده‌های شخصی حقیقی اساسی است،<sup>۲</sup> ازاین‌رو هر نوع پردازش اعم از اصلاح و ویرایش و حذف داده‌ها در انحصار مالک داده است و مطابق با ماده ۶ این کنوانسیون، جز با رضایت شخص مالک داده و فقط در موردی که او اجازه دهد، نباید داده‌های شخصی پردازش شود مگر در شرایط محدود که در همین ماده تصریح شده است.<sup>۳</sup>

1. The General Data Protection Regulation (GDPR) (EU) 2016/679

2 (1) The protection of natural persons in relation to the processing of personal data is a fundamental right.

3 Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;



### ۱-۲-۳. فیلترینگ و نقض حق امنیت در دسترسی به داده‌ها

«امنیت در «دسترسی به داده‌ها یا اطلاعات» به معنای نبود ممانعت غیرمجاز در دسترسی به اطلاعات» (عالی‌پور، ۱۳۹۰، ص ۴۵) و امکان استفاده امن از فناوری اطلاعات و ارتباطات است. پالایش محتوا به شیوه جاری این حق بر امنیت را با تهدید جدی مواجه ساخته است. برای مثال، با عمومی شدن استفاده از شبکه اجتماعی تلگرام در میان شهروندان ایرانی، علاوه بر بارگذاری اطلاعات توسط کاربران عادی در گروه‌ها و کانال‌های شبکه اجتماعی مذکور، برخی از ادارات و ارگان‌های دولتی نیز داده‌های اطلاعاتی بسیاری را در آن بارگذاری کردند. با مسدود شدن این شبکه اجتماعی، حق دسترسی به این داده‌ها و اطلاعات که غالباً غیربزهکارانه بود برای تمامی کاربران سلب یا دست‌کم دشوار شده است؛ به گونه‌ای که بدون استفاده از ابزارهای وی پی ان نمی‌توان به اطلاعاتی که پیش از فیلتر شدن در آن وجود داشت دست یافت. به این ترتیب باید اذعان داشت، فیلترینگ فراگیر به شیوه جاری که متوجه همه کاربران اعم از بزهکار و غیربزهکار می‌شود، اگر موجب اتلاف داده‌ها (که در خصوص وبگاه‌ها رخ می‌دهد) نشود، موجب دشواری دسترسی به آن‌ها (در فضاهای با میزبان خارجی مانند شبکه‌های اجتماعی) می‌شود.<sup>۱</sup> بنابراین، پالایش محتوا با دشوار ساختن دسترسی به داده‌ها، از آن جهت به حق امنیت شهروندان خلل وارد ساخته است که فراغت و اطمینان خاطر آنان در استفاده و دسترسی به داده‌ها را سلب کرده است. با همین ملاحظات است که پیشنهاد شده است «نهادی مستقل و حقوقی وجود داشته باشد تا با نظارت صحیح بر نحوه اجرای قواعد حمایت از داده از نقض این حق جلوگیری کند» (زارعیان و واحد، ۱۳۹۹، ص ۴۷)، آن‌گونه که در بسیاری از کشورهای اروپایی و برخی کشورهای آسیای شرقی وجود دارد.<sup>۲</sup>

### ۲. پالایش محتوا در سنجه نظریه‌های کنترل در دانش جرم‌شناسی

به‌رغم تلاش جرم‌شناسان برای طراحی الگوهای پیشگیری از جرم بر مبنای تبیین‌های علمی و توصیه‌هایشان به رعایت اصول و رهیافت‌های دانش جرم‌شناسی در اجرای برنامه‌های پیشگیری، به نظر می‌رسد «این تلاش‌ها در رقابت با جنبه‌های احساسی و سیاسی حاکم بر پیشگیری از جرم (همچون توجه به کمیت و سرعت رسیدن به نتیجه) با موفقیت چندانی همراه نبوده است» (فرجیها، ۱۳۸۸، ص ۲۹۵). سیاست‌گذاری برای پیشگیری بدون توجه به رهیافت‌های دانش جرم‌شناسی صورت می‌گیرد. در وضعیت کنونی که مقوله پیشگیری از موضوعی علمی و فنی به دغدغه سیاست‌گذاری تبدیل شده است، نهایتاً می‌توان هم‌خوانی یا ناهم‌خوانی راهبردها و تدابیر پیشگیرانه در حال اجرا را با آموزه‌ها و رهیافت‌های علمی سنجید.

ویژگی انکارناپذیر فیلترینگ به شیوه جاری در ایران دامنه زیاد کنترل از نظر کمی (حجم فیلترینگ) و کیفی (موضوعات مورد فیلترینگ) است. به بیان دیگر، هم حجم و تعداد مصادیق و هم گستره وسیع موضوعاتی که فیلتر شده‌اند حکایت از «کنترل شدید» شهروندان فضای سایبر دارد. این وضعیت برای کاربرانی که فعالانه از فضای سایبر استفاده می‌کنند و به ساخت محتوا در این فضا مبادرت می‌ورزند و هم برای کاربرانی که صرفاً به بهره‌برداری منفعلانه از فضای سایبر بدون ساخت محتوا تمایل دارند وجود دارد. جست‌وجوی نظریات جرم‌شناسی مرتبط با موضوع

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party

۱. علاوه بر این، گفت‌وگو رسمی و غیررسمی مراجع سیاست‌گذار در خصوص فیلترینگ فضاهای مجازی عمدتاً مبتنی بر تهدید، ارباب، استفاده از ظرفیت‌های کیفری و... است که موجب احساس ناامنی یا نبود احساس امنیت در میان کاربران فضای سایبر شده است؛ مرور اظهارات مقامات متصدی فیلترینگ و هشدارهای مکرر ایشان مبنی بر مسدودسازی شبکه‌های اجتماعی و برنامه‌های کاربردی حکایت از آن دارد که شهروندان فضای مجازی احساس امنیت لازم را در این فضاها ندارند. شاهد سخن آن‌ها که بسیاری از کانال‌ها یا گروه‌ها که بیم مسدود شدن دارند، در دوره فعالیت خود آدرس کانال یا گروه دیگر را به‌عنوان آدرس کمکی برای ادامه فعالیت در صورت فیلترینگ معرفی می‌کنند.

۲. برای مطالعه تطبیقی در زمینه حمایت از داده‌ها در کشورهای مختلف ر.ک: زارعیان، داود و واحد، فائزه (۱۳۹۹). بررسی حقوقی رگولاتوری‌های حمایت از داده. فصلنامه علمی رسانه، ۳۱(۱)، ۷۲-۴۷.

بحث مجاللی بیشتر می‌طلبند ولی دست‌کم واکاوی نظریه‌ها با کلیدواژه «کنترل شدید» به مدخل‌های زیادی در این باره منتهی می‌شود که در میان آن‌ها دو نظریه «تراز کنترل» و «انتقال فضا» ارتباط بیشتری با جنبه‌های کمی و کیفی موضوع پالایش محتوا دارند.

## ۱-۲. کنترل شدید کاربران منفعل در سنجه نظریه تراز کنترل

چارلز تیتل نظریه‌ای کلی درباره کژروی پیشنهاد می‌کند که نظریه‌ای پیچیده و تلفیقی به حساب می‌آید. مؤلفه کلیدی این نظریه «تراز کنترل»<sup>۱</sup> یا تعادل کنترل است که به علت محوریت یافتن این مؤلفه تئوری به همین نام خوانده شده است.<sup>۲</sup> این نظریه، در راستای تحلیل بزهکاری و سرکشی از قانون، میزان کنترل را بررسی می‌کند؛ در واقع در این نظریه سازگاری و هم‌نوبی با میزان کنترل همبسته است، نه با اصل کنترل. ادعای اصلی این نظریه آن است که «میزان کنترلی که بر هر فرد اعمال می‌شود، نسبت به میزان کنترلی که او می‌تواند اعمال کند، امکان رخ دادن کژروی و نیز نوع کژروی احتمالی وی را تعیین می‌کند.» (Tittle, 1995, p. 35) به این معنا که «اگر کنترلی که افراد اعمال می‌کنند با کنترلی که بر آن‌ها صورت می‌گیرد برابر باشد، کمتر احتمال دارد که افراد مرتکب جرم شوند» (Tittle, 2010, p. 21). اگر این تعادل بر هم زده شود، یعنی کنترلی که بر افراد اعمال می‌شود بیش از کنترلی باشد که آن‌ها می‌توانند اعمال کنند یا برعکس، احتمال وقوع جرم افزایش می‌یابد. به این ترتیب، یک رهیافت این نظریه این است که افرادی که به‌گونه‌ای نامتوازن و شدید از سوی دیگران کنترل شوند تمایل بیشتری به کژروی و نافرمانی پیدا می‌کنند.

منعی وجود ندارد که از رهیافت‌های عمومی این نظریه برای تحلیل موضوع بهره برد و پالایش محتوا یا فیلترینگ را به مثابه ابزار کنترل دولتی در نظر گرفت. بر این مبنا می‌توان گفت کنترل زیادی که با کاربست پالایش محتوا و محدودیت دسترسی به برخی محتواها بر طیف گسترده‌ای از انتخاب‌های کاربران در فضاهای سایبری ایران اعمال می‌شود و تأمین نشدن نظر مردم در این خصوص به نادیده گرفتن یا نقض تدابیر مسدودسازی منجر شده است؛ آن‌گاه که کاربر ایرانی در فضاهای مجازی آزادی خود را می‌خواهد و با وبگاه‌ها یا شبکه‌های اجتماعی مسدود شده مواجه می‌شود و علتی پذیرفتنی برای این حجم از کنترل نمی‌یابد، احتمالاً و بر مبنای این نظریه سرکشی از قانون را بر اطاعت از سلیقه متصدیان فیلترینگ ترجیح می‌دهد.

## ۲-۲. کنترل شدید کاربران فعال در سنجه نظریه انتقال فضا

در سال ۲۰۰۸، جایشانکار نظریه‌ای با عنوان «انتقال فضا» را پایه‌ریزی کرد. این نظریه، در تحلیل علت‌شناسی بزهکاری سایبری، رهیافت‌های هفت‌گانه‌ای را ارائه داد. در رهیافت ششم این نظریه به این موضوع پرداخته شده است که چرا و چگونه احتمال ارتکاب جرم سایبری در جوامع بسته از احتمال ارتکاب جرایم مشابه در جوامع باز بیشتر است. جایشانکار در تبیین این رهیافت نظریه خود بیان می‌دارد: «مردم در جوامع آزاد گزینه‌های متعددی برای بروز نارضایتی و خشم خود دارند، در حالی که در جوامع بسته تلاش‌ها در جهت هم‌رنگ شدن اجباری اجتماع به بروز رفتارهای مجرمانه زیرزمینی می‌انجامد.» (Jaishankar, 2008, p. 293) در ارتباط این نظریه با موضوع پالایش فضای مجازی می‌شود گفت، در جامعه‌ای که برخی هنجارهای عرفی کمتر اجازه بروز و ظهور شادی فعالیت پرنشاط اجتماعی به نوجوانان می‌دهد، برای نوجوانانی که می‌خواهند نقش فعال و پرنشاطی داشته باشند دیر با زود پدیده کوچ اجباری به فضاهای مجازی رخ می‌دهد. این افراد درصدد برمی‌آیند، فارغ از مخالفت اطرافیان، با میزبانی در فضای مجازی و ساخت محتوا نقش فعال داشته باشند. اگر فضای سایبر نیز با محدودیت‌های زیاد در بارگذاری محتواها همراه باشد، چون این افراد زیستگاه سومی برای خود نمی‌یابند، احتمالاً در مخالفت با این محدودیت‌ها می‌کوشند از مجازی بودن‌های فضای سایبر و دشواری‌های کشف و تعقیب جرم در این محیط تا می‌توانند استفاده سوء کنند؛ به

### 1. Control Balance

۲. برای مطالعه بیشتر درباره این نظریه بنگرید به: تامس، برنارد، جفری، اسنیس و الکساندر، جروالد (۱۳۹۴). جرم‌شناسی نظری ولد. علی شجاعی (مترجم). تهران: انتشارات دادگستر، ۴۱۸-۴۱۲.

این ترتیب میزان سرکشی از مقرره‌های قانونی و حتی ارتکاب جرم در این محیط به صورت مضاعف تشدید می‌شود. در واقع، در چنین جوامعی، کنترل شدید مخالفت شدیدتر شهروندان به‌ویژه جوانان و نوجوانان فراری از دنیای واقعی را به همراه خواهد داشت؛ زیرا انتظار شهروندان چنین جوامعی از فضای سایبر فضایی آزاد از کنترل و متفاوت با دنیای پیرامونی خود است. هنگامی که با محدودیت و کنترل در این فضا مواجه شوند، تمامی ابزارهای فناوری در دسترس را برای نقض کنترل به‌کار می‌گیرند تا آرمان خود از آزادی را در تنها مکان ممکن یعنی فضای سایبر رقم بزنند.

### ۳. سنجش کارآمدی پالایش محتوا در ایران

قلمرو فضای سایبر بسیار گسترده‌تر از آن است که هر اقدام غیرقانونی در آن توسط متصدیان دستگاه عدالت کیفری رصد و کنترل شود. همچنین ساختار فضای سایبر به‌گونه‌ای است که هرگز کوچک‌ترین تحمیل قیم‌مآبانه را نمی‌پذیرد؛ زیرا در ساختار فضای سایبر تصمیمات و اقدامات عمودی یک‌سویه جایی ندارد. بی‌توجهی به این ویژگی‌های منحصر به فرد فضای مجازی موجب توسل متصدیان دستگاه عدالت کیفری به فیلترینگ فراگیر عمودی شده است. باید توجه داشت که تأثیر نامطلوب سیاست‌های پالایش‌سازی تحمیلی دولتی بسیار گسترده است و ممکن است نه تنها به ناکارآمدی در پیشگیری از جرم منتهی شود، آثار و عواقب ناخوشایندی را نیز در پی داشته باشد؛ مطالعه نظری و فراتحلیل آمار و ارقام موجود به‌ویژه مقایسه وضعیت فضای مجازی پس از فیلترینگ فراگیر شبکه‌های اجتماعی با وضعیت پیش از آن نشان می‌دهد که پالایش‌سازی به شیوه جاری در ایران نتایج نامطلوبی همچون نافرمانی مدنی و عمومی شدن جرم را به دنبال داشته است.

### ۳-۱. نافرمانی مدنی کاربران

بررسی‌ها نشان می‌دهد که با وجود همه محدودیت‌های سلبی اعمال‌شده از سوی سیاست‌گذاران رسانه‌ای، شهروندان ایرانی اینترنت چندان از فیلترینگ و قوانین اینترنتی تعیین‌شده تبعیت نمی‌کنند. شاهد سخن پرشماری اعضای ایرانی در شبکه‌های اجتماعی فیلترشده مانند فیس‌بوک، توئیتر و اخیراً تلگرام است. بنا بر آمار مؤسسه بین‌المللی «آمار دنیای اینترنت»، بیش از ۴۰ میلیون ایرانی در شبکه اجتماعی فیس‌بوک، که سال‌هاست در ایران مسدود است، عضویت دارند.<sup>۱</sup> همچنین، بنابر نتایج نظرسنجی مرکز افکارسنجی دانشجویان ایران (ایسپا) وابسته به جهاد دانشگاهی، ۷۹ درصد از کاربران تلگرام پس از حدود دو ماه از فیلترینگ این شبکه اجتماعی در اردیبهشت ۱۳۹۷ همچنان در این پیام‌رسان حضور دارند.<sup>۲</sup> بدیهی است دسترسی به فضاهای مسدودشده در محیط سایبر جز با نصب و استفاده از فیلترشکن ممکن نیست. به این ترتیب باید اذعان نمود که سیاست‌های غلط پالایش محتوا، مستقیم یا غیرمستقیم، موجبات نافرمانی مدنی در گستره جمعیتی چند ده میلیون نفری در فضای سایبر ایران را فراهم کرده است. به دیگر سخن، فیلترینگ شبکه‌های ارتباطی و اجتماعی موجود در فضای مجازی نه تنها موجب کوچ کاربران از شبکه‌های اجتماعی فیلترشده نشده است، موجب دانلود بی‌سابقه نرم‌افزارهای وی پی ان یا آنچه در ایران به فیلترشکن شهرت دارد شده است. به‌طور نمونه، بررسی میزان بارگذاری برنامه‌های وی پی ان توسط کاربران ایرانی در اپ‌استورها<sup>۳</sup> نشان از دانلود بی‌سابقه ابزارهای فیلترشکن در دو مقطع زمانی دی‌ماه ۱۳۹۶ و اردیبهشت ۱۳۹۷، بعد از فیلترشکن تلگرام به صورت موقت و دائم دارد. به گزارش روزنامه ایران، طی یک هفته پس از فیلترینگ تلگرام در دی‌ماه ۱۳۹۶، دانلود فیلترشکن سایفون از ۳۵ هزار بار دانلود در روز به روزانه ۷۰۰ هزار بار رسیده است که خود رقم جالب‌توجهی است (جلیلی، ۱۳۹۶). همچنین، بنابر اعلام رئیس پلیس فتا، بیش از ۱۰ تا ۱۲ میلیون نفر در ایران از ابزارهای

۱. برای دسترسی به آمار مذکور مراجعه کنید به: <https://www.internetworldstats.com/middle.htm#ir>

۲. برای مشاهده این نظرسنجی ر.ک به: <http://ispa.ir/Default/Details/fa/1925> -نتایج نظرسنجی -ایسپا- نشان داد: ۷۹ درصد از -استفاده‌کنندگان- تلگرام، -همچنان- در -این-

پیام‌رسان- حضور- دارند

۳. اپ‌استورها مراکز دانلود برنامه‌های کاربردی‌اند. گوگل‌پلی، مهم‌ترین اپ‌استور در جهان، یکی از فعال‌ترین اپ‌استورها است که انواع برنامه‌های کاربردی در آن برای کاربران قابل بارگذاری است.

فیلترشکن استفاده می‌کنند (هادیان‌فر، ۱۳۹۷). بنابر آنچه در وبگاه پلیس فتا اعلام شده است، ۳۰ درصد از کاربران ایرانی از برنامه‌های فیلترشکن استفاده می‌کنند.<sup>۱</sup>

### ۳-۲. عمومی شدن بزهکاری

مطابق با آمار پلیس فتا از سال ۱۳۹۰ تا ۱۳۹۷ جرایم سایبری ۹۰۰ درصد افزایش داشته است. بی‌شک تحلیل این افزایش بی‌سابقه در جرم دشوار است، اما نمی‌شود نادیده گرفت که نصب میلیون‌ها برنامه وی پی ان توسط کاربران ایرانی به‌نوعی تمامی تدابیر پالایش محتوایی را که در سال‌های اخیر برای پیشگیری از جرم صورت گرفته بود بی‌اثر ساخته است؛ زیرا عموم کاربران، با بهره‌برداری از فیلترشکن‌های رایگان موجود در محل‌های توزیع و عرضه برنامه‌های کاربردی، به‌سادگی این امکان را یافتند که به همه فضاهایی که قبلاً دسترسی به آن‌ها برایشان ممکن نبود وارد شوند. بنابراین، در حال حاضر، به‌واسطه سیاست‌های نادرست در فضای مجازی، نه فقط بزهکاران بلکه بسیاری از شهروندان متعارف فضای سایبر به ارتکاب جرم برانگیخته می‌شوند و «بزهکاری، دست‌کم در برخی مصادیق خود، دیگر محدود به گروه‌های اقلیت بزهکارانه نیست بلکه جزئی از بافتار [ویژگی‌های ثابت] فضای سایبر شده است و توسط شهروندان متعارف فضای سایبر نیز انجام می‌شود» (حاجی‌ده‌آبادی و سلیمی، ۱۳۹۵، ص ۳۰۳). در بررسی آماری که نگارندگان این نوشتار با استفاده از امکانات ابزار گوگل‌ترندز در تیرماه سال ۱۳۹۸ انجام دادند، میزان جست‌وجوی یک واژه هزینه‌نگاری در یک سال گذشته در جست‌وجوگر گوگل واکاوی شد. نتایج این بررسی نشان می‌دهد که روند جست‌وجوی این واژه هزینه‌نگاری در یک سال گذشته کاملاً سیر صعودی داشته است که بی‌گمان این موضوع با سیاست‌گذاری‌های اخیر و تشدید فیلترینگ در فضای مجازی ارتباط خواهد داشت. مقایسه میزان جست‌وجوی واژه‌های هزینه‌نگاری در شهرهای مختلف کشور نیز نتایجی هم‌راستا با فرضیه عمومی شدن جرم در فضای سایبر به دست می‌دهد. با استفاده از سامانه گوگل‌ترندز این مقایسه صورت گرفت و مشخص شد که جست‌وجوی این دسته از واژه‌ها در شهرهای کوچک ایران بیش از شهرهای بزرگ مثل تهران است.<sup>۲</sup> این موضوع نیز به‌وضوح از پیامدهای نامطلوب انتشار گسترده ابزارهای فیلترشکن در میان کاربران ایرانی که در نتیجه فیلترینگ فراگیر رخ داده است پرده‌برداری می‌کند.

از دیگر نتایج منفی پالایش فضای سایبر به شیوه جاری، بسترسازی برای بزهکاری و بزه‌دیدگی نوجوانان است. با فیلترینگ گسترده به‌ویژه فیلترینگ شبکه‌های اجتماعی، والدین و بزرگسالان و افراد سالم و محتاط فضای سایبر از استفاده و بهره‌برداری از فضاهای سایبر محروم می‌شوند و با خالی شدن مکان‌های فیلترشده از این دسته از کاربران، نوجوانان یا بومی‌های سایبری<sup>۳</sup> بدون نظارت والدین و کنترل اجتماعی کاربران دیگر با سهولت و سرعت بیشتری به محیط‌های ناسالم وارد می‌شوند. همچنین، عوامل سن و جنسیت از حیث تأثیر در میزان بزه‌دیدگی ادغام شده‌اند و بیشتر بزه‌دیدگان سایبری در جرایم منافی عفت را دختران نوجوان تشکیل داده‌اند.<sup>۴</sup> «در شیوه‌های جدید بزه سایبری، در بیشتر موارد پسران نوجوانی که در خلوت خود و از طریق شبکه‌های اجتماعی و سراهای گفت‌وگو شیطنت‌های نوجوانی را به فضای مجازی منتقل کرده‌اند، دختران کم‌سن‌وسالی را که با وجود زندگی در کنار پدر و مادر و اطرافیان خود، به‌علت حضورنداشتن آن‌ها در این فضا، کاملاً رها شده و بی‌خانمان‌اند، به‌آسانی به‌عنوان آماج جرم انتخاب می‌کنند» (حاجی‌ده‌آبادی و سلیمی، ۱۳۹۸، ص ۴۵).

۱. برای مشاهده جزئیات بیشتر به وبگاه پلیس فتا به آدرس ذیل مراجعه کنید: <https://www.cyberpolice.ir/node/142098#no-back>

۲. برای اطلاعات بیشتر در این زمینه ر.ک:

<https://www.google.com/trends/explore#q=%D&geo=IR%B%AD%9DA%A%B%https://www.google.com/trends/explore#q=%D>

۳. منظور از بومی‌های سایبری یا دیجیتال نیتیوها (Digital Natives) جوانان و نوجوانانی هستند که در آغاز هزاره سوم و در عصر شکوفایی فناوری اطلاعات و ارتباطات دوران رشد و تکوین شخصیت را گذرانده‌اند و فضای سایبر برای ایشان زیستگاه اول شناخته می‌شود؛ چه آن‌که این افراد بیشتر ساعات خود را در فضاهای مجازی می‌گذرانند و از آن مهم‌تر، فرایند اجتماعی شدن یا جامعه‌پذیری را در این محیط تجربه کرده‌اند.

۴. موضوعی که مانع از به تصویر کشیده شدن وخامت بحران جرم سایبری در همه کشورها و به‌ویژه در ایران است، رقم سیاه این جرایم-یعنی جرایمی که به هر دلیلی کشف نمی‌شوند- است که این ارقام در جرایم علیه زنان به علل مختلف به‌مراتب بیشتر از جرایم علیه مردان است. (هالدر و جایشانکار، ۱۳۹۳، ص ۲۲)

#### ۴. بایسته‌های الگوی جایگزین فیلترینگ در ایران

انتظار کارایی و کاهش میزان جرم از پالایش محتوا به شیوه جاری، به علت غیرعادلانه و غیرعلمی بودن آن، معقول نیست؛ زیرا از یک سو فایده‌مندی پیشگیری در گرو تنظیم دقیق آن و ابتنا بر رهیافت‌های دانش‌بنیان است و از سوی دیگر تمکین شهروندان به الزامات ناشی از برنامه پیشگیرانه در گرو احترام به حقوق آنان است. آمار و ارقام و داده‌های تجربی مختلف هم - آن‌گونه که گذشت - نشان از ناکارآمدی و حتی نتایج معکوس شیوه رایج پیشگیری از جرم دارد. از این رو، طراحی الگوی جایگزین برای پالایش محتوا در فضای مجازی ضروری به نظر می‌رسد. الگویی که هم به بایدها و نبایدهای حقوق بشری و هم به مسائل فنی - ساختاری و جرم‌شناختی فضای سایبر توجه داشته باشد. هر چند ارائه الگویی جامع کاری تفصیلی و فراتر از حوصله این مقاله است. اما در این مجال برخی بایسته‌های مبنایی الگوی پیشنهادی، یعنی «حق‌مدار و ایجابی‌بودن»، و برخی شاخص‌های عملیاتی و اجرایی آن، یعنی «جامعوی و ریزومی‌بودن»، مطرح می‌شود.<sup>۱</sup>

##### ۴-۱. بایسته‌های مبنایی

پایبندی برنامه پیشگیری از جرم به مبانی خاص و از پیش مشخص عادلانه‌بودن پیشگیری را تضمین می‌کند و مانع از انحراف تدابیر پیشگیرانه می‌شود. تعیین‌نشدن مبانی مشخص موجب می‌شود کاربست یک تدبیر، با نقض غرض اولیه، رفته‌رفته ضررهایی بیش از جرم بر جامعه تحمیل کند. «حق‌محوربودن» در معنای مخالف تکلیف‌مداربودن و «ایجابی‌بودن» در معنای مقابل سلبی و منفی‌بودن تدبیر پیشگیرانه را می‌شود دو بایسته مبنایی برای الگوی پیشگیری عادلانه در نظر گرفت.

##### ۴-۱-۱. حق‌محوربودن تدابیر

دخالت شهروندان در پیشگیری از جرم باید در راستای «حق مشارکت فرهنگی» به خود جامعه عمل بپوشاند. در منشور حقوق شهروندی به این حق شهروندان در مواد ۹۵ تا ۱۰۳ پرداخته شده است. در مواد ۹۹ و ۱۰۳، حق مذکور با کیفیت زیر شناسایی شده است.

ماده ۹۹: «شهروندان حق دارند از امکانات لازم برای مشارکت در حیات فرهنگی خود و همراهی با دیگر شهروندان ... با رعایت قوانین برخوردار باشند.»

ماده ۱۰۳: «حق همه شهروندان است که ضمن برخورداری از مشارکت و حضور در فضاها و مراکز عمومی، تشکیل‌ها و سازمان‌های اجتماعی، فرهنگی و هنری مخصوص خود را تشکیل دهند.»

به موجب این حق، شهروندان می‌توانند به همان اندازه که از فرهنگ جامعه پیرامون تأثیر می‌پذیرند بر آن تأثیر بگذارند و نمی‌توان بی‌علت یک شهروند را از بافتن تاروپود فرهنگی جامعه کنار گذاشت. برخلاف راهبرد تکلیف‌مدار جاری که حقوق و آزادی‌های شهروندان را یک‌سویه و دستوری قربانی امنیتی می‌کند که مدعی دستیابی به آن است، باید به دنبال اجرایی‌سازی ساختن برنامه‌های پیشگیری در الگویی حق‌مدار بود؛ زیرا تأمین و تقویت حقوق بنیادین شهروندان در بلندمدت خود بهترین راه‌حل مبارزه با جرم خواهد بود (ابراهیمی و رجیبی، ۱۳۸۹، ص ۸۵). بنابراین اگر پیشگیری از جرم در فضای سایبر با رعایت حقوق و آزادی‌های فردی و مبتنی بر حق‌ها و نه تکالیف شهروندان ابتنا یابد، پیشگیری پایدار از جرم محقق می‌شود. به این ترتیب، برخلاف شیوه جاری که تکلیف به ارائه‌نکردن محتوا برای کاربران فعال و تکلیف به دسترسی‌نداشتن برای کاربران منفعل می‌کند، باید با حمایت‌هایی از قبیل عرضه پهنای باند ارزان‌قیمت برای فعالان فرهنگی، معافیت‌های مالیاتی بر کسب‌وکارهای

۱. لازم به ذکر است، حق‌مدار بودن و ایجابی بودن تدابیر پیشگیرانه موضوعی است که در اصل در راستای تأمین معیار عدالت یا عادلانه شدن پیشگیری است اما از آن جهت که همسو با رهیافت‌های دانش جرم‌شناسی و سیاست جنایی مشارکتی نیز می‌باشد با معیار دوم پیشگیری یعنی علمی یا دانش‌بنیان بودن ارتباط جالب توجهی برقرار می‌کند. هم‌چنین جامعوی و ریزومی بودن پیشگیری رهیافتی است که برآمده از رهیافت‌های دانش جرم‌شناسی است اما اگر ورود جامعه به بحث پیشگیری به مثابه حق جامعه قلمداد شود می‌توان در راستای عادلانه شدن پیشگیری به آن نگریست.

سالم و تدابیر مشابه دیگر حق کاربران فعال برای ارائه محتوا یا کسب وکار شناسایی شود و به جای حذف ابزار یا خدمات، مانند یک پیام‌رسان، با فراهم کردن انتخاب گزینه‌های مختلف در هر مورد، ضمن ایجاد رقابت سالم بین کاربران فعال، حق انتخاب بهترین خدمات را برای کاربران منفعل به رسمیت شناخت.

#### ۴-۱-۲. ایجابی بودن تدابیر

برخلاف برنامه رایج پیشگیری در فضای سایبر، یعنی پالایش محتوا که راهبردی سلبی است و از طریق حذف محتوا به دنبال سالم‌سازی فضای مجازی است، «سیاست‌های مبتنی بر تولید محتوای سالم در فضای مجازی یا دیجیتال‌سازی یا دیجیتالی کردن محتواهای فرهنگی غیردیجیتال» (عاملی، ۱۳۹۰، ص ۳۶۵) راهبرد دیگری است که به صورت ایجابی همان هدف را دنبال می‌کند و با تأثیرگذاری عمیق و بلندمدت در ذائقه کاربران، برخلاف پالایش محتوا که جنبه تسکینی و موقت دارد، به صورت بنیادین با پدیده جرم مقابله می‌کند و پیشگیری پایدار از جرم را محقق می‌سازد. همچنین، در دستور کار قراردادن برنامه‌های آموزشی - آگاهی‌ساز از دیگر راهبردها است، زیرا آموزش و آگاهی‌بخشی به عموم شهروندان فضای مجازی و ارتقای سواد امنیتی رسانه‌ای دانش‌آموزان برای حفاظت ایشان از بزه‌دیدگی راهبردی ایجابی است که تأثیر بسزایی در پیشگیری از جرایم سایبری ایفا دارد. در پژوهش‌های متعددی<sup>۱</sup> اثربخشی برنامه‌های آموزشی - آگاهی‌ساز گزارش شده است. برای نمونه، ارزیابی برنامه آموزشی - آگاهی‌ساز با عنوان «طرح اقدام مثبت از راه آموزش فراگیر» که در مدارس آمریکا صورت گرفته است، حکایت از «هوشیاری دانش‌آموزان و کاهش شدید بزه‌دیدگی در مدارس داشت» (گانفردسون، ۱۳۹۴، ص ۹۷۱). در برخی کشورهای همسایه نیز برنامه‌هایی از این سنخ در حال اجرا است. برای نمونه، «در کشور ترکیه، اداره فناوری اطلاعات و ارتباطات<sup>۲</sup> پروژه‌ای را با همکاری وزارت آموزش و پرورش ملی به منظور آموزش معلمان در خصوص استفاده ایمن‌تر از اینترنت انجام داده است. بر این اساس، بیش از یک‌صد هزار آموزگار در بازه زمانی ۲۰۱۳ تا ۲۰۱۶ در این برنامه آموزش دیده‌اند. همچنین، در این کشور محتوای درسی با عنوان «دستورالعمل‌های جلوگیری از اذیت سایبری در محیط مدرسه» به دانش‌آموزان آموخته می‌شود» (احمدی مقدم، ۱۳۹۶، ص ۱۰۰). هرچند گزارشی از نتایج این برنامه در دست نیست، با توجه به نتایج ارزیابی برنامه‌های مشابه در مجموع می‌وان به چنین برنامه‌هایی امید بست.

#### ۴-۲. شاخص‌های اجرایی

التزام برنامه به مبانی صحیح کافی نیست. برنامه پیشگیری ممکن است در اجرا دچار اشکال شود و این موضوع، یعنی روش اجرای برنامه پیشگیری از جرم، به شدت در کارآمدی و اثربخشی آن تأثیر می‌گذارد. «جامعوی بودن» در مفهوم مقابل دولتی بودن و «ریزومی بودن» در مفهوم مقابل عمودی و متمرکز بودن دو شاخص اجرایی الگوی پیشگیری اثربخش در فضای سایبر است.

#### ۴-۲-۱. جامعوی بودن تدابیر پیشگیرانه

در جهت کاربست پیشگیری جامعوی، نه تنها باید از پالایش فضاهایی که امکان بهره‌برداری مثبت از آن‌ها وجود دارد مانند شبکه‌های اجتماعی خودداری شود، بلکه باید به دعوت عموم مردم و به ویژه افراد شریف جامعه از قبیل قضات، اعضای هیئت علمی، فرهنگیان، دعوت‌گران دینی و والدین به این فضاها پرداخت. حضور این افراد، علاوه بر این که برای دسته‌ای از بزهکاران غیرحرفه‌ای به ویژه نوجوان «احساس شرم»<sup>۳</sup> یا

۱. نتایج برخی از این پژوهش‌ها در دانشنامه بزه‌دیده‌شناسی و پیشگیری از جرم ذیل مدخل‌های «خبرنامه‌های جرم»، «بزه‌دیده‌شناسی و پیشگیری از جرم در کتاب‌های مصور» و «از بزه دور شویم» قابل مشاهده است.

2. ICTA

۳. احساس شرم در دانش جرم‌شناسی بازتاب فراوانی داشته است. تا آنجا که این احساس در نظر برخی صاحب‌نظران (Braithwaite, 1989) به عنوان مبنای روان‌شناختی برای استقرار عدالت ترمیمی به کار گرفته شده است. برخی پژوهشگران داخلی نیز به کارکرد شرم در پیشگیری از تکرار جرم یعنی مرحله سوم پیشگیری پرداخته‌اند (غلامی، ۱۳۸۸). آنچه در این نوشتار از احساس شرم برمی‌آید پیشگیری از جرم در مرحله اول آن است.

انصراف از جرم را فراهم می‌کند، مقدمه‌ای برای تفویض نقش‌های فعالانه در راستای پیشگیری از جرم خواهد شد و با نقش‌آفرینی و فعالیت این‌دسته از کاربران هنجارهای مبتنی بر اخلاق در فضای سایبر تکوین می‌یابد یا تقویت می‌شود. حتی در زمینه فیلترینگ می‌شود با کاستن از اختیار نهادهای دولتی و تفویض دست‌کم بخشی از مسئولیت به شهروندان فضای سایبر یا برخی از کاربران شریف فضای سایبر، ضمن اتخاذ رویکردی سنجیده و ملایم در برابر مسئله، به جامعه در جایگاه بزه‌دیده نگریست و به یکی از نیازهای جامعه از عدالت یعنی «داشتن فرصتی برای ایجاد احساس جمعی، مسئولیت‌پذیری و پاسخ‌گویی متقابل» (زهر، ۱۳۸۸، ص ۵۰) توجه نمود. این موضوع به برقراری تعادل بین میزان کنترلی که بر شهروندان اعمال می‌شود و میزان کنترلی که آن‌ها اعمال می‌کنند می‌انجامد و مطابق با نظریه تراز کنترل میزان درگیر شدن افراد در فعالیت‌های مجرمانه را کاهش می‌دهد. برای نمونه، در بسیاری از فضاهای تعاملی محیط سایبر، مانند شبکه‌های اجتماعی و تالارهای گفت‌وگو (چت‌روم‌ها) و مکان‌های بازی و سرگرمی، گزینه‌های فراوانی زیر عنوان تنظیمات حریم خصوصی، گزارش‌دهی جرم، مسدودسازی مزاحم، ابزارهای امنیتی و... وجود دارد که کاربران فضای سایبر می‌توانند با اعمال آن‌ها، علاوه بر این‌که زمینه بزه‌دیدگی خود را کاملاً از بین ببرند، به سالم‌سازی محیط سایبر و اخراج بزه‌کاران و آلوده‌کنندگان فضای سایبر بپردازند. افزایش چنین تمهیداتی و از آن مهم‌تر آگاهی‌بخشی به کاربران فضای سایبر برای استفاده از این ابزارها بزهکاری در فضای سایبر را کاهش چشمگیر خواهد داد.

#### ۲-۲-۴. ریزومی بودن تدابیر پیشگیرانه

ساختار غیرمتمرکز، سیال، متکثر، نامکان و افقی فضای سایبر نوع راهبردها و طریقه اجرای آن‌ها را شدیداً تحت تأثیر قرار می‌دهد. در محیط سایبر، نظام «حکمرانی عمودی و سلسله‌مراتبی» که دولت را در رأس هرم و شهروندان را در کف هرم قرار می‌دهد مطلوب و متبوع شهروندان نیست. در این فضا، نقش شهروندان از «مشارکت مدنی» به «مدیریت مدنی» در حال گذار است. این ساختار منحصر به فرد ریزومی شدن جرم را بیش از هر فضای دیگری پدیدار ساخته است.<sup>۱</sup> با ریزومی شدن بزهکاری در فضای سایبر، پیشگیری از جرم هم ناگزیر باید ریزومی دنبال شود.

در الگوی پیشگیری ریزومی، جامعه مدنی و بخش خصوصی در تراز حاکمیت قرار می‌گیرند، با دولت تصمیم می‌گیرند، با دولت اجرا می‌کنند و بر دولت نظارت می‌کنند. در واقع، پیشگیری ریزومی از جرم به معنای پیشگیری غیرمتمرکز، افقی، متکثر و زنجیره‌ای است و در مقابل پیشگیری عمودی و یک‌جانبه دولت قرار دارد. این نوع از پیشگیری به راحتی در فضای سایبر قابلیت اعمال و اجرا دارد؛ برای نمونه، خدمات‌دهندگان، اعم از خدمات دسترسی یا خدمات میزبانی، می‌توانند با عرضه رایگان ابزارهای ضد بدافزار (ویروس و کرم‌های رایانه‌ای) گام بزرگی در راستای پیشگیری از جرم بردارند. ترویج و انتشار ابزارهای فیلترینگ خانگی را می‌شود به منزله تدبیر پیشگیرانه ریزومی دیگری در دستور کار قرار داد. آن‌گاه که خانواده‌ها ابزارهای فیلترینگ خانگی را اعمال می‌سازند، در مقایسه با فیلترینگ متمرکز دولتی، علاوه بر این‌که امکان مصرف محتواهای ناسالم توسط فرزندان کاهش بیشتری دارد، خطر بزهکاری و بزه‌دیدگی نوجوانان نیز کاسته می‌شود.

#### نتیجه‌گیری

پیشگیری از جرم با ابزار پالایش محتوا یا فیلترینگ به شیوه جاری در ایران نه عادلانه است و نه با آموزه‌های علمی هم‌خوانی دارد. دلیل ناعادلانه بودن این شیوه از پیشگیری نقض گسترده «حقوق بنیادین» افراد یعنی حق آزادی و حق امنیت و حق برابری است؛ استفاده گسترده و پر شمار از فیلترینگ به منزله «ابزار سانسور» و «ضمانت اجرای دریافت نکردن مجوز» موجب خدشه به حق آزادی شهروندان شده است. علاوه بر حق آزادی، حق امنیت از آن‌رو مورد خدشه قرار گرفته است که فیلترینگ به جای پالایش محتوای مجرمانه یا ناسالم به مسدودسازی یا بلوکه کردن دسترسی به کل فضای مورد نظر می‌پردازد. از این‌رو، در بسیاری از موارد مانند وبگاه‌ها که میزان داخلی دارند، «تخریب یا اتلاف تمامیت داده‌ها

۱. ریزومی شدن جرایم مفهومی ضدتمرکز است که متضمن گسترش سیال و متکثر، و نامکانی و زنجیره‌ای شدن جرایم در جامعه است (دارابی، ۱۳۹۵، ص ۱۹۹).

یا اطلاعات» رخ داده است و در مواردی نظیر شبکه‌های اجتماعی که فضاهای فیلترشده در خارج از کشور میزبانی می‌شده‌اند و همچنان پس از فیلترینگ به فعالیت خود ادامه می‌دهند، «دشواری دسترسی به اطلاعات» رخ داده است. اما غیرعلمی بودن پالایش محتوا در فضای سایبر را می‌شود در مخالفت آن با رهیافت‌های دانش جرم‌شناسی یافت. از حیث نظری، بر مبنای نظریه تراز کنترل، اگر افراد جامعه به میزانی که کنترل می‌شوند قدرت کنترل نداشته باشند به بزهکاری متمایل می‌شوند. همچنین، بر مبنای نظریه انتقال فضا، میزان بزهکاری سایبری در جوامع بسته به جوامع آزاد است؛ بنابراین «کنترل شدید» بر شهروندان فضای سایبر نه تنها به پیشگیری از جرم نمی‌انجامد، ممکن است در جهت افزایش رقم بزهکاری عمل کند. برآیند عملی پالایش محتوا در ایران هم نشان می‌دهد که پالایش محتوا تبعات و آثار نامطلوبی در پی داشته است؛ «نافرمانی مدنی»، «عمومی شدن جرم» و «افزایش بزهکاری و بزه‌دیدگی نوجوانان» بخشی از این نتایج نامطلوب است که آمار و ارقام رسمی و غیررسمی تحقق آن‌ها را اثبات کرده است.

بنابر آنچه گفته شد، تجدیدنظر در سیاست‌ها و طراحی الگوی جایگزین پیشگیری از جرم در فضای سایبر گریزناپذیر است؛ الگوی پیشگیرانه‌ای که عادلانه و درعین حال مبتنی بر رهیافت‌های علمی باشد. البته باید تأکید داشت که این به معنای کنار گذاشتن کامل پالایش محتوا نیست، بلکه همان‌طور که پیش‌تر گفته شد و مطابق با تجربه برخی کشورها، در این الگو به پالایش حداقلی محتوا و در موارد ضروری اکتفا شود. در الگوی نوین مقابله با بزه سایبری، در راستای عادلانه‌شدن پیشگیری از بزهکاری ضروری است به پیشگیری از جرم به مثابه حقی برای کاربران فضای سایبر نگریده شود و شهروندان رایاسپهر در احقاق حق خود در ساخت محتواها و سالم‌سازی فضای مجازی پشتیبانی شوند. پیشگیری علمی یا نظریه‌مند از جرم هم اقتضا می‌کند که سازوکارها و تدابیر اجرایی پیشگیری در فضای سایبر به صورت جامع‌وی و ریزومی تنظیم شود؛ به این معنا که پیشگیری از جرم در فضای سایبر توسط افراد، سازمان‌های مردم‌نهاد، خدمات‌دهندگان اینترنتی و به صورت غیر متمرکز و افقی و انتشار یافته دنبال شود.

## منابع

ابراهیمی، شهرام و رجیبی، ابراهیم (۱۳۸۹). پیشگیری در نظریه‌های جرم‌شناسی و گستره محدودیت‌های آن، فصلنامه علمی-پژوهشی آموزه‌های حقوق کیفری، بهار (۱۳)، ۱۵-۳۸.

احمدی مقدم، جواد (۱۳۹۶). پیشگیری از بزه دیدگی اطفال در خصوص جرائم اخلاقی در فضای مجازی با تأکید بر شبکه‌های اجتماعی. پایان‌نامه کارشناسی ارشد، دانشگاه عدالت.

اسماعیل‌پور، حامد و شریعت‌باقری، محمدجواد (۱۳۹۳). کاوش در مفهوم و جایگاه حق آزادی و امنیت شخصی. فصلنامه علمی حقوقی دادگستری، ۷۸(۸۶)، ۷-۳۳.

بارلو، جان پری (۱۹۹۶). اعلامیه استقلال فضای سایبر؛ <https://www.eff.org/cyberspace-independence>

بصیریان جهرمی، حسین و خانیکی، هادی (۱۳۹۳). سیاست‌گذاران ایرانی و سیاست‌گذاری رسانه‌های اجتماعی؛ چالش‌ها، الگوها و ارائه یک مدل پیشنهادی. برنامه‌ریزی رفاه و توسعه اجتماعی، ۲۱، ص ۲۵-۷۰.

خلیلی، مصطفی و جوادی آملی، عبدالله (۱۳۸۴). حق و تکلیف در اسلام. قم: انتشارات مؤسسه اسراء.

جلالی فراهانی، امیرحسین (۱۳۸۹). کنوانسیون جرایم سایبر و پروتکل الحاقی آن. تهران: انتشارات خرسندی.

جلیلی، میترا (۱۳۹۶). افزایش ۱۶۵۰ درصدی دانلود فیلترشکن «سایفون». روزنامه ایران؛

<http://www.magiran.com/npview.asp?ID=3691040>



حاجی‌ده‌آبادی، محمدعلی و سلیمی، احسان (۱۳۹۵). عمومی‌شدن جرم در فضای سایبر؛ از علت‌شناسی تا پاسخ‌دهی در پارادایم عدالت ترمیمی. دانش‌نامه عدالت ترمیمی؛ مجموعه مقاله‌های همایش بین‌المللی عدالت ترمیمی و پیشگیری از جرم. تهران: انتشارات میزان، ۳۰۳-۳۲۵.

حاجی‌ده‌آبادی، محمدعلی و سلیمی، احسان (۱۳۹۸). بزه‌کاری و بزه‌دیدگی بومی‌های اینترنت از علت‌شناسی تا پاسخ‌دهی در پارادایم ترمیمی، مطالعات حقوق کیفری و جرم‌شناسی، ۴۹(۱)، ۴۱-۶۳.

خرم‌آبادی، عبدالصمد (۱۳۸۷). پنج میلیون سایت ایرانی در کشور فیلتر شده است. خبرگزاری مهر؛ [mehrnews.com/news/784979](http://mehrnews.com/news/784979).  
دارابی، شهرداد (۱۳۹۵). ریزومیک‌شدن پیشگیری از جرم در پرتو ریزومیک‌شدن ارتکاب جرم. آموزه‌های حقوق کیفری، ۲(۲) ۱۹۹-۲۱۸.  
رضایی، مهدی و بابازاده مقدم، حامد (۱۳۹۳). اصول تدوین قوانین و مقررات برای اینترنت با تأکید بر مصوبات یونسکو و شورای اروپا. پژوهش حقوق عمومی، ۱۵(۴۲)، ۴۳-۸۲.

زارعیان، داود و واحد، فائزه (۱۳۹۹). بررسی حقوقی رگولاتوری‌های حمایت از داده. رسانه، ۳۱(۱) ۴۷-۷۱.  
زهر، هوار (۱۳۸۸). کتاب کوچک عدالت ترمیمی. حسین غلامی (مترجم). تهران: انتشارات مجلد، چاپ دوم.  
سعد، علی (۱۳۹۴). درآمدی بر سیاست‌های فیلترینگ سایت‌های اینترنتی. مطالعات رسانه‌های نوین، ۸(۲)، ۱۴۱-۱۶۵.  
سواری، حسن و پورحسن، شکوفه (۱۳۹۲). تقابل سازوکارهای پیشگیری از جرائم سازمان‌یافته با موازین حقوق بشری. پژوهش‌های حقوق تطبیقی، ۱۷(۳)، ۶۹-۹۰.

عالی‌پور، حسن (۱۳۹۰). حقوق کیفری فناوری اطلاعات (جرایم رایانه‌ای). تهران: انتشارات خرسندی.  
عاملی، سید سعیدرضا (۱۳۹۰). رویکرد دو فضایی به آسیب‌ها، جرایم، قوانین و سیاست‌های فضای مجازی. تهران: انتشارات امیرکبیر.  
علیزاده، عبدالرضا و کاویانی، محمدهادی (۱۳۹۰). حق امنیت فردی در قانون اساسی جمهوری اسلامی ایران. مطالعات حقوق خصوصی، ۴۱(۴)، ۲۵۷-۲۷۲.

غلامی، حسین (۱۳۸۸). شرم و پیشگیری از تکرار جرم، مطالعات پیشگیری از جرم نیروی انتظامی، ۴(۱۰)، ۵۱-۸۵.  
فرجیها، محمد (۱۳۸۸). پیشگیری نظریه‌مند از جرم. مجموعه مقالات همایش ملی علمی-کاربردی پیشگیری از وقوع جرم قوه قضائیه، جلد دوم، تهران: انتشارات میزان، چاپ دوم.

فضلی، مهدی (۱۳۸۹). مسئولیت کیفری در فضای سایبر. تهران: انتشارات خرسندی، چاپ اول.  
قربان‌نیا، ناصر (۱۳۹۲). حقوق طبیعی و حقوق بشر. دوفصلنامه بین‌المللی حقوق بشر، ۸(۱)، ۴۱-۵۸.  
گانتفردسون، دنیس (۱۳۹۴). طرح اقدام مثبت از راه آموزش فراگیر. شادی عظیم‌زاده (مترجم). دانشنامه بزه‌دیده‌شناسی و پیشگیری از جرم. جلد دوم. تهران: انتشارات میزان، ۹۶۹-۹۷۱.

مرکز ملی افکار سنجی دانشجویان ایران (ایسپا). (۱۳۹۵). «از هر ۱۰ ایرانی ۶ نفر در شبکه‌های اجتماعی مجازی عضو هستند»؛ <http://www.ispa.ir/Default/Details/fa/1662> (۱۷ آذر ۱۳۹۸)

نجفی ابرندآبادی، علی حسین (۱۳۹۰). پیشگیری عادلانه از جرم. علوم جنایی: مجموعه مقالات تجلیل از استاد دکتر محمد آشوری، تهران: انتشارات سمت، ۵۵۹-۵۹۹.

نجفی ابرندآبادی، علی حسین و رضوانی، سودابه (۱۳۹۴). سلب آزادی پیشگیری محور با تأکید بر ماده ۱۵۰ قانون مجازات اسلامی ۱۳۹۰. پژوهش حقوق کیفری، ۴(۱۲)، ۹-۴۲.

هادیان فر، کمال (۱۳۹۷). چند نفر در ایران از فیلترشکن استفاده می‌کنند؟، خبرگزاری ایسنا، [isna.ir/xd3PqM](http://isna.ir/xd3PqM).

- هالدر، دباراتی و جایشانکار، کی (۱۳۹۳). جرم رایانه‌ای و بزهدیدگی زنان؛ قانون‌ها، حق‌ها و مقره‌ها. مهرداد رایجیان اصلی، حسین محمد کوره‌پز، احسان سلیمی (مترجمان). تهران: انتشارات مجد.
- Aryan, S., Aryan, H., & Halderman, J. A. (2013). Internet censorship in Iran: A first look. In *3rd USENIX Workshop on Free and Open Communications on the Internet (FOCI 13)*.
- Braithwaite, J. (1989). *Crime, shame and reintegration*. Cambridge University Press.
- Jaishankar K., (2008). Space Transition Theory of Cyber Crimes. In Schmallager, F., & Pittaro, M. (Eds.), *Crimes of the Internet* (pp.283-301). Upper Saddle River, NJ: Prentice Hall.
- Jones, A. (26 July 2010). Pentagon Papers II? On WikiLeaks and the First Amendment. *The Wall Street Journal* (blog). Archived from the original on 11 May 2013. Retrieved 6 December 2010.
- Tittle, R. (1995) *Control Balance: Toward a General Theory of Deviance*. Westview Press, Inc Boulder, CO 80301, United States of America
- Tittle, C. R. (2010). Control balance theory and social policy. *Criminology and public policy: Putting theory to work*, 6-24.
- Wenar, L. (2005). The Nature of Rights. *Philosophy and Public Affairs*, 33(3), 223-252.