




Filtering the cyberspace as a crime or a way for its prevention?

Leala Pornajafi¹
Hossein Fakhr^{2*}
Babak Pourghahramani³

Abstract

Almost all governments, whether libertarian or authoritarian, resort to filtering in order to prevent crime in the cyberspace due to political, cultural, etc. considerations but often due to technical and criminological limitations and inappropriate filtering, not only are they not successful in achieving their goal, but also violate fundamental human rights such as the right to freedom of expression and information and the right to privacy. Therefore, this article, examines whether filtering is a crime prevention way or as a crime itself. This article concludes in a descriptive-analytical approach that if governments are satisfied to the legality of filtering and disregard for conditions such as the necessity and appropriateness in filtering it has led to their excessive interference in the fundamental human rights of citizens and the damages caused by such filtering can be raised by the use of critical criminology teachings with the approach of social pathology in the form of state crime.

Keywords: *Filtering, Cyberspace, situational prevention, fundamental rights, state crime*

1. Introduction

Filtering is the first option of some governments to prevent cybercrimes. They intend to achieve this goal by disconnecting unauthorized content or making the crime more difficult, but because of the inefficiency of filtering techniques and easy access to anti-filters, they do not succeed. In addition, prevention of crime is a pretext in the hands of authoritarian systems to prevent the free flow of information in the community, the revelation of organized corruption news, and

1. Assistant Professor of Criminal Law and Criminology, Bonab Branch, Islamic Azad University, Bonab, Iran.

*2. Associate Professor of Tabriz University. Law Department. Tabriz, Iran. (Corresponding Author: h-fakhr@tabrizu.ac.ir)

3. Associate Professor of Criminal Law and Criminology, Maragheh Islamic Azad University, Maragheh, Iran.

the co-operation of public opinion. In this paper, first, filtering functions are examined as one of the crime prevention measures. Then, with regard to the filtering's consequences on human rights, the necessity of examining excessive filtering as a state crime is considered as critical criminology with the approach of social pathology and finally, according to human rights documents, it is recommended that their use can prevent violations of fundamental human rights in filtering.

2. Methodology

The methodology of this article is descriptive-analytical approach which has accomplished research on various literatures in criminal sciences.

3. Results and discussion

The expansion of cyberspace in the last two decades has had a profound impact on communication development, information exchange and increased business. It also provides an easy, complex and cheekbones for new effects of delinquency and some governments have to filtering cyberspace in the hope of difficulty making access to crime target, controlling access and reducing tools, motivations and crime revenues. But regardless of the inefficiencies of this type of prevention, excessive filtering without distinguishing between permissible and unauthorized content and sometimes even obstruction of cyberspace and social networks claiming to support ethical values and public security, into a means of repression of totalitarian systems. According to the authors, in terms of violations of privacy, media freedom and free intelligence, this situation provides the basis for the growth of government corruption and is a state crime against the fundamental rights of citizens.

4. Conclusion

Cyberspace filtering must be subject to principles such as loss, legality, and necessity, and pursue legal goals such as maintaining public order and security, protecting the moral health of the community and preventing crime. Therefore, extensive and unnecessary filtering, but also blocking citizens' access to cyberspace and social networks as a tool of totalitarian systems to prevent free flow of information, a clear case of government crime and Article 570 of the Islamic Penal Code (Book Fifth: Ta'zir and preventive Punishments).

5. Selection of References

Article 19, (2016), "Freedom of expression unfiltered: How blocking and filtering affect free speech", London, **Article 19**, pp.1-26. last visited : 3/12/2019, Available at: [www. Article 19.org](http://www.Article19.org).

- Banday,M.Tariq & Shah,N.A (2010), “A concise study of web filtering”,**Sprouts:Working paper on information systems**,10(31),pp.1-11.
- Breindl,Yana & Theiner,Patric & Busch,Andreas (2015), “Internet blocking regulation :a comparative analysis of 21 liberal democracies”, presented at the u4 cluster conference:Governance of a contemporary multilateral institutional architecture,**.of political science**,pp.1-42.
- Callanan,Cormac & Gercke,Marco & DeMarco,Estelle & Ziekenheiner,Hein (2009), “Internet blocking balancing cybercrime responses in democratic societies”, **Open society Institute**, Action internet solutions.
- Jaishankar, Karupannan (2008), “ Space transition theory of cyber crimes,in book: crime of the internet,chapter: space Transition Theory of cybercrime”, Editores: Frank, Schmallegger, Michael, Pittaro, Publisher pearson
- OpenNet Initiative (2004), “ A Starting point: legal implication of internet filtering”, **OpenNet Initiative**, pp.1-17, .last visited: 12/7/2019,Available at: www.opennetinitiative.org.
- Reyns, Bradford & Henson, Billy (2013), “security in digital world: understanding and preventing cybercrime victimization”, Switzerland **.Security Journal**, 26(4), pp 311-314.
- Vicks, Mery E (2013), “An examination of internet filtering and safety policy trends and issues in south Carolina,s K-12, ” public schools, Nova Southeastern University (NSU).
- Zittrain, Jonathan & L,John & G, Palfrey Jr (2007), “Access denied:the practice and policy of Global internet filtering”, Oxford ,**Oxford internet institute research report**,no. 14, pp.1-30.

Citation:

Pornajafi, L,Fakhr, H., Pourghahramani, B. (2022 & 2023), “Filtering the cyberspace as a crime or a way for its prevention?”, **Criminal Law Research**, 13(26), pp. 163-187.
DOI:10.22124/jol.2022.20840.2214

Copyright:

Copyright for this article is retained by the author(s), with first publication rights granted to *Criminal Law Research*. This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution License (<https://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided that the original work is properly cited.



پرتال جامع علوم انسانی

پالایش فضای سایبری به مثابه جرم یا ابزار پیشگیری از آن؟

لیلا پور نجفی^۱

حسین فخر^۲

بابک پورقهرمانی^۳

چکیده

تقریباً همه دولت‌ها بنا به ملاحظات مختلف در راستای پیشگیری از جرم در فضای مجازی، به پالایش متوسل می‌شوند. ولی اغلب، از یک طرف به دلیل محدودیت‌های فنی و جرم‌شناختی و از طرف دیگر به علت اجرای غیراصولی پالایش، در وصول به هدف خود موفق نشده بلکه برخی حقوق بنیادین بشری را نیز نقض می‌نمایند. در این تحقیق این‌که آیا پالایش ابزار پیشگیری از جرم است یا به مثابه خود جرم بررسی شده است. مقاله با شیوه تحلیلی-توصیفی به این نتیجه دست یافته که اکتفای دولت‌ها به قانونی بودن پالایش و عدم توجه به شرایطی چون «ضرورت و تناسب» در اعمال آن، موجب مداخله بی‌رویه آن‌ها در حقوق بنیادین شهروندان شده و آسیب‌های ناشی از پالایش غیراصولی به رغم متصف نشدن به‌عنوان مجرمانه در قوانین داخلی، می‌تواند با بهره‌مندی از آموزه‌های جرم‌شناسی انتقادی با رویکرد آسیب اجتماعی‌شناسی، در قالب جرم دولتی مطرح گردد.

واژگان کلیدی: پالایش، فضای سایبری، پیشگیری وضعی، حقوق بنیادین، جرم دولتی

✉ h-fakhr@tabrizu.ac.ir

۱. استادیار حقوق کیفری و جرم‌شناسی، دانشگاه آزاد اسلامی واحد بناب، بناب، ایران.

۲. دانشیار گروه حقوق دانشگاه تبریز، تبریز، ایران. (نویسنده مسئول)

۳. دانشیار حقوق کیفری و جرم‌شناسی، دانشگاه آزاد اسلامی واحد مراغه، مراغه، ایران

مقدمه

رسانه‌ها گاه به دلیل برداشت نادرست مخاطبین از محتواهای آن‌ها و گاه به علت ترویج جرم، ممکن است به ایجاد فرهنگ بزهکارانه کمک کنند. در این میان تأثیر اینترنت به دلیل گستره نفوذ و ارتباط دوسویه آن با مخاطبان، چشمگیرتر است. شبکه جهانی اینترنت به دلیل معرفی الگوهای فکری مختلف، در جهت‌دهی باورهای مردم تأثیری انکارناپذیری داشته و از یکسو با ترویج الگوهای مجرمانه و از سوی دیگر به «علت تعارض فرهنگی ناشی از تضاد هنجارهای فضای فیزیکی با هنجارهای فضای سایبری» (Jaishankar, 2008: 13) «ابزارهای کارآمدتری جهت ارتکاب جرایم در اختیار مجرمان بالقوه قرار می‌دهد» (Reyns & Henson, 2013: 311). فضای سایبری علاوه بر اینکه ابزاری برای ارتکاب جرایم سنتی همچون سرقت و کلاهبرداری یا آموزش این جرایم است، فضایی برای «جرایم سایبری محض» (نجفی ابرندآبادی، ۱۳۹۵ الف: ۱۱) نظیر هک کردن و انتشار بدافزارهاست که از جمله جرایم نوظهور بوده و صرفاً در فضای سایبری و علیه داده‌های موجود در آن محقق می‌شوند. جرایم سایبری به معنای اعم کلمه جرایمی هستند که بعضاً با استفاده از داده‌ها یا سامانه‌های رایانه‌ای محقق می‌شوند و بعضاً هم علیه آن سامانه‌ها یا داده‌ها ارتکاب می‌یابند و وقوع این جرایم رهاورد پیدایش فضای سایبری است.

یکی از اقدامات پیشگیرانه دولت‌ها جهت مقابله با جرایم فضای سایبری اعمال پالایش است. آنها تصور می‌کنند پالایش با افزایش تلاش لازم برای ارتکاب جرم، در روند ارتکاب آن اختلال ایجاد می‌نماید، ولی به علت نقص فنون پالایش، «حتی پیشرفته‌ترین کشورها در زمینه علوم رایانه‌ای، نمی‌توانند اطلاعاتی را که کاربران قصد انتشار یا دسترسی به آن را دارند، پوشش دهند» (Zittrain & et al, 2007: 7) و کاربران معمولاً با عبور از فیلتر به محتوای پالایش شده دسترسی پیدا می‌کنند و در نتیجه دولت‌ها از رسیدن به هدف خود در پیشگیری از جرم ناکام می‌مانند. ناکارآمدی پالایش در وصول به هدف خود ناشی از عدم رعایت اصل ضرورت در اعمال پالایش است.

مطابق بند ۲ ماده ۲۹ اعلامیه جهانی حقوق بشر و ماده ۱۹ میثاق بین‌المللی حقوق مدنی و سیاسی و برخی دیگر از اسناد حقوق بشری اعم از جهانی یا منطقه‌ای، دولت‌ها در تحمیل هرگونه محدودیت بر حقوق اساسی شهروندان، ملزم به رعایت اصولی از جمله اصل قانون‌مندی، اصل هدف مشروع و اصل ضرورت هستند و از آنجا که پالایش فضای مجازی، محدودیت‌هایی بر حقوق بنیادین، همچون آزادی بیان و اطلاعات، حریم خصوصی مراسلات و حریم خصوصی داده‌های شخصی ایجاد می‌کند، برای انطباق با حقوق بشر باید از اصول مذکور تبعیت نماید. عدم رعایت اصول مورد نظر در اعمال پالایش، علاوه بر اینکه ممکن است تبعات جرم‌شناختی چون ناکارآمدی پالایش و در

نتیجه جابجایی جرم را به دنبال داشته باشد، موجب لطمه اساسی به حقوق بنیادین یاد شده می‌شود.

پالایش گسترده و بی‌رویه، که عمدتاً در رژیم‌های اقتدارگرا اعمال می‌گردد، نقض حقوق مذکور را به دنبال خواهد داشت. این مداخلات و لطمات ناشی از آن، با وجود عدم تصریح در قوانین جزایی، به دلیل این که «محصول سازمان‌دهی اجتماعی ناشی از ارتباطات متعارض قدرت هستند» (ون هام، ۱۳۹۵: ۹۹۴) نسبت به اعمالی که جرم‌انگاری شده‌اند، تبعات زیانبارتری دارند. بنابراین، پرسش اصلی تحقیق این است که مهم‌ترین چالش فراروی دولت‌ها در زمینه پالایش فضای سایبری در حوزه حقوق بنیادین شهروندان چیست؟ آیا با بهره‌گیری از آموزه‌های جرم‌شناسی انتقادی، نقض ساختارمند حقوق بشر به واسطه پالایش غیراصولی را می‌توان جرم دولتی تلقی نمود؟

«منظور از پالایش فضای مجازی جلوگیری از دسترسی به برخی صفحات وب، گروه‌های خبری و... است که از نظر هیئت حاکمه، متضمن محتوای مجرمانه یا غیرقانونی باشد.» (پورنجفی قوشچی، فخر، پورقهرمانی، ۱۳۹۹: ۳۷) و جرم دولتی رفتار سازمان‌یافته هیئت حاکمه یک کشور در جهت نقض حقوق بشر یا حقوق بین‌الملل بشردوستانه است که در قالب «مخاطرات طبیعی، تروریسم حکومتی، جرایم جنگی، نسل‌کشی، فساد و...» ارتکاب می‌یابد.

در این مقاله ابتدا کارکردهای پالایش به‌عنوان یکی از تدابیر پیشگیری از وقوع جرم بررسی می‌گردد. در ادامه توجه به تبعات حقوق بشری پالایش، ما را به ضرورت بررسی پالایش غیراصولی به‌عنوان جرم دولتی، آن‌گونه که در جرم‌شناسی انتقادی با رویکرد آسیب اجتماعی‌شناختی مطرح شده است، رهنمون خواهد ساخت و در نهایت، با عنایت به اسناد حقوق بشری مندرج در فوق، اصولی پیشنهاد خواهد شد که به‌کارگیری آنها در اعمال پالایش، خواهد توانست از نقض حقوق بنیادین جلوگیری نماید.

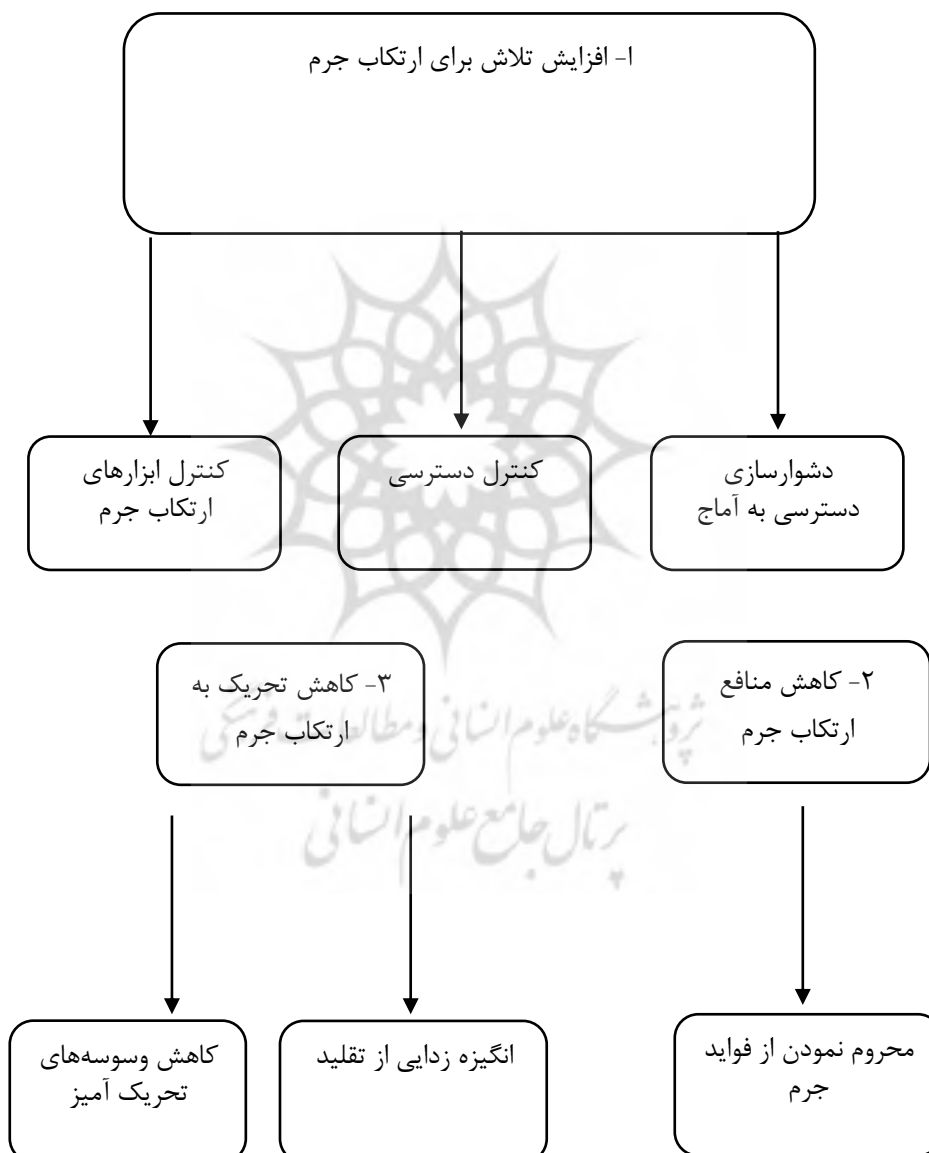
۱. پالایش به مثابه ابزار پیشگیری وضعی از جرم

امروزه جرایم سایبری و بزهکاران فعال در حوزه فناوری اطلاعات، علاوه بر امنیت ملی کشورها، امنیت جامعه جهانی را نیز در معرض تهدید جدی قرار داده‌اند. (نجفی ابرندآبادی، ۱۳۹۵ ب: ۲۶ و ۲۵) از این رو دولت‌ها سعی دارند «با بهره‌مندی از فن‌آوری‌های نوین که به موازات ریزومیک شدن جرایم معرفی می‌شوند، تهدیدات پدیده‌های نوظهور را خنثی سازند.» (دارابی، ۱۳۹۵: ۲۰۹). در این راستا جهت مبارزه با جرایم فضای مجازی به اقدامات پیشگیرانه، از جمله اعمال پالایش متوسل می‌شوند و فرضشان بر این است که پالایش به علت قابلیت‌های چندگانه‌اش، می‌تواند

۱. ر.ک به: گرین، پنی، و تونی، وارد، «جرم حکومتی، دولت‌ها، خشونت و فساد»، ترجمه نبی اله غلامی.

به‌عنوان یک ابزار پیشگیرنده موقعیت‌مدار، بزهکاران بالقوه را از ارتکاب جرم منصرف نماید. برای پالایش کارکردهایی در راستای پیشگیری وضعی از جرم می‌توان شناسایی نمود که از جمله آن است:

- ۱- افزایش تلاش لازم برای ارتکاب جرم شامل: دشوارسازی دسترسی به آماج، کنترل دسترسی، کنترل ابزارهای ارتکاب جرم
- ۲- کاهش منافع ارتکاب جرم یا محروم نمودن از عواید جرم
- ۳- کاهش تحریک به ارتکاب جرم شامل: کاهش وسوسه‌های تحریک‌آمیز و انگیزه‌زدایی از تحریک (ابراهیمی، ۱۳۹۳: ۱۰۰-۱۰۱ و کلارک، آ.روی. جی، ۱۳۸۸: ۲۲۴-۲۴۷)



۱.۱. افزایش تلاش لازم برای ارتکاب جرم

ارتکاب جرم ارتباط مستقیمی با میزان تلاش لازم برای انجام آن دارد و هر قدر اقدامات بیشتری برای ارتکاب جرم لازم باشد، رغبت فرد به ارتکاب آن کمتر شده و مرحله گذر از اندیشه به فعل مجرمانه کمتر رخ می‌دهد. در نتیجه، افزایش تلاش لازم برای ارتکاب جرم، می‌تواند یکی از تدابیر پیشگیرانه وضعی قلمداد شود. «این تلاش می‌تواند از طریق سخت‌سازی آماج جرم، کنترل دسترسی به مکان‌ها و کنترل ابزارها و سلاح‌ها افزایش یابد» (خانعلی‌پور و اجارگاه، ۱۳۹۰: ۷۷). پالایش با داشتن قابلیت‌های فوق، چه بسا بتواند در افزایش تلاش لازم برای ارتکاب جرم مؤثر واقع شده و از وقوع جرم پیشگیری نماید.

به موجب تکنیک دشوارسازی، با دسترسی بیشتر به آماج، احتمال بزه‌دیدگی بیشتر خواهد شد. پس باید با ایجاد موانعی مثل نرده یا دیوار در فضای فیزیکی، دسترسی بزهکاران به آماج جرم را دشوارتر نمود. در فضای سایبری نیز می‌توان با ایجاد موانعی از جنس مجازی، از وقوع جرم جلوگیری نمود، بدین نحو که می‌توان «با نصب سامانه‌ها یا برنامه‌های خاص همچون پالایش بر روی گره‌های دسترسی به شبکه، اعم از رایانه‌های شخصی، مسیریاب‌ها، سامانه‌های ارائه‌دهنده خدمات شبکه‌ای و نیز ایجادکنندگان نقطه تماس بین‌المللی، از ورود یا ارسال برخی محتوای غیرمجاز یا غیرقانونی جلوگیری نمود» (آقاجانی، ۱۳۸۸: ۱۷۰). پالایش می‌تواند دسترسی به سیل‌های جرم را دشوار ساخته و از بزه‌دیدگی آنها جلوگیری نماید. به این واسطه کاربران در دسترسی به برخی محتواها که با لحاظ مؤلفه‌های فرهنگی، مذهبی، اخلاقی، سیاسی، اجتماعی و ... در هر کشور از جمله مصادیق مجرمانه شناخته شده، با مانع مواجه می‌گردند.

از دیگر شیوه‌های افزایش تلاش لازم برای ارتکاب جرم، کنترل دسترسی است. «در این روش همگان اجازه ورود به محدوده تعیین شده را نداشته و صرفاً گروه خاصی می‌توانند به اماکن مورد نظر وارد شوند. با استفاده از این تدبیر می‌توان از ورود افراد ناصالح جلوگیری کرده و از بزه‌دیدگی آماج احتمالی پیشگیری نمود. به عنوان نمونه، با گماشتن نگهبان، در ورودی اماکن حساس امنیتی، از ورود افراد ناصالح و سرقت اطلاعات جلوگیری می‌شود» (فرهادی‌آلاشتی، ۱۳۹۵: ۶۰). یا امروزه با استفاده از ابزارهای فنی نظیر کارت‌های هوشمند یا گذرواژه و به‌ویژه گذرواژه‌های زیست‌سنجی می‌توان از ورود افراد به اماکنی که مجوز ورود ندارند، پیشگیری نموده و در نتیجه از ارتکاب جرم توسط آنها جلوگیری نمود. پالایش قابلیت تطبیق با این کارکرد را نیز دارد چون با ایجاد محدودیت در دستیابی به برخی منابع اینترنتی، مانع از رویارویی مجرمین و قربانیان بالقوه می‌شود و در واقع با

1. Nodels
2. Routers

دور کردن بزه دیدگان بالقوه، از آنها در مقابل امواج بزهکاری در محیط سایبر حمایت می‌نماید. نمونه بارز این قابلیت، پالایش در سطح فردی (Bandy&Shah,2010:2) توسط والدین است که بر رایانه‌های خانگی اجرا و با فیلتر نمودن محتواهای غیرمجاز یا نامناسب برای کودکان و مسدود نمودن برخی از وب سایت‌های حاوی مطالب غیرقانونی و غیراخلاقی، از بزه‌دیدگی احتمالی فرزندان پیشگیری می‌شود.

کنترل ابزارهای ارتکاب جرم نیز یکی دیگر از شیوه‌های افزایش زحمات ارتکاب جرم است و آن تدابیری است که دسترسی به وسایل ارتکاب جرم را محدود می‌نماید. البته به دلیل تفاوت ابزارهای ارتکاب جرم در فضای مجازی نسبت به فضای مادی، روش‌های کنترل ابزار جرم نیز متفاوت خواهد بود. «یکی از این ابزارها در فضای سایبر، بدافزارهایی چون ویروس‌ها^۱، کرم‌ها^۲ و... می‌باشد. با این ابزارها می‌توان از فضای سایبر سوءاستفاده‌های زیادی نمود؛ از سرقت رمز عبور قربانی جرم گرفته تا تخریب سامانه‌های رایانه‌ای» (نادرخانی، ۱۳۹۰: ۴۰). این بدافزارها از طریق سایت‌ها، سامانه‌های اینترنتی و... امکان نشر پیدا می‌کنند. بدیهی است با اتخاذ تدابیر امنیتی مناسب ناظر بر پیشگیری از توزیع بدافزارها، عرصه بر بزهکاران با انگیزه این حیطة تنگ خواهد شد. مسدود نمودن وبسایت‌های توزیع کننده این بدافزارها از جمله تدابیر مورد نظر است که دسترسی بزهکاران به ابزارهای جرم را کنترل می‌نماید.

البته به دلیل وجود ترفندهای متنوع در نشر بدافزارها، پالایش فقط می‌تواند بخش کوچکی از آنها را محدود نماید و عمده بدافزارها از آن جهت که در قالب برنامه‌های مجاز نفوذ می‌نمایند، تدابیر دیگری جهت کنترل می‌طلبند. درواقع، پالایش نیز همچون دیگر تدابیر پیشگیری وضعی، با ایراد جایابی جرم مواجه است چرا که با اعمال آن «ریشه اصلی جرم یا انگیزه ارتکاب آن از بین نرفته است» (صفاری، ۱۳۸۰: ۱۹۸) و مجرم با انگیزه و مضمم، می‌تواند برای دسترسی به محتوای ممنوعه و ارتکاب جرم، به دیگر قابلیت‌های فضای مجازی متوسل شود.

۱.۲. کاهش منافع ارتکاب جرم

بر اساس نظریه انتخاب عقلانی^۳، مجرم بالقوه شخصی حسابگر است و زمانی که تشخیص دهد منافع احتمالی جرم بر مضرات آن غلبه خواهد کرد، مرتکب جرم می‌شود. بدیهی است «این سودها فقط مادی نیستند چرا که معمولاً در جرایم، موضوع‌های دیگری همچون سوءاستفاده‌های جنسی، هیجان، انتقام و نظیر اینها هم مطرح می‌شود» (کلارک، ۱۳۸۸: ۲۳۵). پس، یکی از شیوه‌های

1. Virus
2. Worm
3. Rational option

پیشگیری از ارتکاب جرم، پی بردن به منافع ناشی از جرم و محروم نمودن مرتکب از آن منافع است. این روش امکان استفاده از عواید ناشی از جرم را منتفی می‌سازد. «براساس این روش، حتی اگر بزهکار بتواند مرتکب جرم شود، قادر به استفاده از عواید آن و تبدیل کالای مورد نظر خود نخواهد بود» (فرهادی‌آلاشتی، همان: ۸۴). شاید بتوان پالایش سایت‌های قمار برخط، انجمن‌های غیرقانونی و سایت‌های مرتبط با تجارت هرزه‌نگاری را از جمله مصادیق کارآیی این تدبیر در فضای مجازی قلمداد نمود که می‌تواند به‌عنوان شیوه‌ای ناظر بر کاهش منافع جرم، از بزه‌دیدگی احتمالی کاربران جلوگیری نماید.

۱. ۳. کاهش تحریک به ارتکاب جرم

این شیوه بر تأثیر هیجان در ارتکاب جرم تأکید می‌کند و از آن جا که عوامل محرک، منشا بسیاری از جرایم در فضای مجازی می‌باشند پس حذف عوامل محرک هیجان در مجرمین بالقوه می‌تواند از تدابیر پیشگیرانه موقعیت‌مدار تلقی گردد. این کارآیی در پالایش از طریق کاهش تحریک هیجانی و جلوگیری از تقلید، به خصوص در مجرمان اتفاقی محقق می‌شود.

برخی از مجرمان از جمله مجرمان هیجانی «معمولاً برای ارتکاب جرم آمادگی قبلی ندارند، اما در پاره‌ای اوقات ممکن است تحت تأثیر حساسیت فطری و عصبی خود مرتکب جرم شوند» (صانعی، ۱۳۷۷: ۱۱). در واقع، قرار گرفتن در وضعیت‌های خاص و تحریک‌آمیز، موجب ارتکاب جرم توسط آنها می‌شود و چه بسا اگر عامل تحریک‌کننده نمی‌بود، مرتکب جرم نمی‌شدند. در فضای مجازی نیز نمی‌توان از تأثیر عوامل هیجان‌انگیز در تحقق جرم غافل شد. زیرا وجود برخی محتواها همچون محتواهای مربوط به هرزه‌نگاری و دسترسی اتفاقی یا حتی عمدی کاربران به آنها در ایجاد انگیزه ارتکاب برخی جرایم مؤثر واقع می‌شود. مثلاً دسترسی به تصاویر مربوط به هرزه‌نگاری کودکان، می‌تواند باعث شود حتی افرادی که منحرف جنسی نیستند به علت تعقیب مستمر چنین تصاویری، به ارتکاب رفتارها و خشونت‌های جنسی برخط علیه کودکان، رغبت پیدا کنند (Callanan & et al, 2009: 189). مسدودسازی محتوای مرتبط با هرزه‌نگاری و بالاحص هرزه‌نگاری کودکان به دلیل کاهش وسوسه‌های ارتکاب جرم، می‌تواند دلیل منطقی برای کنترل این ابزار در جهت تقلیل بزه‌دیدگی کودکان قلمداد گردد.

با پالایش تصاویر مستهجن تبلیغی که در تجارت‌های مرتبط با هرزه‌نگاری به منظور تهییج کاربران جهت ورود به سایت‌های غیرقانونی و فروش محصولات آنان مورد استفاده قرار می‌گیرد، هم می‌توان از طریق کاهش تحریک به ارتکاب جرم و هم با کاهش منافع ارتکاب آن، از وقوع جرم جلوگیری نمود.

وانگهی به علت وجود ارتباطات بدون مرز در اینترنت، گروه‌های مجرمانه می‌توانند با افراد زیادی در نقاط مختلف جهان ارتباط برقرار کرده و الگوهای مجرمانه خود را ارائه دهند و کاربران در اثر معاشرت با این گروه‌ها، فنون و انگیزه‌های ارتکاب جرم را آموخته و تقلید می‌نمایند. پس، همان‌گونه که در فضای فیزیکی «زدودن فوری علایم جرم مثل پاک کردن دیوارنویسی، تقلید ارتکاب جرم از ناحیه دیگران را کاهش می‌دهد» (پاک‌نهاد، ۱۳۹۴: ۲۵۹)، پالایش صفحات مجرمانه و غیرقابل دسترس نمودن محتویاتی که به آموزش جرایمی نظیر کلاهبرداری، ساخت مواد منفجره، هک کردن و... در فضای مجازی می‌پردازند، نیز می‌تواند به‌عنوان مانعی در جهت تقلید از جرم در این فضا متجلی شود.

در نهایت می‌توان گفت با آن‌که دولت‌ها و حتی «دموکراسی‌های آزادی‌خواه به منظور پیشگیری از جرم در فضای مجازی، اعمال فنون پیچیده پالایش را جهت محدود نمودن دسترسی به اینترنت انکار نمی‌کنند» (Breindl&etal,2015:3) ولی به دلیل ایرادات پالایش، چندان نمی‌توانند در تحقق اهداف خود موفق شوند، تا جایی که حتی گاه عدم اعمال این تدبیر به علت ناکارآمدی آن، باصرفه‌تر به نظر می‌رسد. «چرا که به‌کارگیری فن‌آوری‌های جدید اطلاعات و ارتباطات هم، آثار موقت و مسکنی از نظر کاهش وقوع جرم دارد» (نجفی ابرندآبادی، ۱۳۸۸: ۷۴۹). وقتی مجرم به دلیل اعمال فن‌آوری‌هایی چون پالایش، از دسترسی به محتوای مجرمانه و ارتکاب جرم به شیوه خاص منع می‌گردد، از اسلوب دیگری برای رسیدن به هدف خود استفاده می‌کند. جابجایی شیوه ارتکاب جرم در فضای مجازی در مقایسه با فضای فیزیکی به شکل آسان‌تر و سریع‌تر اتفاق می‌افتد و استدلال کسانی که معتقدند «اگر جابجایی هم رخ دهد باز به علت تأخیر در ارتکاب جرم، می‌توان پیشگیری را موفق دانست» (صفاری، همان: ۲۱۲) شاید در خصوص فضای مجازی چندان قابل دفاع نباشد. پس، دشوارسازی آماج جرم از طریق پالایش، دست‌کم در مجرمان قاصد مؤثر واقع نمی‌شود. زیرا، آنان بلافاصله از طریق نصب فیلترشکن، از پالایشگرها عبور کرده^۱ و با بهره‌مندی از وبسایت‌های فیلترنشده دیگر، فیلترها را دور زده و به محتوای مجرمانه دسترسی پیدا می‌کنند.

باری، در هیچ کشوری شیوه‌های پالایش بی‌نقص نیست. «حتی با تجربه‌ترین کشورها در این زمینه، به سختی می‌توانند از طریق پالایش اطلاعاتی را که کاربران قصد انتشار یا دسترسی دارند، پوشش دهند» (Zittrain&etal,opcit:7). در واقع، اکثر شیوه‌های پالایش حداقل با یک یا چند روش قابل دور زدن هستند.^۲ از این رو، کاربران قاصد معمولاً با عبور از آن، به محتوای فیلترشده دسترسی پیدا می‌کنند و پالایش فقط ممکن است از دسترسی تصادفی کاربران غیرقاصد جلوگیری

1. see: Tariq Banday (2010), «A concise study of web filtering».

2. see: Vicks, M., « An examination of internet filtering and safety policy trends and issues in south Carolina », s K-12 public schools.

نماید. با این حال، برخی دولت‌ها چنان بی‌رویه در این راستا می‌تازند که به دلیل نقض حقوق اساسی شهروندان، واکنش افکار عمومی و مجامع حقوق بشری را برمی‌انگیزند.

۲. پالایش به مثابه جرم

پالایش، گرچه می‌تواند پیشگیری از بزهکاری‌های احتمالی را تسهیل کند، ولی ممکن است برای برخی از مصادیق حقوق بشر تبعاتی داشته باشد. در حالی که آن حقوق بخش مهمی از ارزش‌هایی است که در اسناد مهم بین‌المللی و منطقه‌ای و قوانین اساسی کشورها مورد تأکید قرار گرفته است. آسیب‌های حقوق بشری پالایش ناشی از دو عامل است: ۱- عدم ارتقای فن‌آوری‌های مربوطه ۲- پالایش افراطی. نقص فنون پالایش یا عدم به‌روزرسانی آن ممکن است موجب پالایش بیش از حد شده و محتواهای مجاز را نیز شامل شود و در نتیجه «آزادی‌های مدنی به صورت غیر ضروری مورد مداخله قرار گیرد» (Open net initiative, 2004: 8) ولی چنین مداخلاتی بطور ناخواسته رخ داده و با روزآمد نمودن فن‌آوری‌های پالایش یا گزارش افراد ذینفع و در نتیجه تجدیدنظر متولیان امر در لیست سیاه مربوط به پالایش قابل رفع است.

آنچه به لحاظ حقوق بشری شایان اهمیت فراوانی است، پیامدهای منفی ناشی از پالایش افراطی است که عمدتاً توسط نظام‌های سیاسی اقتدارگرا و تحت پوشش تأمین نظم عمومی، امنیت ملی، پیشگیری از جرم و... انجام می‌پذیرد و به دلیل رویکرد سرسختانه دولت‌ها، هیچ‌گونه انعطافی را بر نمی‌تابد. چنین صدماتی از نگاه افکار عمومی و مجامع حقوق بشری پنهان نمی‌ماند و باب جدیدی در جرم‌شناسی مفتوح می‌نماید. بدین نحو که می‌توان از رهگذر جرم‌شناسی انتقادی با رویکرد آسیب اجتماعی‌شناختی به تحلیل آن پرداخته و آن را به‌عنوان یکی از مصادیق جرایم دولتی مطرح نمود.

۲.۱. پالایش افراطی: ناقض حقوق بنیادین

پالایش افراطی و بی‌رویه موجب می‌شود برخی از مصادیق «حقوق اساسی اشخاص، از جمله حق آزادی بیان» (Zittrain & et al, op.cit: 25)، «حق زندگی خصوصی و خانوادگی» (Callanan & et al, op.cit: 151) اعم از حریم خصوصی مراسلات و حریم داده‌های شخصی، با گسترش قدرت دولت در فضای سایبر در معرض تهدید و مداخله قرار بگیرد در حالی که این حقوق

1. Over-filtering
2. blacklist
3. state crimes

بر اساس قوانین داخلی کشورها و اسناد بین‌المللی، در ردیف مهم‌ترین حقوق و آزادی‌های بنیادین قرار می‌گیرند.

۱.۱.۲. حق زندگی خصوصی

حق احترام به زندگی خصوصی در اغلب اسناد حقوق بشری همچون ماده ۱۲ اعلامیه جهانی حقوق بشر، ماده ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی، ماده ۸ کنوانسیون اروپایی حقوق بشر و... به رسمیت شناخته شده است. در حمایت از این حق در فضای سایبر، به اسنادی نظیر «رهنموده‌هایی برای قانون‌گذاری فایل داده شخصی کامپیوتری» مصوب کمیسیون حقوق بشر سازمان ملل در سال ۱۹۸۹، دستورالعمل‌های مختلف پارلمان اروپا، ماده ۱۵ کنوانسیون جرایم سایبری و... اشاره نموده همگی بیانگر اتخاذ گام‌های اساسی در سطح بین‌المللی جهت حمایت از این حق در فضای سایبر هستند.

در این مبحث فقط آن بخش از زندگی خصوصی که ممکن است با پالایش تضعیف شود، بررسی می‌شود که عبارتند از: حریم خصوصی مراسلات و حریم خصوصی داده‌های شخصی. نظام تقنینی ایران نسبت به بسیاری از جنبه‌های حریم خصوصی حساسیت ویژه داشته و علاوه بر قانون اساسی (اصول ۲۲ و ۲۵) در قوانین عادی هم به آن تأکید کرده است. ولی متأسفانه در جهت حمایت‌های قانونی از این جنبه‌های حریم خصوصی، احتمالاً به دلیل نوظهور بودن آن، همچنان با خلاء مواجه است و تمسک به اصول قانون اساسی جمهوری اسلامی ایران که در بهترین حالت از مبتدیاتی چون مسکن، نامه و... حمایت می‌کند، نمی‌تواند به نیازهای مبتلابه فضای مجازی در این خصوص پاسخ دهد. البته برخی مواد منشور حقوق شهروندی به ابعاد تازه حریم خصوصی تصریح نموده است. این منشور با آنکه اعتبار قانون مصوب مجلس را ندارد و الزام‌آور نیست ولی از جهت جلب توجه به ابعاد نوین حریم خصوصی، می‌تواند همچون چراغی فراروی قانون‌گذار باشد.

۱.۱.۱.۲. حریم خصوصی مراسلات

«مراسلات»^۲ و از جمله آن ارتباطات اینترنتی به عنوان یکی از مصادیق حق زندگی خصوصی است که در اسناد پیش گفته بر محرمانه بودن آن تصریح شده است. در ماده ۳۷ منشور حقوق شهروندی لزوم احترام به گونه‌های جدید این حق، از جمله نامه‌های الکترونیکی، ارتباطات اینترنتی و... نیز مورد تأکید قرار گرفته است.

۱. ر.ک. به: مقدمه حقوق سایبراز سیامک قاجارقیونلو.

پالایش ممکن است موجب تضعیف حق مزبور شود. زیرا متولیان پالایش به منظور کشف و در نتیجه فیلتر نمودن محتواهای غیرقانونی و مجرمانه، که عمدتاً با هدف پیشگیری از جرم انجام می‌پذیرد، محتواهای تبادل شده بین کاربران و به‌ویژه کاربرانی را که در مظان اتهام جرم قرار دارند، تحت نظر گرفته و بدون اجازه کاربران، آن داده‌ها را جمع‌آوری و بعضاً ذخیره‌سازی می‌نمایند و با این اقدام خود، حق محرمانگی مراسلات اینترنتی را مخدوش می‌کنند. در این خصوص دادگاه اروپایی حقوق بشر در رای «جمع‌آوری و ذخیره‌سازی اطلاعات شخصی مرتبط با برنامه‌های تلفن فرد یا ایمیل‌های او و نیز ذخیره‌سازی استفاده شخص از اینترنت بدون علم وی را، دخالت در حق زندگی خصوصی و نیز حق مراسلات مندرج در ماده ۸ کنوانسیون اروپایی حقوق بشر دانسته است» (Ibid).

۲.۱.۱.۲. حریم خصوصی داده‌های شخصی

یکی دیگر از مصادیق حق زندگی خصوصی، که با توسعه ارتباطات بروز پیدا کرده، «حریم اطلاعات شخصی» است. امروزه سازمان‌های دولتی به منظور انجام امور و پیشبرد اهداف خود داده‌هایی از شهروندان در اختیار دارند و مکلف هستند به موجب اصول حمایت از داده‌ها،^۱ ضمن تأمین امنیت داده‌های مورد نظر، از افشای آن به دیگران خودداری نمایند. «هرگونه تخلفی از قواعد مزبور به منزله نقض حریم اطلاعات اشخاص تلقی خواهد شد» (پورقهرمانی و صابرنژاد، ۱۳۹۴: ۳۷). در صورتی که نهادهای دارنده اطلاعات شخصی، در ارتباط با تأمین امنیت آن اطلاعات با تکلیف قانونی مواجه نباشند، احتمال دارد از طریق این داده‌ها امکان نظارت بر فعالیت شهروندان در فضای مجازی را برای نهادهای حکومتی به منظور کشف محتواهای مجرمانه جهت فیلتر نمودن آن فراهم نمایند و حق مذکور را به خطر اندازند.

در خصوص اهمیت این حق نو ظهور باید ذکر شود علاوه بر این که اغلب کشورها سطوح متعارفی از اصول حمایت از داده‌ها را در قوانین داخلی خود برقرار می‌نمایند در سطح فراملی مقررات عمومی حفاظت از داده (GDPR)^۲ به ابتکار اتحادیه اروپا تدوین گشته است. پیش از آن ماده ۸ منشور حقوق اساسی اتحادیه اروپا و نیز «دستورالعمل‌های^۳ آن، دول عضو را به تضمین احترام به حق مزبور در قلمرو داخلی خود مکلف ساخته بود» (Callanan&etal, op.cit:152). در ایران نیز، برخی مواد منشور حقوق شهروندی (مواد ۳۵، ۳۸، ۳۷ و ۳۹) و قانون تجارت الکترونیکی (مواد ۵۸ و ۵۹) لزوم احترام به داده‌های شخصی را مورد تصریح قرار داده است. پس، می‌توان گفت توانمندسازی

1. Data protection

2. The Genral Data protection regulation

3. 2002/58/ec&95/46/ec

سیستم‌های حمایت ازداده، امروزه در جامعه دموکراتیک امری ضروری است و دولت‌ها ملزم هستند این مهم را ضمن پیش‌بینی در قوانین، در عملکرد خود نیز رعایت نمایند.

۲.۱.۲. آزادی بیان و اطلاعات

دراهمیت تضمین احترام به این حقوق علاوه بر ماده ۱۹ اعلامیه جهانی حقوق بشر، بند دوم ماده ۱۹ میثاق بین‌المللی حقوق مدنی و سیاسی، ماده ۱۰ کنوانسیون اروپایی حقوق بشر، می‌توان به اسناد خاص فضای سایبر، نظیر پاراگراف ۲۴ از بند ۳ «بیانیه اصول اجلاس عالی سران در خصوص جامعه اطلاعاتی»، پاراگراف چهارم «سندتعهدتونس» (حسین پور و صابر نژاد، ۱۳۹۴: ۹۳ و ۹۲) و مواد ۳ و ۴ «اعلامیه آفریقایی حقوق و آزادی‌های اینترنتی» اشاره نمود.^۱

تقریباً همه اسناد مربوط به حق آزادی بیان، به حق دریافت و ارسال اطلاعات نیز تأکید نموده است. به موجب این اسناد جستجو و دریافت اطلاعات، لازمه آزادی بیان است. طبق این اسناد، آزادی اطلاعات نه به‌عنوان حقی جداگانه، بلکه به‌عنوان رکن رکن حق آزادی بیان مطرح می‌شود که به موجب آن مردم «حق دسترسی به اطلاعات موجود در مؤسسات عمومی و آن دسته از مؤسسات خصوصی که خدمات عمومی ارائه می‌دهند» (انصاری، ۱۳۹۷: ۲۱) را دارند.

در این راستا «کمیته حقوق بشر سازمان ملل در سال ۲۰۱۱ حق آزادی بیان را برای تمامی اشکال بیان و نیز تمامی رسانه‌ها اعم از الکترونیکی و اینترنتی به رسمیت شناخته است.» (Article 19, 2016: 11) همچنین این امر در ماده ۲ اعلامیه آفریقایی حقوق و آزادی‌های اینترنتی مصوب ۲۰۱۳ با صراحت بیشتری تأکید شده است، با بیان اینکه: «دسترسی به اینترنت... جهت برخورداری از حقوق و آزادی‌ها از جمله آزادی بیان و اطلاعات ضروری است...» در نظام حقوقی داخلی حق آزادی بیان از اصل ۲۴ و ۲۷ و حق آزادی اطلاعات تلویحاً از اصول ۳، ۴ و ۸ قانون اساسی قابل استنباط است. علاوه بر آن، قانون مستقلی با عنوان «قانون انتشار و دسترسی آزاد به اطلاعات» در راستای به رسمیت شناختن حق اخیر تصویب شده که در ماده ۵، دسترسی به اطلاعات را حق همه مردم دانسته است. این حق موجب نظارت مستمر مردم بر عملکرد حاکمان می‌شود فلذا به‌عنوان «یکی از ابزارهای مهم شفاف‌سازی حکومت» (انصاری، همان: ۲۴) عمل کرده و ضمن جلوگیری حاکمان از فساد، آنها را به پاسخگویی وادار می‌کند.

تردید نیست بشرا روزی جهت ابراز آزادی بیان و اطلاعات، ناگزیر از دسترسی به اینترنت است و تحدید اینترنت و از جمله پالایش افراطی آن، به علت ایجاد محدودیت در دسترسی کاربران

1. Africa Declaration on internet Rights and Freedoms

به اطلاعات مؤسسات عمومی و در نتیجه منع آنان از نظارت مستمر بر عملکرد حاکمان، حق آزادی اطلاعات کلیه شهروندان را تضعیف کرده و حتی ممکن است نقض نماید.

کاربران فعالی که از فضای مجازی در راستای تولید محتوا بهره می‌برند، با اعمال پالایش، محدودیتی بیش از تضعیف حق آزادی اطلاعات متحمل می‌شوند. بدین معنا که پالایش علاوه بر اینکه می‌تواند محتواهای مورد درخواست آنان را مسدود کرده و باعث محرومیتشان از حق آزادی اطلاعات شود، همچنین ممکن است آنان را از ادامه فعالیت در تولید محتوا و در نتیجه حق آزادی بیان محروم نماید. زیرا در فضای مجازی علاوه بر تولید محتواهایی که مطلوب حکومت‌ها است، ممکن است محتواهایی نیز تولید شود که به دلیل داشتن نگاه منتقدانه نسبت به حکومت‌ها، به مذاق آنها خوش نمی‌آید، فلذا در اغلب موارد، حکومت‌ها و به خصوص نظام‌های اقتدارگرا سعی می‌کنند با جرم‌انگاری مبادله هرگونه مطالب مخالف با ساختار فکری خود، به توسعه قلمروی مصادیق مجرمانه و سرکوبی شهروندان معترض از طریق پالایش پرداخته و اقدام خود را با عناوینی چون تأمین نظم عمومی، پیشگیری از جرم و... توجیه نمایند. در چنین حکومت‌هایی ایدئولوژی در نظر گرفته شده تحکیم پایه‌های قدرت حاکم است. در این راستا حکومت، با مداخله در بیشتر حوزه‌های زندگی شهروندان، قلمروی آزادی آنان را به حداقل می‌رساند. ایجاد واهمه از فضای مجازی در شهروندان و توسل به «عوام‌گرایی به‌عنوان ابزار تفوق مردم‌سالاری صوری، عامل دیگری بر تهدید آزادی شهروندان در راستای امنیتی کردن فضاهای عمومی از راه گسترش حوزه‌های نظارت پیشگیرانه است» (احمدی و شمعی، ۱۳۹۵: ۴۴) نتیجه اتخاذ چنین رویکردی، پالایش افراطی و مداخله بیش از حد در حق آزادی بیان افراد خواهد بود. این در حالی است که امروزه در نظام‌های مردم‌سالار «سیاست جنایی ملهم از حقوق پیشگیری تحت تأثیر اسناد بین‌المللی کیفری و حقوق بشری، برای تأمین امنیت اجتماعی پایدار، رویکرد کرامت‌مدار پیدا کرده است» (نجفی ابرندآبادی، ۱۳۹۴ الف: ۱۰ و ۱۱) چرا که از نظر آنان محدودیت‌های ناشی از پیشگیری جز با شفافیت و دقت بودن دامنه آن، برخلاف حقوق بنیادین بشری خواهد بود.

۲.۲. پالایش: جرمی فراتر از قوانین ملی

پالایش بی‌رویه لطمه جدی به برخی حقوق اساسی شهروندان وارد می‌نماید. با این حال قوانین داخلی به جرم‌انگاری چنین رفتارهایی رغبت نشان نمی‌دهند زیرا هرگونه تعریف قانونی از چنین عملی، جرم‌انگاری اعمال هیئت حاکمه توسط خود آنها خواهد بود و طبیعی است که حکومت‌ها از پیش‌بینی این جرایم در قوانین خود استقبال ننمایند.

رویکردهای کلاسیک جرم‌شناسی نیز همسو با قانون‌گذاران داخلی، بر جرایم سنتی متمرکز شده و از توجه به اعمالی که به عناوین مجرمانه متصف نشده‌اند، غافل مانده‌اند و ایرادات جرم‌شناسان انتقادی به آنها، نیز از همین مسئله نشأت گرفته است. آنان بر این نظرند که جرم‌شناسان کلاسیک به نام اصل قانونی بودن جرم و مجازات، فقط به مطالعه آن دسته از رفتارهایی که در قانون جرم تلقی شده، پرداخته و از بررسی سایر پدیده‌های ضد انسانی خودداری کرده‌اند و با این رویکرد، «هیئت حاکمه را تحکیم نموده‌اند.» (نجفی ابرندآبادی، ۱۳۷۳ و ۱۳۷۴: ۲۱۳) حال آنکه در بیشتر موارد، این اعمال به دلیل اینکه «محصول سازماندهی اجتماعی ناشی از ارتباطات متعارض قدرت هستند» (ون هام، همان: ۱۹۹۴) آسیب‌زننده‌تر نیز می‌باشند.

اگر ما در بررسی پالایش، به نظر جرم‌شناسان کلاسیک اکتفا نماییم، به یقین از شناخت علل جرایم سایبری مصرح در قانون و ارائه راه‌هایی جهت اصلاح مجرمان این جرایم فراتر نخواهیم رفت و چه بسا استفاده از آخرین فن‌آوری‌های پالایش را جهت مقابله با این جرایم پیشنهاد نماییم بدون اینکه به آسیب‌های ناشی از پالایش که دامن‌گیر شهروندان اکثر جوامع است، نیم‌نگاهی بیندازیم. در واقع مداخلات بی‌رویه بر حقوق بنیادین شهروندان که نتیجه اجتناب‌ناپذیر پالایش بی‌رویه است، از دایره مطالعه ما خارج خواهد افتاد. در حالی که می‌توان با بهره‌گیری از داده‌های جرم‌شناسی انتقادی به‌ویژه رویکرد آسیب اجتماعی‌شناسی، چنین صدماتی را که نسبت به جرایم متعارف تبعات زیانبارتری دارند، به چالش کشید.

رویکرد آسیب اجتماعی‌شناسی، بازتاب دیدکلان جرم‌شناسی انتقادی در خصوص خطرات کنترل نشده‌ای چون جرایم علیه محیط زیست، آثار باستانی، حقوق بشر و... است. بر اساس این دیدگاه، «جرم یک مفهوم مضیق است و بر اساس معیارهای حاکمیت ایجاد می‌شود و اغلب دوشخص را به‌عنوان بزه‌کار و بزه دیده درگیر می‌کند، حال آنکه باید به آسیب‌ها و صدمات شدید اجتماعی پرداخت که مهم‌ترین ارزش‌های یک گروه اجتماعی یا یک ملت را خدشه‌دار کرده» (نجفی ابرندآبادی، ۱۳۹۰: ۱۰۲۷) و عمدتاً هم در قوانین جزایی منعکس نمی‌گردد. حجم عظیم این صدمات از جمله مداخلات حقوق بشری ناشی از پالایش افراطی، توسط صاحبان قدرت و هیئت حاکمه ایجاد می‌شود. ارتباط این آسیب‌ها با ساختار قدرت و عدم تصریح آن در قوانین کیفری، مانع از مطالعات جرم‌شناختی آن نخواهد بود بلکه «این دغدغه‌ها به طرقی بنیادین با موضوعات مطروحه در جرم‌شناسی فراملی تلاقی می‌یابند» (فردریش، ۱۳۹۶: ۹۰) و با بهره‌گیری از «استانداردهای حقوق بشری و آسیب‌های اجتماعی» (دکسردی، ۱۳۹۴: ۱۱۷) می‌توانند در قالب جرم دولتی مطرح گردند.

۳.۲. شناسایی پالایش افراطی به عنوان جرم دولتی

جرم دولتی به مفهوم «رفتار سازمان یافته هیئت حاکمه یک کشور در جهت نقض یا نادیده گرفتن حقوق شهروندان» (غلامی و عباسی، ۱۳۹۶: ۸۴) تعریف شده است. برخی نیز آن را «اقدامات غیرقانونی، ضداجتماعی و ظالمانه‌ای دانسته‌اند که به نفع دولت‌ها یا نهادهای دولتی و نه برای سود و نفع فردی (عوامل فردی دولت) ارتکاب می‌شوند.» (کوزلاریچ و دیگران، ۱۳۸۹: ۱۲۰) چنین تعاریفی در تلاشند «تا از اشکالات ایجاد شده توسط تعاریف حقوقی مضیق از جرم، که به حکومت‌ها اجازه تعریف جرایم را می‌دهد، اجتناب کرده» (گرین؛ وارد، ۱۳۹۸: ۹) و «جرم را با مفهوم گسترده‌تر «آسیب اجتماعی» برابر سازند.» (همان: ۲۹)

در پرداختن به جرایم دولتی توجه به مبانی توجیه‌کننده تشکیل دولت‌ها، در تحلیل این جرایم مفید فایده خواهد بود. از نظر طرفداران حقوق طبیعی، «انسان بر اساس خرد خویش به این امر پی می‌برد که برای حفظ و اجرای حقوق طبیعی خود اعم از حق زندگی، امنیت و آزادی، در قالب قرارداد اجتماعی حکومتی تأسیس کند.» (سبزه‌ای، ۱۳۸۶: ۹۲) بر اساس این قرارداد، هر فرد بخشی از آزادی خود را جهت تضمین حقوق مذکور به حکومت تفویض می‌کند. ولی چشم‌پوشی شهروندان از برخی حقوق خود در جهت تفویض آن به حکومت، به مفهوم واگذاری بی‌حد و حصر کلیه حقوق آنها به هیئت حاکمه نیست بلکه شرط لازم آن، عدم تعدی حکومت به آزادی‌های بنیادین آنها است. برای اینکه حکومت‌ها نتوانند از قرارداد اجتماعی شهروندان مبنی بر تفویض برخی اختیارات به آنها، به‌عنوان دستاویزی جهت تضییع حقوق بنیادین بهره‌جویند، عمدتاً بر اساس اصل قانونی بودن جرم و مجازات، حدود حقوق و گذارنده و ضمانت اجرای تخطی از آن، به صراحت مشخص می‌گردد. هر چند معمولاً ادعا می‌شود این اصل از یک‌تازی حکومت‌های خودکامه جلوگیری کرده و حقوق شهروندان را نیز به نحو بهتری تضمین می‌نماید ولی نظر به اینکه تصویب قوانین توسط هیئت حاکمه صورت می‌گیرد، در برخی از موارد، آنان با سوءاستفاده از اختیارات تفویض شده و نیز استفاده ابزاری از این اصل، حقوق شهروندان را به صورت ساختارمند نقض کرده و آسیب‌های جدی بدان وارد می‌سازند.

پالایش فضای سایبری نیز، گرچه با استفاده از اختیار قانون‌گذاری حکومت‌ها جهت پیشگیری از وقوع جرم یا تأمین امنیت، اعمال می‌شود ولی عمدتاً ابزار دست دولت‌های اقتدارگرا قرار می‌گیرد. به طوری که آنان تحت لوای پالایش به ظاهر قانونی و مشروع، حقوق و آزادی‌های اساسی پیش‌گفته را سلب می‌نمایند. در واقع اصلی که یکی از مبانی آن مقابله با تعرض حکومت‌ها بر حقوق شهروندان است، در راستای تعرض به حقوق اساسی همان شهروندان و در نتیجه ارتکاب جرم دولتی مورد سوءاستفاده قرار می‌گیرد. در حالی که «به منظور عادلانه شدن تدابیر پیشگیرنده، دولت‌ها باید

همان حقوق و آزادی‌های فردی‌ای را ملاحظه نمایند که هنگام پیشگیری کیفری رعایت می‌شوند.» (نجفی، ۱۳۹۴ ب: ۵۸۴) فلذا جهت تضمین حقوق بنیادین شهروندان، صرف قانونی بودن اقدامات دولت‌ها، کافی نخواهد بود بلکه هرگونه پیشروی نسبت به این حقوق، علاوه بر قانون‌مندی، باید «ازهدف مشروع برخوردار بوده و در یک جامعه دموکراتیک ضروری باشد.» (کوچ نژاد، ۱۳۸۳: ۱۶۹) از این رو پالایش نیز به‌عنوان یکی از روش‌های اعمال محدودیت برحقوق افراد، لاجرم باید از همان قواعد تبعیت نماید.

باری هرچند حکومت‌ها محتواهای مجرمانه قابل پالایش را، در قوانین خود پیش‌بینی می‌نمایند و در بیشتر موارد فقط به پالایش محتوای مجرمانه مقرر در قانون بسنده می‌نمایند ولی گاه به‌دلیل وضع قوانین جزایی تفسیربردار و گاه به جهت گشاده‌دستی در تعیین فهرست مصادیق مجرمانه توسط مقنن، از همان اصل قانونی بودن جرم و مجازات در راستای تضعیف حقوق بنیادین شهروندان و به‌ویژه سرکوبی مخالفین بهره‌برداری می‌کنند. تخطی مجریان قانون از اصول حاکم بر اعمال محدودیت برحقوق بنیادین، در تطبیق محتواها با فهرست مجرمانه‌ای که مقنن تصویب نموده است، عامل مضاعف دیگری در جهت تعرض به این حقوق می‌باشد. اتخاذ این رویکردها توسط هیئت حاکمه، ماحصلی جز پالایش غیراصولی نخواهد داشت و چنین پالایشی، بسته به نوع، میزان و قلمروی محتوای فیلترشده، حق آزادی بیان و اطلاعات و نیز برخی جنبه‌های حریم خصوصی را که از جمله حقوق بنیادین بشری هستند، نقض می‌نماید و از آنجا که «نقض حقوق بشر به‌عنوان هسته تعریف جرم [دولتی] در نظر گرفته می‌شود»، (روث؛ کازلاریچ، ۱۳۹۹: ۳۴) فلذا پالایش افراطی نیز از جهت تعرض به حقوق مذکور در فوق، می‌تواند به‌عنوان جرم دولتی قلمداد شود. در نظام جزایی کشورمان «تفویض مقام تقنین مبنی بر تعیین فهرست مصادیق مجرمانه به کارگر تعیین مصادیق مجرمانه (سلیمی، ۱۳۹۷: ۱۰۳)» در ماده ۷۵۰ قانون مجازات اسلامی - که فقط یکی از اعضای ۱۲ نفره آن کارگروه از نمایندگان مجلس است - و نیز واگذاری «اختیار تحکیم» (همان) به این مقام غیرقضایی مبنی بر تعیین مصادیق فوق، طبق ماده ۷۵۱ قانون مذکور، از عواملی است که می‌تواند به معضل مورد نظر دامن بزند.

پس می‌توان گفت آسیب‌های ناشی از پالایش افراطی هم منتسب به قانون‌گذاران است و هم متوجه عملکرد مجریان قانون. بدین شرح که، اگر قانون‌گذاران در وضع قوانینی که مجوز اعمال پالایش می‌باشد، اصل مداخله حداقلی را مبنا قرار ندهند، یا مجریان قانون در اجرای پالایش و تطبیق حکم باموضوع، به اصول «ضرورت و تناسب» که اسناد حقوق بشری جهت اعمال محدودیت برحقوق بنیادین پایبندی بدان را لازم دانسته، مقید نباشند، به جرم دولتی متهم خواهند شد.

با ملاحظه اصل ضرورت، مجریان قانون از میان تدابیر متعددی که می‌توانند اهداف مشروع مورد نظر مقنن را نمایند، باید تدبیری انتخاب نمایند که کمترین لطمه را به منافع و آزادی‌های خصوصی افراد وارد می‌کند. براین اساس، هرگونه محدودیت نسبت به حقوق بنیادین، باید متضمن دو شرط باشد: ۱- محدودیت مورد نظر در پاسخ به نیاز مهم جامعه اتخاذ شود. ۲- تدبیر اتخاذ شده با هدف خود تناسب داشته باشد. تردیدی نیست پالایش نیز به‌عنوان یکی از مصادیق محدودیت‌های تحمیل شده بر افراد، لاجرم باید از هر دو شرط پیش گفته تبعیت نماید.

به موجب شرط اول پالایش باید با توجه به اهداف مشروعی که در تعقیب آن است، کارایی کافی جهت پاسخ به نیاز جدی جامعه‌ای که در آن اجرا می‌شود، را داشته باشد. در این راستا باید مطالعات دقیقی انجام شود تا پس از روشن شدن ابهامات زیر از کارکرد پالایش اطمینان حاصل شود. بدین منظور باید بررسی شود عکس‌العمل افراد در مقابل پالایش محتوای مجرمانه چیست؟ آیا آنها فیلترها را دور نمی‌زنند یا از پروتکل‌های دیگری جهت تعقیب این محتواها استفاده نمی‌کنند؟ به عبارت دیگر نسبت تقریبی دسترسی به محتوای غیرقانونی از طریق سایت‌هایی که قرار است فیلتر شود، با میزان توزیع تقریبی آن از طریق دیگر سایت‌ها مقایسه گردد. در این بررسی‌ها، همچنین باید روشن شود محتواهای فیلتر شده بعد از چه مدت زمان و با چه کیفیتی ممکن است دوباره ظاهر شوند؟ چنانچه ماحصل این مطالعات بتواند اثبات نماید که پالایش می‌تواند به اهداف مشروع خود، از جمله پیشگیری از بزهکاری و بزه‌دیدگی کاربران که از مصادیق نیاز مبرم یک جامعه است دست یابد، در این صورت اجرای آن مفید بوده و متضمن الزام فوق مبنی بر پاسخ به نیاز اساسی جامعه خواهد بود.

جهت احراز «متناسب بودن» پالایش، باید دلایل کافی وجود داشته باشد مبنی بر این که منفعت خاصی در خطر است و حمایت از آن، مستلزم مداخله از طریق پالایش است. در واقع متولیان پالایش باید به این نتیجه برسند که دولت بر اساس برخی ضوابط همچون ضابطه ضرر، به مداخله در قلمرویی که در صدد اعمال پالایش است، مجاز می‌باشد. به علاوه آنها باید قبل از اعمال پالایش، منافع و مضرات ناشی از پالایش را ارزیابی کرده و جز به‌عنوان آخرین راه چاره، بدان متوسل نشوند. در این راستا باید میزان تأثیر پالایش بر حقوق و آزادی‌های بنیادین، روشن شده و محدودیت‌های تحمیل شده بر این حقوق، بتواند با حفظ منافع ناشی از آن جبران شود به طوری که ارزش منفعت مورد حمایت، نسبت به حق مورد مداخله بیشتر باشد و ارزیابی گردد که هیچ روش دیگری غیر از پالایش که مداخله کمتری در حقوق و آزادی‌های شهروندان داشته و برای رسیدن به هدف مورد نظر مطلوب‌تر بوده، وجود نداشته است.

دولت‌ها در صورتی که در اعمال پالایش، از شرایط فوق تخطی نمایند، ممکن است در مظان ارتکاب جرم دولتی قرار بگیرند. بدیهی است بزهکاران این جرم، حکومت و سازمان‌های حکومتی اعم از قانون‌گذاران و مجریان قانون می‌باشند که با ارتکاب چنین جرایمی «سیاست‌ها و اهداف نهادهای سیاسی را تعقیب می‌کنند.» (باراک، ۱۳۹۶: ۱۰۵) بزه دیدگان آن، شهروندانی هستند که به علت اتخاذ سیاست‌های خلاف قواعد حقوق بشر توسط دولت‌ها، متحمل صدمه در حقوق بنیادین خود شده‌اند. قوانینی که از آن تخطی می‌شود، «قوانین حقوق بین‌الملل، قوانین داخلی و اخلاقیات اجتماعی، به صورتی که توسط مخاطبان تفسیر شده‌اند، هستند. این مخاطبان شامل جامعه مدنی داخلی و بین‌المللی، حکومت‌های دیگر و آژانس‌های دیگر در داخل خود حکومت بزهکاری باشند» (گرین؛ وارد، پیشین: ۲۳) و ضمانت اجرای چنین جرمی «انتقاد یا شورش توسط خود مردم حکومت، آسیب رساندن به اعتبار داخلی و بین‌المللی حکومت و تحریم‌های نظامی و اقتصادی توسط سایر حکومت‌ها» (همان) است.

شایان ذکر است تلقی نمودن پالایش افراطی به عنوان جرم دولتی، از یک طرف به علت داشتن نگرشی کلان به موضوع و از طرف دیگر به جهت زیرسوال بردن اقدامات هیئت حاکمه و مصون ندانستن آنها از عواقب اعمال زیانبارشان، ساختار شکنی مثبت قلمداد شده و باعث می‌شود موضوعاتی همچون نقض حقوق بشر، به عرصه جرم‌شناسی راه پیدا نماید. همچنین، از حیث پرداختن به «پدیده مجرمانه» که دایره شمول عامتری نسبت به جرایم داخلی دارد، واجد اهمیت فراوانی است. گرچه عواملی چون اصل حاکمیت ملی، مانع از اعمال مجازات‌های مصطلح، بر دولت‌های مجرم شده و نیز باعث می‌شود «جرم‌شناسی جرایم دولتی، همواره بر جرایم ارتكابی در گذشته متمرکز شود» (قورچی بیگی، ۱۳۹۵: ۳۱۹) ولی این امر، نه تنها فرصت‌هایی را که از رهگذر مکتب آسیب اجتماعی‌شناسی در جهت مفهوم‌شناسی جرایم حقوق بشری دولت‌ها، عاید جرم‌شناسی شده است، سلب نمی‌کند بلکه راه را جهت ارائه نظریه‌های علت شناختی موضوع و در نتیجه بروز شاخه‌های تخصصی جرم‌شناسی در آینده، هموار می‌سازد.

نتیجه‌گیری

امروزه دولت‌ها جهت پیشگیری از جرایم فضای مجازی، به پالایش آن روی می‌آورند. این اقدام به علت داشتن برخی قابلیت‌ها، می‌تواند به عنوان یک تدبیر فنی پیشگیری وضعی از جرم ایفای نقش نماید. ولی همچون دیگر تدابیر پیشگیرنده موقعیت‌مدار با ایراداتی مواجه است. یکی از آن ایرادات به صورت جابجایی شیوه ارتکاب جرم خودنمایی می‌کند. در واقع زمانی که مجرم به دلیل پالایش، از دسترسی به محتوای مجرمانه یا ارتکاب جرم به شیوه خاص منع می‌گردد، جهت رسیدن به

اهداف خود، از اسلوب دیگری استفاده خواهد نمود. پس پالایش، دست کم در مجرمان قاصد مؤثر واقع نمی‌شود. زیرا آنان بلافاصله از طریق نصب ضد پالایش، از پالایشگرها عبور می‌کنند. می‌توان گفت این مشکل ناشی از ایرادی است که بیشتر جنبه فنی دارد، در واقع عدم ارتقای فن‌آوری‌های مربوط به پالایش از یک سو و مجهز بودن مرتکبین به آخرین دستاوردهای علمی از سوی دیگر، یکی از عوامل ناکارآمدی پالایش در پیشگیری از وقوع جرم است.

وانگهی ضعف پالایش در تحت پوشش قرار دادن تمام مصادیق مجرمانه (پالایش کمتر از حد)، عامل دیگری در این راستاست. چون موجب می‌شود مجرمین از طریق پروتکل‌های فیلتر نشده دیگر به محتوای مجرمانه دست یابند. تبعات پالایش بیش از حد، به مراتب از موارد اخیر بیشتر است، زیرا محتواهای مجاز را نیز در بر گرفته و در نتیجه موجب مداخله غیر ضروری در آزادی‌های مدنی نظیر حق آزادی بیان می‌شود. با این حال چنین مداخلاتی به‌طور ناخواسته رخ می‌دهد و چه بسا با ارتقای فنون پالایش رفع گردد.

مهم‌ترین آسیب‌هایی که با پالایش رخ می‌نماید، تعرض عمدی دولت‌ها به حقوق بنیادین، از طریق پالایش غیر اصولی است، بدین نحو که برخی دولت‌ها عمداً با توسعه دامنه مصادیق مجرمانه از طریق پالایش افراطی و صرفاً با استناد به اصل «قانون‌مندی»، حقوق بنیادین شهروندان را نقض می‌کنند. بدیهی است چنانچه اقدام به پالایش بدون رعایت مؤلفه‌های لازم، به صورت بی‌رویه و فقط با تکیه بر قانون وضع شده توسط هیئت حاکمه اعمال گردد، حقوق بنیادینی چون حریم خصوصی مراسلات، حریم داده‌های شخصی و حق آزادی بیان و اطلاعات را مخدوش خواهد ساخت. بدین نحو که از یک طرف با فراهم ساختن امکان زیر نظر گرفتن فعالیت‌های شهروندان در فضای مجازی و در نتیجه ضبط و نگهداری برخی محتواهای مبادله شده توسط آنها، حریم خصوصی مراسلات و داده‌های شخصی کاربران را تضعیف خواهد نمود. از طرف دیگر با ایجاد ممنوعیت در دسترسی کاربران به برخی اطلاعات برخط و یا با جلوگیری از امکان تبادل و انتشار چنین محتواهایی در اینترنت، حق آزادی بیان و اطلاعات آنها را نقض خواهد کرد.

آسیب‌های ناشی از این تعرضات به حقوق بنیادین، نمی‌تواند صرفاً به دلیل متصف نشدن به عناوین مجرمانه، از مطالعه حقوقی خارج افتد بلکه می‌تواند در قالب پدیده مجرمانه که دایره شمول عامتری نسبت به جرایم دارد، به چالش کشیده شود. چراکه در بیشتر موارد، این آسیب‌ها به این دلیل که محصول یکه‌تازی حکومت‌های اقتدارگرا بر حقوق مخالفین خود جهت به انزوا کشیدن آنها می‌باشد، تبعات زیانبارتری نسبت به جرایم مندرج در قانون دارند. به طوری که امروزه توجه به آسیب‌های ناشی از چنین اقداماتی، اذهان جرم‌شناسان را به توصیف جرایم دولتی رهنمون ساخته است. بنابراین از این نگاه حکومت‌ها، دیگر نهادهای مقدس عاری از مسئولیت قلمداد نمی‌شوند بلکه

درمقابل پیامدهای زیانبار ناشی از عملکرد خود مسئول هستند و سوءاستفاده آنها از اختیارات خود، مبنی بر استفاده ابزاری از اصل قانونی بودن جرم و مجازات در توسعه دامنه محتوای مجرمانه و در نتیجه اعمال پالایش غیراصولی، باعث خواهد شد حقوق شهروندان به صورت ساختارمند نقض شده و آسیب‌های جدی بدان وارد آید.

گرچه این آسیب‌ها عمدتاً به علت موانعی چون حاکمیت ملی، عنوان مجرمانه ندارد ولی می‌تواند از منظر جرم‌شناسی انتقادی بارویکرد آسیب اجتماعی شناختی مورد بررسی قرار گیرد. پس اگر حکومت‌ها در جرم‌انگاری محتوای مجرمانه و پالایش آن، گشاده‌دستی به خرج داده و با پالایش گسترده و غیراصولی حقوق شهروندان را نقض نمایند، نمی‌توانند از زیر بار مسئولیت ناشی از اعمال زیانبار خود، شانه خالی نمایند بلکه در سطح فراملی و در ارزیابی‌های حقوق بشری به حکومت‌های غیردمکراتیک شهره خواهند شد. فلذا همانطوری که فقدان قانون داخلی مبنی بر جرم‌انگاری آسیب‌های منتج از پالایش، اعمال ضدحقوق بشری ناشی از آن را توجیه نخواهد کرد، همچنین پیش‌بینی مصادیق مجرمانه پالایش شده در قانون، موجبات مصونیت دولت‌ها را فراهم نخواهد ساخت.

از این رو حکومتی که مدعی مردم‌سالاری است و به حقوق بنیادین بشری ارجحیت می‌دهد، باید جهت اعمال پالایش اصولی، علاوه بر اصل «قانون‌مندی»، همچنین به ضوابط دیگری که در اسناد حقوق بشری جهانی و منطقه‌ای جهت تحمیل هرگونه محدودیت بر حقوق بنیادین، لازم دانسته شده است، پایبند باشد تا به ناقض حقوق بشر شهره نگردد. بر اساس اسناد فوق، اعمال محدودیت بر حقوق بنیادین و از جمله پالایش، باید واجد جامع شرایط زیر باشد: به موجب قانون شفاف و قابل فهم مقرر شود. مبنای وضع قانون بیشتر بر ضابطه ضرر استوار باشد و بر ضوابط دیگر چون پدرسالاری قانونی و اخلاق‌گرایی جز در شرایط استثنایی تکیه نشود. در واقع مداخله قانون‌گذار باید حداقلی باشد. یک یا چند مورد از اهداف مشروعی را که در اسناد بین‌المللی یا قوانین داخلی تصریح شده است، دنبال نماید. از قبیل احترام به حقوق دیگران، حفظ نظم یا امنیت ملی، پیشگیری از جرم، حمایت از اخلاق و سلامت جامعه. ضرورت داشته باشد. یعنی از میان تدابیر متعددی که می‌تواند اهداف مشروع مورد نظر را تأمین نماید، باید کمترین لطمه را به آزادی‌های افراد بزند. بدین منظور، باید میزان تأثیر پالایش بر حقوق بنیادین روشن شود و محدودیت‌های تحمیل شده بر این حقوق، بتواند با حفظ منافع ناشی از پالایش جبران شود به طوری که ارزش منفعت مورد حمایت، نسبت به حق مورد مداخله بیشتر باشد و هیچ روش دیگری غیر از پالایش، که محدودیت کمتری در حقوق شهروندان ایجاد کرده و برای رسیدن به هدف مورد نظر مطلوب‌تر باشد، وجود نداشته است.

پالایش ضروری، باید مناسب با هدف مورد نظر باشد. بدین معنا که هم معلوم گردد که حقوق خاصی در خطر است و تضمین آن جز با اعمال پالایش ممکن نیست و هم احراز شود پالایش از لحاظ فنی قابلیت تأمین هدف مورد نظر را دارد. چنانچه مشخص شود کاربران بانصب ضدپالایش یا از طریق توسل به پروتکل‌های دیگر، به محتواهای فیلتر شده دست پیدا خواهند کرد، پالایش باوجود داشتن دوشروط اول، به علت عدم کارآیی، غیرضروری و نامتناسب قلمداد خواهد شد.

بدیهی است به منظور احراز این شرط، در بیشتر موارد باید مطالعات و بررسی‌های کارشناسانه‌ای انجام شود تا از کارکرد پالایش جهت وصول به اهداف پیش‌گفته اطمینان حاصل شود. فلذا بدون بررسی نظر متخصصین امر، شهروندان، قربانیان جرایم سایبری، مرتکبین اتفاقی و مرتکبین حرفه‌ای این جرایم، نمی‌توان از کارکرد پالایش در تأمین اهداف مورد نظر اطمینان حاصل نمود. فقط زمانی که ارزیابی‌ها نشان دهد پالایش جامع تمام شرایط فوق است، در مطابقت آن با معیارهای حقوق بشر و در نتیجه غیرمجرمانه قلمداد شدن آن، تردیدی وجود نخواهد داشت.

منابع

الف. فارسی

آقاجانی، سجاد (۱۳۸۸)، «بررسی راهکارهای مبارزه با جرایم رایانه‌ای با توجه به مقررات داخلی و بین‌المللی»، پایان‌نامه کارشناسی ارشد حقوق جزا و جرم‌شناسی، دانشگاه پیام نور، تهران.

احمدی، سید محمدصادق و شمعی، محمد (۱۳۹۵)، «نظارت پیشگیرانه دولت؛ تقابل امنیت و آزادی»، فصلنامه راهبرد، سال بیست و پنجم، شماره ۷۹، صص. ۲۹-۴۶.

انصاری، باقر (۱۳۹۷)، حقوق رسانه، چاپ دهم، تهران: سمت.

ابراهیمی، شهرام (۱۳۹۳)، جرم‌شناسی پیشگیری، جلد اول، چاپ سوم، تهران: میزان.

باراک، گرگ (۱۳۹۶)، «به سوی مطالعات تلفیقی جنایات بین‌المللی و بزهکاری دولتی - شرکتی: رویکردی دوسویه به نقض آشکار حقوق بشر»، ترجمه حامد صفایی آتشگاه، در: جرم‌شناسی فراملی به سوی جرم‌شناسی جنایات بین‌المللی، به کوشش حمیدرضا نیکوکار، چاپ اول، تهران: میزان. صص. ۱۰۵-۱۳۷.

پاک‌نهاد، امیر (۱۳۹۴)، سیاست جنایی ریسک جرم، چاپ دوم، تهران: میزان.

پورقهرمانی، بابک و صابر نژاد، علی (۱۳۹۴)، حریم خصوصی در فضای سایبر از منظر حقوق بین‌الملل، چاپ اول، تهران: مجد.

پورنجفی قوشچی، لیلا؛ فخر، حسین؛ پورقهرمانی، بابک (۱۳۹۹)، «پالایش فضای مجازی در پرتو اسناد حقوق بشری»، **آموزه‌های حقوق کیفری**، دوره هفدهم، شماره ۱۹، صص. ۶۷-۳۵.

حسین پور، پری و صابرزاد، علی (۱۳۹۴)، **آزادی اطلاعات در فضای سایبر از منظر حقوق بین‌الملل**، چاپ اول، تهران: مجد.

خانعلی پور واجارگاه، سکینه (۱۳۹۰)، **پیشگیری فنی از جرم**، چاپ اول، تهران: میزان.

دارابی، شهرداد (۱۳۹۵)، «ریزومیک شدن پیشگیری از جرم در پرتو ریزومیک شدن ارتکاب جرم»، **آموزه‌های حقوق کیفری**، شماره ۱۳، صص. ۲۱۸-۱۹۹.

دکسردی، والتر اس (۱۳۹۴)، **جرم‌شناسی انتقادی معاصر**، ترجمه مهرداد رایجیان اصلی و حمیدرضا دانش ناری، چاپ دوم، تهران: دادگستر.

روث، داوون ال و کازلاریچ، دیوید (۱۳۹۹)، **بزه‌دیده‌شناسی جرم حکومتی**، ترجمه نبی‌اله غلامی، چاپ اول، تهران: شهردانش.

سبزه‌ای، محمدتقی (۱۳۸۶)، «جامعه مدنی به مثابه قرارداد اجتماعی: تحلیل مقایسه‌ای اندیشه‌های هابز، لاک و روسو»، **فصلنامه حقوق و سیاست**، شماره ۲۲، سال نهم، صص. ۹۸-۶۷.

سلیمی، احسان (۱۳۹۷)، «آسیب اجتماعی شناختی پیشگیری از جرایم سایبری در ایران»، رساله دکتری حقوق کیفری و جرم‌شناسی، دانشگاه قم.

صانعی، پرویز (۱۳۷۷)، **حقوق جزای عمومی**، چاپ چهارم، تهران: گنج دانش.

صفاری، علی (۱۳۸۰)، «انتقادات وارده بر پیشگیری وضعی از جرم»، **مجله تحقیقات حقوقی**، شماره ۳۵-۳۶، صص. ۱۹۳-۲۲۳.

غلامی، نبی‌اله و عباسی، محمود (۱۳۹۶)، «درآمدی بر مفهوم جرم دولتی از منظر اصول اخلاق زیستی»، **مجله اخلاق زیستی**، شماره ۲۴، دوره هفتم، صص. ۹۷-۸۴.

فردریش، دیوید (۱۳۹۶)، «به سوی جرم‌شناسی جنایات بین‌المللی: ارائه چهارچوب مفهومی و مبنایی»، ترجمه مهدی کاظمی جویباری، در: **جرم‌شناسی فراملی به سوی جرم‌شناسی**

جنایات بین‌المللی، به کوشش حمیدرضا نیکوکار، چاپ اول، تهران: میزان.

فرهادی‌آلاشتی، زهرا (۱۳۹۵)، **پیشگیری وضعی از جرایم سایبری: راهکارها و چالشها**، چاپ اول، تهران: میزان.

قاجارقیونلو، سیامک (۱۳۹۱)، **مقدمه حقوق سایبر**، چاپ اول، تهران: میزان.

قورچی بیگی، مجید (۱۳۹۵)، «جرم‌شناسی جرایم دولتی؛ از غفلت جرم‌شناسی تا جرم‌شناسی آینده‌نگر»، به کوشش حسین غلامی در: **علوم جنایی تطبیقی در پرتو همکاری‌های**

- بین‌المللی، مجموعه مقالات نکوداشت دکتر سیلویا تلنباخ، چاپ اول، تهران: میزان، صص. ۳۰۴-۳۲۴.
- کلارک، آر.وی. جی (۱۳۸۸). **جرم‌شناسی پیشگیری**، ترجمه مهدی مقیمی و مهدیه تقی‌زاده، تهران: نشر زرد.
- کوچ‌نژاد، عباس (۱۳۸۳)، «محدودیت‌های حقوق بشر در اسناد بین‌المللی»، **حقوق اساسی**، سال دوم، شماره سوم، صص. ۱۶۹-۱۷۸.
- کوزلاریچ، دیوید؛ مانتو، ریک؛ جی میلر، ویلیام (۱۳۸۹)، «بزه‌دیده‌شناسی جرایم دولت»، ترجمه قورچی‌بیگی، مجید، **فصلنامه اطلاع‌رسانی حقوقی**، معاونت تحقیقات، آموزش و حقوق شهروندی، شماره ۲۲-۲۱، صص. ۱۱۷-۱۳۸.
- گرین، پنی؛ وارد، تونی (۱۳۹۸)، **جرم‌حکومتی، دولت‌ها، خشونت و فساد**، ترجمه نبی‌اله غلامی، چاپ اول، تهران: انتشارات مجد.
- نادرخانی، نیما (۱۳۹۰)، «ابزارهای مورد استفاده مجرمان و خرابکاران رایانه‌ای»، **فصلنامه کارآگاه**، دوره دوم، سال چهارم، شماره ۱۴، صص. ۳۸-۶۱.
- نجفی ابرندآبادی، علی حسین (۴-۱۳۷۳)، «**نظریه‌های جرم‌شناسی**»، مجموعه تقریرات، صص. ۱۷۷-۲۲۹.
- نجفی ابرندآبادی، علی حسین (۱۳۸۸)، «**جرم‌شناسی نو-کیفرشناسی نو؛ درآمدی بر سیاست جنایی مدیریتی خطر مدار**»، زیر نظر علی حسین نجفی ابرندآبادی، **مجموعه مقاله‌های تازه‌های علوم جنایی**، چاپ اول، تهران: میزان، صص. ۷۱۷-۷۵۰.
- نجفی ابرندآبادی، علی حسین (۱۳۹۰)، «از جرم‌شناسی تا آسیب اجتماعی‌شناسی»، در: یادنامه شادروان دکتر رضا نوریها، **مجله تحقیقات حقوقی**، شماره ۵۶، صص. ۱۰۱۵-۱۰۳۱.
- نجفی ابرندآبادی، علی حسین (۱۳۹۴)، به سوی تعریف یک سیاست ملی پیشگیری از بزهکاری، **دیباچه در: دانشنامه پیشگیری از جرم آکسفورد**، براندون. سی. ولش؛ دیوید پی. فارینگتون، به کوشش حمیدرضا نیکوکار، صص. ۹-۱۶.
- نجفی ابرندآبادی، علی حسین (۱۳۹۴)، «پیشگیری عادلانه از جرم»، در: **علوم جنایی، مجموعه مقالات تجلیل از دکتر محمد آشوری**، چاپ چهارم، تهران: سمت، صص. ۵۵۹-۵۹۸.
- نجفی ابرندآبادی، علی حسین (۱۳۹۵)، «از جرم‌شناسی حقیقی تا جرم‌شناسی مجازی»، **دیباچه در: جرم‌شناسی**، ژرژ، پیکا، ترجمه علی حسین نجفی ابرندآبادی، چاپ چهارم، تهران: میزان، صص. ۹-۱۷.

نجفی ابرندآبادی، علی حسین (۱۳۹۵)، «جرم‌شناسی در آغاز هزاره سوم»، دیباچه در: **دانشنامه جرم‌شناسی** از: علی حسین نجفی ابرندآبادی و حمید هاشم‌بیگی، چاپ چهارم، تهران: انتشارات گنج دانش. صص. ۱۳-۲۸.

ون هام، فرانسواز (۱۳۹۵)، «آسیب اجتماعی‌شناسی: رشته‌ای جدید، توسعه قلمرو جرم‌شناسی؟»، ترجمه سید حسین حسینی، و اقبال محمدی، در: **دایره‌المعارف علوم جنایی، مجموعه مقاله‌های تازه‌های علوم جنایی**، چاپ دوم، تهران: میزان. صص. ۹۸۵-۱۰۰۳.

ب. انگلیسی

Article 19, (2016), "Freedom of expression unfiltered: How blocking and filtering affect free speech", London, **Article 19**, last visited : 3/12/2019, Available at: www. Article 19.org. pp.1-26.

Banday, M. Tariq & Shah, N. A (2010), "A concise study of web filtering", **Sprouts: Working paper on information systems**, 10(31), pp.1-11.

Breindl, Yana & Theiner, Patric & Busch, Andreas (2015), "Internet blocking regulation :a comparative analysis of 21 liberal democracies", presented at the u4 cluster conference: Governance of a contemporary multilateral institutional architecture, of political science, pp.1-42.

Callanan, Cormac & Gercke, Marco & DeMarco, Estelle & Ziegenheiner, Hein (2009), **Internet blocking balancing cybercrime responses in democratic societies**, Open society Institute, Action internet solutions.

Jaishankar, Karupannan (2008), "Space transition theory of cyber crimes, in book: **crime of the internet, chapter: space Transition Theory of cyber crime**", Editores: Frank, Schmalleger, Michael, Pittaro, Publisher pearson.

OpenNet Initiative (2004), "A Starting point: legal implication of internet filtering", **OpenNet Initiative**, .last visited: 12/7/2019, Available at: www.opennet initiative.org. pp.1-17.

Reyns, Bradford & Henson, Billy (2013), "security in digital world: understanding and preventing cybercrime victimization", Switzerland, **Security Journal**, 26(4), pp. 311-314.

Vicks, Mery E (2013), **An examination of internet filtering and safety policy trends and issues in south Carolina, s K-12**, public schools, Nova Southeastern University (NSU).

Zittrain, Jonathan & L,John & G, Palfrey Jr (2007), "Access denied:the practice and policy of Global internet filtering", Oxford ,**Oxford internet institute research report**,no. 14, pp.1-30.

روش استناد به این مقاله:

پورنجفی، لیلا؛ فخر، حسین و پورقهرمانی، بابک (۱۴۰۱)، «بالایش فضای سایبری به مثابه جرم یا ابزار پیشگیری از آن؟»، پژوهشنامه حقوق کیفری، دوره ۱۳، پیاپی ۲۶، صص. ۱۶۳-۱۸۷. DOI:10.22124/jol.2022.18816.2078

Copyright:

Copyright for this article is retained by the author(s), with first publication rights granted to *Criminal Law Research*. This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution License (<https://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided that the original work is properly cited.

