Criminal Law Research
Vol. 13, No. 2, (Serial 26)
Fall2022 & Winter 2023
Research Article

University of Guilan
Iranian association of penal law

DOI:10.22124/jol.2022.20840.2214
DOR: 20.1001.1.23222328.1401.13.2.7.7

Received: 2021/10/17 **Accepted: 2022/08/20**

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

Leala Pornajafi[1]
Hossein Fakhr[2]*
Babak Pourghahramani[3]

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.

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 socity Institute**, Action internet solutions.

Jaishankar, Karupannan (2008), " Space transition theory of cyber crimes,in book: crime of the internet,chapter: space Trasition Theory of cybercrime", Editores: Frank, Schmalleger, 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.opennet initiative.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

DOI:10.22124/jol.2022.20840.2214
DOR: 20.1001.1.23222328.1401.13.2.7.7

مقاله پژوهشی
صفحات: ۱۸۷-۱۶۳
تاریخ ارسال: ۱۴۰۰/۷/۲۵
تاریخ پذیرش: ۱۴۰۱/۰۵/۲۹

نشریه علمی پژوهشنامه حقوق کیفری
سال سیزدهم، شماره دوم، پاییز و زمستان ۱۴۰۱، پیاپی ۲۶

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

لیلا پور نجفی [۱]
حسین فخر [۲] ✉
بابک پورقهرمانی [۳]

چکیده

تقریبا همه دولت‌ها بنا به ملاحظات مختلف در راستای پیشگیری از جرم در فضای مجازی، به پالایش متوسل می‌شوند. ولی اغلب، از یک طرف به‌دلیل 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 شیوهٔ 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

---

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
✉ h-fakhr@tabrizu.ac.ir

مقدمه

رسانه‌ها گاه به‌دلیل برداشت نادرست مخاطبین از محتواهای آن‌ها و گاه به علت ترویج جرم، ممکن است به ایجاد فرهنگ بزهکارانه کمک کنند. دراین میان تأثیر اینترنت به‌دلیل گستره نفوذ و ارتباط دوسویه آن با مخاطبان، چشمگیرتر است. شبکهٔ جهانی اینترنت به‌دلیل معرفی الگوهای فکری مختلف، درجهت‌دهی 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 قرارمی‌دهد (Reyns&Henson,2013:311). فضای سایبری علاوه بر اینکه ابزاری برای ارتکاب جرایم سنتی همچون سرقت وکلاهبرداری یا آموزش این جرایم است، فضایی برای«جرایم سایبری محض» (نجفی ابرندآبادی،۱۳۹۵ الف: ۱۱) نظیر هک کردن و انتشار بدافزارهاست که ازجمله جرایم نوظهور بوده و صرفا در فضای سایبری و علیه داده‌های موجود درآن محقق می‌شوند. جرایم سایبری به معنای اعم کلمه جرایمی هستندکه بعضا با استفاده از داده‌ها یا سامانه‌های رایانه‌ای محقق می‌شوند و بعضا 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 اخلال ایجاد می‌نماید، ولی به علت نقص فنون پالایش،«حتی پیشرفته‌ترین کشورها در زمینهٔ علوم رایانه‌ای، نمی‌توانند اطلاعاتی را که کاربران قصد انتشار یا دسترسی به آن را دارند، پوشش دهند (Zittrain& et al, 2007:7) و کاربران معمولا با عبور از فیلتر به محتوای پالایش شده دسترسی پیدا می‌کنند و درنتیجه 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 بند۲ماده۲۹ اعلامیه جهانی حقوق بشر و ماده۱۹ 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 ازجمله اصل قانون‌مندی، اصل هدف مشروع و اصل ضرورت هستند و از آنجا که پالایش فضای مجازی، محدودیت‌هایی برحقوق 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 عمدتا در رژیم‌های اقتدارگرا اعمال می‌گردد، نقض حقوق مذکور را به دنبال خواهد داشت. این مداخلات و لطمات ناشی از آن، باوجود عدم تصریح در قوانین جزایی، به‌دلیل این‌که «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 زمینهٔ پالایش فضای سایبری در حوزه حقوق بنیادین شهروندان چیست؟ آیا با بهره‌گیری ازآموزه‌های جرم‌شناسی انتقادی، نقض ساختارمند حقوق بشر به واسطهٔ 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 درجهت نقض حقوق بشر یا حقوق بین‌الملل بشردوستانه است که در قالب«مخاطرات طبیعی، تروریسم حکومتی، جرایم جنگی، نسل کشی، فساد[1]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 حوزهٔ فناوری اطلاعات، علاوه بر امنیت ملی کشورها، امنیت جامعه جهانی را نیز در معرض تهدید جدی قرار داده‌اند. (نجفی ابرندآبادی،۱۳۹۵ ب: ۲۶و۲۵) ازاین 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، ازجمله اعمال پالایش متوسل می‌شوند و فرضشان براین است که پالایش به علت قابلیت‌های چندگانه‌اش، می‌تواند

---

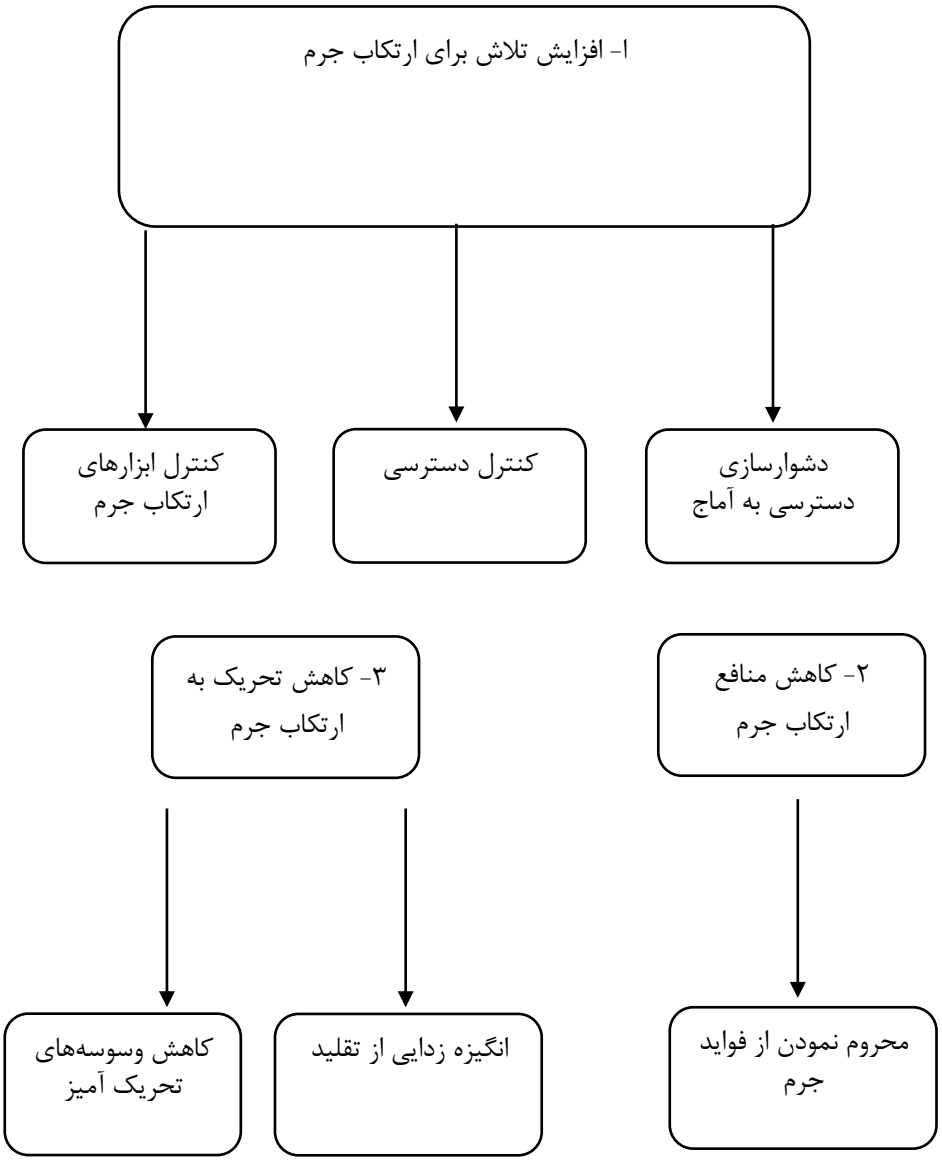
۱. ر.ک به : گرین، پنی، و تونی،وارد، «جرم حکومتی،دولت‌ها،خشونت و فساد»،ترجمه نبی اله غلامی.

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 ازجمله 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 ،آر.وی. 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 هرقدر 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. درنتیجه، 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 واجارگاه، ۱۳۹۰: ۷۷). پالایش با داشتن قابلیت‌های فوق، چه‌بسا 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[1]دسترسی به شبکه، اعم از رایانه‌های شخصی، مسیریاب‌ها[2]، سامانه‌های ارائه‌دهنده خدمات شبکه‌ای و نیز ایجادکنندگان نقطه تماس بین‌المللی، از ورود یا ارسال برخی محتواهای غیرمجاز یا غیرقانونی جلوگیری نمود» (آقاجانی،۱۳۸۸:۱۷۰). پالایش می‌تواند دسترسی به سیبل‌های جرم را دشوار ساخته و از بزه دیدگی آنها جلوگیری نماید. به این واسطه کاربران در دسترسی به برخی محتواها که با لحاظ مؤلفه‌های فرهنگی، مذهبی، اخلاقی، سیاسی، اجتماعی و ... در هرکشور 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 محدودهٔ تعیین شده را نداشته و صرفا 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. به‌عنوان 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 درواقع با

1.Nodels
2 .Routers

دورکردن بزه دیدگان بالقوه، از آنها در مقابل امواج بزهکاری در محیط سایبر حمایت می‌نماید. نمونه بارز این قابلیت، پالایش در سطح فردی (Banday&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 به‌دلیل 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[1]،کرم‌ها[2]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 حیطه تنگ خواهد شد. مسدود نمودن وب‌سایت‌های توزیع‌کننده این بدافزارها ازجمله تدابیر مورد نظر است که دسترسی بزهکاران به ابزارهای جرم را کنترل می‌نماید.

البته به‌دلیل 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 جابجایی 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 مصمم، 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[3]، مجرم بالقوه شخصی حسابگر است و زمانی‌که تشخیص دهد منافع احتمالی جرم بر مضرات آن غلبه خواهدکرد، مرتکب جرم می‌شود. بدیهی است«این سودها فقط مادی نیستند چرا که معمولا 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، پی‌بردن 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 ازجمله 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«معمولا برای ارتکاب جرم آمادگی قبلی ندارند، اما در پاره‌ای اوقات ممکن است تحت‌تأثیر 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. مثلا 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 بالاخص هرزه‌نگاری کودکان به‌دلیل 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 نظیرکلاهبرداری، ساخت مواد منفجره، هک کردن و... در فضای مجازی می‌پردازند، نیز می‌تواند به‌عنوان مانعی درجهت 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، اِعمال فنون پیچیده پالایش را جهت محدود نمودن دسترسی به اینترنت انکار نمی‌کنند» (Breindl&etal,2015:3) ولی به‌دلیل ایرادات پالایش، چندان نمی‌توانند در تحقق اهداف خود موفق شوند، تا جایی‌که 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 مسکّنی از نظر کاهش وقوع جرم دارد» (نجفی ابرندآبادی،۱۳۸۸: ۷۴۹). وقتی مجرم به‌دلیل اعمال فن‌آوری‌هایی چون پالایش، از دسترسی به محتوای مجرمانه و ارتکاب جرم به شیوهٔ خاص منع می‌گردد، از اسلوب دیگری برای رسیدن به هدف خود استفاده می‌کند. جابجایی شیوهٔ ارتکاب جرم در فضای مجازی در مقایسه با فضای فیزیکی به شکل آسان‌تر و سریع‌تر اتفاق می‌افتد و استدلال کسانی که معتقدند«اگرجابجایی 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 عبورکرده[1] و یا با بهره‌مندی از وب‌سایت‌های فیلترنشده دیگر، فیلترها را دور زده و به محتوای مجرمانه دسترسی پیدا می‌کنند.

باری، درهیچ کشوری شیوه‌های پالایش بی‌نقص نیست.«حتی با تجربه‌ترین کشورها دراین زمینه، به سختی می‌توانند ازطریق پالایش اطلاعاتی را که کاربران قصد انتشار یا دسترسی دارند، پوشش دهند» (Zittrain&etal,opcit:7). درواقع، اکثرشیوه‌های پالایش حداقل با یک یا چند روش قابل دور زدن هستند.[2] ازاین رو،کاربران قاصد معمولا 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 cincise study of web filtering».
2.see: Vicks, M.,« An examination of interner filtering and safety policy trends and issues in south Carolina» ,s K-12 public schools.

نماید. با این حال، برخی دولت‌ها چنان بی‌رویه دراین راستا می‌تازند که به‌دلیل 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. درحالی‌که آن حقوق بخش مهمی از ارزش‌هایی است که دراسناد مهم بین‌المللی و منطقه‌ای و قوانین اساسی کشورها مورد تأکید قرارگرفته است. آسیب‌های حقوق بشری پالایش ناشی ازدو عامل است:۱-عدم ارتقای فن‌آوری‌های مربوطه۲-پالایش افراطی. نقص فنون پالایش یا عدم به‌روزرسانی آن ممکن است موجب پالایش بیش از حد شده[1]و محتواهای مجاز را نیز شامل شود و درنتیجه «آزادی‌های مدنی به‌صورت غیرضروری 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 درنتیجه تجدیدنظر متولیان امردر لیست سیاه[2]مربوط به پالایش قابل رفع است.

آنچه به لحاظ حقوق بشری شایان اهمیت فراوانی است، پیامدهای منفی ناشی از پالایش افراطی است که عمدتا توسط نظام‌های سیاسی اقتدارگرا و تحت پوشش تأمین نظم عمومی، امنیت ملی، پیشگیری ازجرم و...انجام می‌پذیرد و به‌دلیل رویکرد سرسختانه دولت‌ها، هیچ‌گونه انعطافی را برنمی‌تابد. چنین صدماتی از نگاه افکار عمومی و مجامع حقوق بشری پنهان نمی‌ماند و باب جدیدی درجرم‌شناسی مفتوح می‌نماید. بدین نحو که می‌توان از رهگذر جرم‌شناسی انتقادی با رویکرد آسیب اجتماعی‌شناختی به تحلیل آن پرداخته و آن را به‌عنوان یکی ازمصادیق جرایم دولتی[3]مطرح نمود.

۲. ۱. پالایش افراطی: ناقض حقوق بنیادین

پالایش افراطی و بی‌رویه موجب می‌شود برخی ازمصادیق«حقوق اساسی اشخاص،ازجمله حق آزادی بیان»(zittrain&etal,op.cit:25)،«حق زندگی خصوصی و خانوادگی (Callanan&etal,op.cit:151)اعم ازحریم خصوصی مراسلات و حریم داده‌های شخصی، با گسترش قدرت دولت در فضای سایبر در معرض تهدید و مداخله قرار بگیرد درحالی‌که این حقوق

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

براساس 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 دراغلب اسناد حقوق بشری همچون ماده ۱۲ اعلامیه جهانی حقوق بشر، ماده ۱۷میثاق بین‌المللی حقوق مدنی و سیاسی، ماده۸ کنوانسیون اروپایی حقوق بشر و...، به رسمیت شناخته شده است. درحمایت از این حق در فضای سایبر، به اسنادی نظیر«رهنمودهایی برای قانون‌گذاری فایل داده شخصی کامپیوتری» مصوب کمیسیون حقوق بشر سازمان ملل درسال ۱۹۸۹، دستورالعمل‌های مختلف پارلمان اروپا،[1] ماده ۱۵ کنوانسیون جرایم سایبری و... اشاره نمودکه همگی بیانگر اتخاذ گام‌های اساسی در سطح بین‌المللی جهت حمایت از این حق درفضای سایبر هستند.

دراین مبحث فقط آن بخش از زندگی خصوصی که ممکن است با پالایش تضعیف شود، بررسی می‌شودکه 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 درجهت حمایت‌های قانونی از این جنبه های حریم خصوصی، احتمالا به‌دلیل 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 دراین خصوص پاسخ دهد. البته برخی مواد منشورحقوق شهروندی به ابعاد تازه حریم خصوصی تصریح نموده است. این منشور با آنکه اعتبار قانون مصوب مجلس را ندارد و الزام‌آور نیست ولی ازجهت جلب توجه به ابعاد نوین حریم خصوصی، می‌تواند همچون چراغی فراروی قانون‌گذار باشد.

۱.۱.۱.۲. حریم خصوصی مراسلات

«مراسلات»[2]و ازجمله آن ارتباطات اینترنتی به‌عنوان یکی ازمصادیق حق زندگی خصوصی است که در اسناد پیش گفته بر محرمانه بودن آن تصریح شده است. در ماده ۳۷منشورحقوق شهروندی لزوم احترام به گونه‌های جدید این حق، ازجمله نامه‌های الکترونیکی، ارتباطات اینترنتی و...نیز مورد تأکید قرارگرفته است.

---

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

2.Correspondence

پالایش ممکن است موجب تضعیف حق مزبور شود. زیرا متولیان پالایش به منظورکشف و درنتیجه فیلتر نمودن محتواهای غیرقانونی و مجرمانه، که عمدتا با هدف پیشگیری ازجرم انجام می‌پذیرد، محتواهای تبادل شده بین کاربران و به‌ویژه کاربرانی را که در مظان اتهام جرم قرار دارند، تحت نظرگرفته و بدون اجازه کاربران، آن داده‌ها را جمع‌آوری و بعضا ذخیره‌سازی می‌نمایند و با این اقدام خود، حق محرمانگی مراسلات اینترنتی را مخدوش می‌کنند. دراین خصوص دادگاه اروپایی حقوق بشر در رایی«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 درحق زندگی خصوصی و نیز حق مراسلات مندرج درماده ۸ کنوانسیون اروپایی حقوق بشردانسته است» (Ibid).

۲.۱.۱.۲.حریم خصوصی داده‌های شخصی

یکی دیگر از مصادیق حق زندگی خصوصی،که با توسعهٔ 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 ازداده‌ها،[1] 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 خواهدشد» (پورقهرمانی و صابرنژاد،۱۳۹۴: ۳۷). درصورتی 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 منظورکشف محتواهای مجرمانه جهت فیلتر نمودن آن فراهم نمایند و حق مذکور را به خطر اندازند.

درخصوص اهمیت این حق نو ظهور باید ذکرشود علاوه براین که اغلب کشورها سطوح متعارفی از اصول حمایت از داده‌ها را درقوانین داخلی خود برقرار می‌نمایند در سطح فراملی مقررات عمومی حفاظت ازداده (GDPR)[2] به ابتکار اتحادیه اروپا تدوین گشته است. پیش ازآن ماده ۸ منشورحقوق اساسی اتحادیه اروپا و نیز«دستورالعمل‌های[3] آن، دول عضو را به تضمین احترام به حق مزبوردر قلمرو داخلی خود مکلف ساخته بود» (Callanan&etal,op.cit:152). درایران نیز، برخی مواد منشورحقوق شهروندی (مواد۳۵، ۳۷،۳۸و۳۹) و قانون تجارت الکترونیکی (مواد۵۸و۵۹) 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، درعملکرد 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 ۱۹میثاق بین‌المللی حقوق مدنی و سیاسی، ماده ۱۰کنوانسیون اروپایی حقوق بشر، می‌توان به اسناد خاص فضای سایبر، نظیر پاراگراف ۲۴ از بند۳«بیانیه اصول اجلاس عالی سران درخصوص جامعه اطلاعاتی»، پاراگراف چهارم «سندتعهدتونس» (حسین پور و صابرنژاد، ۱۳۹۴: ۹۳و۹۲) و مواد ۴و۳ «اعلامیه آفریقایی حقوق و آزادی‌های اینترنتی» اشاره نمود.[1]

تقریبا همه اسناد مربوط به حق آزادی بیان، به حق دریافت و ارسال اطلاعات نیزتأکید 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 رکین 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 می دهند» (انصاری،۱۳۹۷: ۲۱) را دارند.

دراین راستا «کمیته حقوق بشر سازمان ملل در سال ۲۰۱۱حق آزادی بیان را برای تمامی اشکال بیان و نیزتمامی رسانه‌ها اعم از الکترونیکی و اینترنتی به رسمیت شناخته است.» (Article19,2016:11) همچنین این امر در ماده۲ 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....»درنظام حقوقی داخلی حق آزادی بیان ازاصل ۲۴و۲۷ وحق آزادی اطلاعات تلویحا از اصول۳،۶و۸ قانون اساسی قابل استنباط است. علاوه برآن، قانون مستقلی باعنوان«قانون انتشار و دسترسی آزاد به اطلاعات»در راستای به رسمیت شناختن حق اخیرتصویب 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 شفاف سازی حکومت» (انصاری، همان:۲۴) عمل کرده و ضمن جلوگیری حاکمان از فساد، آنها را به پاسخگویی وادار می‌کند.

تردیدی نیست بشرامروزی جهت ابراز آزادی بیان و اطلاعات، ناگزیراز 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 درنتیجه منع آنان ازنظارت 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 براینکه می تواند محتواهای مورد درخواست آنان را مسدود کرده و باعث محرومیتشان ازحق آزادی اطلاعات شود، همچنین ممکن است آنان را از ادامه فعالیت درتولید محتوا و درنتیجه حق آزادی بیان محروم نماید. زیرا درفضای مجازی علاوه بر تولید محتواهایی که مطلوب حکومت‌ها است، ممکن است محتواهایی نیز تولید شود که به‌دلیل 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 توسعهٔ قلمروی مصادیق مجرمانه و سرکوبی شهروندان معترض از طریق پالایش پرداخته و اقدام خودرا با عناوینی چون تأمین نظم عمومی، پیشگیری ازجرم 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«عوام گرایی 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 ازحد درحق آزادی بیان افراد خواهد بود. این درحالی است که امروزه در نظام‌های مردم‌سالار«سیاست جنایی ملهم از حقوق پیشگیری تحت‌تأثیر اسناد بین‌المللی کیفری و حقوق بشری، برای تأمین امنیت اجتماعی پایدار، رویکرد کرامت‌مدار پیداکرده است» (نجفی ابرندآبادی،۱۳۹۴ الف: ۱۰و۱۱) چرا که از نظر آنان محدودیت‌های ناشی از پیشگیری جز با شفافیت و دقیق 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، برجرایم 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 براین نظرندکه جرم‌شناسان کلاسیک به نام اصل قانونی بودن جرم و مجازات، فقط به مطالعه آن دسته از رفتارهایی که درقانون جرم تلقی شده، پرداخته و از بررسی سایر پدیده‌های ضد انسانی خودداری کرده‌اند و با این رویکرد،«هیئت حاکمه راتحکیم نموده‌اند.» (نجفی ابرندآبادی،۱۳۷۳و۱۳۷۴: ۲۱۳) حال آنکه در بیشتر موارد، این اعمال به‌دلیل اینکه «محصول سازماندهی اجتماعی ناشی از ارتباطات متعارض قدرت هستند» (ون هام، همان: ۱۹۹۴) آسیب‌زننده‌تر نیز می‌باشند.

اگر ما در بررسی پالایش، به نظرجرم‌شناسان کلاسیک اکتفا نماییم، به یقین از شناخت علل جرایم سایبری مصرح درقانون و ارائۀ 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 اکثرجوامع است، نیم نگاهی بیندازیم. در واقع مداخلات بی‌رویه برحقوق بنیادین شهروندان که نتیجه اجتناب‌ناپذیر پالایش بی‌رویه است، ازدایرۀ مطالعه ما خارج خواهد افتاد. درحالی‌که 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 درخصوص خطرات کنترل نشده‌ای چون جرایم علیه محیط زیست، آثارباستانی، حقوق بشر و...است. براساس این دیدگاه،«جرم یک مفهوم مضیق است وبراساس معیارهای حاکمیت ایجادمی‌شود 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 یایک ملت را خدشه‌دار کرده» (نجفی ابرندآبادی،۱۳۹۰: ۱۰۲۷) و عمدتا هم درقوانین جزایی منعکس نمی‌گردد. حجم عظیم این صدمات ازجمله مداخلات حقوق بشری ناشی ازپالایش افراطی، توسط صاحبان قدرت و هیئت حاکمه ایجادمی‌شود.ارتباط این آسیب‌ها باساختار قدرت و عدم تصریح آن درقوانین کیفری، مانع از مطالعات جرم‌شناختی آن نخواهد بود بلکه«این دغدغه‌ها به طرقی بنیادین باموضوعات مطروحه درجرم‌شناسی فراملی تلاقی می‌یابند» (فردریش،۱۳۹۶: ۹۰) و با بهره‌گیری از«استانداردهای حقوق بشری وآسیب‌های اجتماعی» (دکسردی،۱۳۹۴: ۱۱۷) می‌توانند درقالب جرم دولتی مطرح گردند.

۳.۲. شناسایی پالایش افراطی به عنوان جرم دولتی

جرم دولتی به مفهوم«رفتارسازمان‌یافته هیئت حاکمه یک کشور درجهت نقض یا نادیده گرفتن حقوق شهروندان» (غلامی و عباسی،۱۳۹۶: ۸۴) تعریف شده است.برخی نیز آن را«اقدامات غیرقانونی، ضداجتماعی و ظالمانه‌ای دانسته‌اندکه به نفع دولت‌ها یا نهادهای دولتی و نه برای سودونفع فردی(عوامل فردی دولت)ارتکاب می‌شوند.» (کوزلاریچ ودیگران ،۱۳۸۹: ۱۲۰) چنین تعاریفی درتلاشند«تا ازاشکالات ایجاد شده توسط تعاریف حقوقی مضیق ازجرم،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، درتحلیل این جرایم مفید فایده خواهد بود. ازنظرطرفداران حقوق طبیعی،«انسان براساس خردخویش به این امر پی می‌بردکه برای حفظ واجرای حقوق طبیعی خود اعم ازحق زندگی، امنیت وآزادی، درقالب قرارداد اجتماعی حکومتی تأسیس کند.» (سبزه‌ای،۱۳۸۶: ۹۲) براساس این قرارداد، هرفرد بخشی ازآزادی خود را جهت تضمین حقوق مذکور به حکومت تفویض می‌کند. ولی چشم‌پوشی شهروندان از برخی حقوق خود درجهت تفویض آن به حکومت، به مفهوم واگذاری بی‌حد وحصرکلیه 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 برتفویض برخی اختیارات به آنها، به‌عنوان دستاویزی جهت تضییع حقوق بنیادین بهره جویند، عمدتا براساس اصل قانونی بودن جرم و مجازات، حدودحقوق واگذارشده و ضمانت اجرای تخطی ازآن، به صراحت مشخص می‌گردد. هرچند معمولا ادعا می‌شود این اصل از یکه‌تازی حکومت‌های خودکامه جلوگیری کرده وحقوق شهروندان را نیز به نحو بهتری تضمین می‌نماید ولی نظر به اینکه تصویب قوانین توسط هیئت حاکمه صورت می‌گیرد، دربرخی ازموارد، آنان با سوءاستفاده از اختیارات تفویض شده و نیز استفاده ابزاری از این اصل، حقوق شهروندان را به‌صورت ساختارمند نقض کرده و آسیب‌های جدی بدان وارد می‌سازند.

پالایش فضای سایبری نیز،گرچه با استفاده ازاختیار قانون‌گذاریِ حکومت‌ها وجهت پیشگیری از وقوع جرم یا تأمین امنیت، اعمال می‌شود ولی عمدتا ابزاردست دولت‌های اقتدارگرا قرار می‌گیرد. به‌طوری که آنان تحت لوای پالایشِ به ظاهر قانونی و مشروع، حقوق و آزادی‌های اساسی پیش‌گفته را سلب می‌نمایند. درواقع اصلی که یکی ازمبانی آن مقابله باتعرض حکومت‌ها برحقوق شهروندان است، در راستای تعرض به حقوق اساسی همان شهروندان و درنتیجه ارتکاب جرم دولتی موردسوءاستفاده قرارمی‌گیرد. درحالی‌که «به منظور عادلانه شدن تدابیر پیشگیرنده، دولت‌ها باید

همان حقوق و آزادی‌های فردی‌ای را ملاحظه نمایندکه 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 ازروش‌های اعمال محدودیت برحقوق افراد، لاجرم باید از همان قواعدتبعیت نماید.

باری هرچندحکومت‌ها محتواهای مجرمانه قابل پالایش را، درقوانین خود پیش‌بینی می‌نمایند و در بیشترموارد فقط به پالایش محتوای مجرمانه مقرر در قانون بسنده می‌نمایند ولی گاه به‌دلیل وضع قوانین جزایی تفسیربردار وگاه به جهت گشاده‌دستی درتعیین فهرست مصادیق مجرمانه توسط مقنن، ازهمان 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 اِعمال محدودیت برحقوق بنیادین، در تطبیق محتواها با فهرست مجرمانه‌ای که مقنن تصویب نموده است، عامل مضاعف دیگری درجهت تعرض به این حقوق می باشد. 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 ازجمله حقوق بنیادین بشری هستند، نقض می‌نماید و ازآنجا که«نقض حقوق بشر به‌عنوان هسته تعریف جرم[دولتی] درنظرگرفته می‌شود»، (روث؛ کازلاریچ،۱۳۹۹: ۳۴) فلذا پالایش افراطی نیز از جهت تعرض به حقوق مذکور در فوق، می‌تواند به‌عنوان جرم دولتی قلمدادشود. درنظام جزایی کشورمان«تفویض مقام تقنین مبنی برتعیین فهرست مصادیق مجرمانه به کارگره تعیین مصادیق مجرمانه (سلیمی، ۱۳۹۷: ۱۰۳)» درماده۷۵۰قانون مجازات اسلامی-که فقط یکی از اعضای۱۲نفره آن کارگروه از نمایندگان مجلس است- و نیز واگذاری«اختیارتحکیم» (همان) به این مقام غیرقضایی مبنی برتعیین مصادیق فوق،طبق ماده ۷۵۱ قانون مذکور، ازعواملی است که می‌تواند به معضل مورد نظر دامن بزند.

پس می‌توان گفت آسیب‌های ناشی ازپالایش افراطی هم منتسب به قانون‌گذاران است و هم متوجه عملکرد مجریان قانون.بدین شرح که، اگر قانون‌گذاران دروضع قوانینی که مجوزاعمال پالایش می‌باشد، اصل مداخله حداقلی را مبنا قرار ندهند، یامجریان قانون دراجرای پالایش وتطبیق حکم باموضوع، به اصول «ضرورت و تناسب» که اسنادحقوق بشری جهت اعمال محدودیت برحقوق بنیادین پایبندی بدان را لازم دانسته، مقید نباشند، به جرم دولتی متهم خواهندشد.

با ملاحظه اصل ضرورت، مجریان قانون از میان تدابیر متعددی که می‌توانند اهداف مشروع مورد نظر مقنن را نماید، 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 موردنظردرپاسخ به نیاز مهم جامعه اتخاذشود.۲- تدبیراتخاذشده با هدف خود تناسب داشته باشد.تردیدی نیست پالایش نیز به‌عنوان یکی از مصادیق محدودیت‌های تحمیل شده برافراد، لاجرم باید از هر دو شرط پیش گفته تبعیت نماید.

به موجب شرط اول پالایش باید با توجه به اهداف مشروعی که درتعقیب آن است،کارآیی کافی جهت پاسخ به نیاز جدی جامعه‌ای که در آن اجرا می‌شود، را داشته باشد. دراین 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 محتواهای 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 ازمصادیق 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 این‌که 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 درصدد 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 به‌طوری که ارزش منفعت مورد حمایت، نسبت به حق مورد مداخله بیشتر باشد و ارزیابی گردد که هیچ روش دیگری غیر از پالایش که مداخلهٔ 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 ازقانون‌گذاران و مجریان قانون می‌باشندکه با ارتکاب چنین جرایمی«سیاست‌ها واهداف نهادهای سیاسی راتعقیب می‌کنند.» (باراک،۱۳۹۶: ۱۰۵) بزه دیدگان آن،شهروندانی هستند که به علت اتخاذ سیاست‌های خلاف قواعد حقوق بشرتوسط دولت‌ها، متحمل صدمه درحقوق بنیادین خود شده‌اند. قوانینی که ازآن تخطی می‌شود،«قوانین حقوق بین‌الملل، قوانین داخلی واخلاقیات اجتماعی، به‌صورتی که توسط مخاطبان تفسیر شده‌اند، هستند. این مخاطبان شامل جامعه مدنی داخلی و بین‌المللی، حکومت‌های دیگر و آژانس‌های دیگر در داخل خودحکومتِ بزهکارمی‌باشند»(گرین؛ وارد، پیشین:۲۳) وضمانت اجراهای چنین جرمی«انتقادیا شورش توسط خود مردمِ حکومت،آسیب رساندن به اعتبار داخلی و بین‌المللی حکومت و تحریم‌های نظامی واقتصادی توسط سایرحکومت‌ها» (همان) است.

شایان ذکراست تلقی نمودن پالایش افراطی به‌عنوان جرم دولتی، ازیک طرف به علت داشتن نگرشی کلان به موضوع و از طرف دیگر به جهت زیرسوال بردن اقدامات هیئت حاکمه و مصون ندانستن آنها ازعواقب اعمال زیانبارشان، ساختارشکنی مثبت قلمدادشده و باعث می‌شود موضوعاتی همچون نقض حقوق بشر،به عرصه جرم‌شناسی راه پیدا نماید.همچنین،ازحیث پرداختن به«پدیده مجرمانه»که دایره شمول عامتری نسبت به جرایم داخلی دارد، واجد اهمیت فراوانی است.گرچه عواملی چون اصل حاکمیت ملی،مانع ازاعمال مجازات‌های مصطلح، بر دولت‌های مجرم شده و نیز باعث می‌شود«جرم‌شناسی جرایم دولتی، همواره برجرایم ارتکابی درگذشته متمرکزشود»(قورچی بیگی،۱۳۹۵: ۳۱۹) ولی این امر،نه تنها فرصت‌هایی راکه از رهگذرمکتب آسیب اجتماعی‌شناسی درجهت مفهوم‌شناسی جرایم حقوق بشری دولت‌ها، عایدجرم‌شناسی شده است،سلب نمی‌کند بلکه راه را جهت ارائهٔ نظریه‌های علت شناختی موضوع و درنتیجه بروز شاخه‌های تخصصی جرم‌شناسی درآینده، هموار می‌سازد.

نتیجه‌گیری

امروزه دولت‌ها جهت پیشگیری ازجرایم فضای مجازی، به پالایش آن روی می‌آورند.این اقدام به علت داشتن برخی قابلیت‌ها، می‌تواند به‌عنوان یک تدبیر فنی پیشگیری وضعی ازجرم ایفای نقش نماید. ولی همچون دیگر تدابیر پیشگیرنده موقعیت‌مدار با ایراداتی مواجه است. یکی ازآن ایرادات به‌صورت جابجایی شیوهٔ ارتکاب جرم خودنمایی می‌کند. در واقع زمانی‌که مجرم به‌دلیل پالایش، ازدسترسی به محتوای مجرمانه یا ارتکاب جرم به شیوهٔ خاص منع می‌گردد، جهت رسیدن به

اهداف خود، ازاسلوب دیگری استفاده خواهدنمود.پس پالایش، دست‌کم درمجرمان قاصد مؤثرواقع نمی‌شود.زیرا آنان بلافاصله ازطریق نصب ضدپالایش، ازپالایشگرها عبورمی‌کنند. می‌توان گفت این مشکل ناشی ازایرادی است که بیشترجنبه فنی دارد، در واقع عدم ارتقای فن‌آوری‌های مربوط به پالایش ازیک‌سو ومجهز بودن مرتکبین به آخرین دستاوردهای علمی ازسوی دیگر، یکی ازعوامل ناکارآمدی پالایش درپیشگیری از وقوع جرم است.

وانگهی ضعف پالایش درتحت پوشش قراردادن تمام مصادیق مجرمانه (پالایش کمتر ازحد)، عامل دیگری دراین راستاست.چون موجب می‌شود مجرمین ازطریق پروتکل‌های فیلترنشده دیگر به محتوای مجرمانه دست یابند.تبعات پالایش بیش ازحد، به مراتب از موارد اخیر بیشتر است، زیرا محتواهای مجاز را نیز در برگرفته و درنتیجه موجب مداخله غیرضروری در آزادی‌های مدنی نظیرحق آزادی بیان می‌شود. با این حال چنین مداخلاتی به‌طور ناخواسته رخ می‌دهد و چه بسا با ارتقای فنون پالایش رفع گردد.

مهم‌ترین آسیب‌هایی که باپالایش رخ می‌نماید، تعرض عمدی دولت‌ها به حقوق بنیادین، ازطریق پالایش غیراصولی است، بدین نحوکه برخی دولت‌ها عمدا با توسعهٔ دامنه مصادیق مجرمانه ازطریق پالایش افراطی و صرفا با استناد به اصل«قانون‌مندی»، حقوق بنیادین شهروندان را نقض می‌کنند. بدیهی است چنانچه اقدام به پالایش بدون رعایت مؤلفه‌های لازم، به‌صورت بی‌رویه و فقط با تکیه برقانون 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 نحوکه ازیک طرف با فراهم ساختن امکان زیرنظرگرفتن فعالیت‌های شهروندان درفضای مجازی و درنتیجه ضبط و نگهداری برخی محتواهای مبادله شده توسط آنها، حریم خصوصی مراسلات و داده‌های شخصی کاربران را تضعیف خواهد نمود. ازطرف دیگر با ایجاد ممنوعیت در دسترسی کاربران به برخی اطلاعات برخط و یا باجلوگیری ازامکان تبادل و انتشارچنین محتواهایی دراینترنت، حق آزادی بیان و اطلاعات آنها را نقض خواهدکرد.

آسیب‌های ناشی از این تعرضات به حقوق بنیادین، نمی‌تواندصرفا به‌دلیل متصف نشدن به عناوین مجرمانه، ازمطالعه حقوقی خارج افتد بلکه می‌تواند درقالب پدیدهٔ مجرمانه که دایره شمول عامتری نسبت به جرایم دارد، به چالش کشیده شود. چراکه در بیشترموارد، این آسیب‌ها به این دلیل که محصول یکه‌تازی حکومت‌های اقتدارگرا برحقوق مخالفین خود جهت به انزوا کشیدن آن‌ها می‌باشد، تبعات زیانبارتری نسبت به جرایم مندرج درقانون دارند.به‌طوری که امروزه توجه به آسیب‌های ناشی ازچنین اقداماتی، اذهان جرم‌شناسان را به توصیف جرایم دولتی رهنمون ساخته است. بنابراین ازاین نگاه حکومت‌ها، دیگر نهادهای مقدس عاری ازمسئولیت قلمداد نمی‌شوند بلکه

درمقابل پیامدهای زیان‌بار ناشی ازعملکردخود مسئول هستند و سوءاستفاده آنها ازاختیارات خود، مبنی براستفاده ابزاری ازاصل قانونی بودن جرم و مجازات درتوسعهٔ دامنه محتوای مجرمانه و درنتیجه اعمال پالایش غیراصولی، باعث خواهد شد حقوق شهروندان به‌صورت ساختارمند نقض شده وآسیب‌های جدی بدان واردآید.

گرچه این آسیب‌ها عمدتا به علت موانعی چون حاکمیت ملی، عنوان مجرمانه ندارد ولی می‌تواند از منظرجرم‌شناسی انتقادی بارویکرد آسیب اجتماعی‌شناختی مورد بررسی قرارگیرد.پس اگرحکومت‌ها درجرم‌انگاری محتوای مجرمانه و پالایش آن،گشاده‌دستی به خرج داده و با پالایش گسترده و غیراصولی حقوق شهروندان را نقض نمایند، نمی‌توانند از زیربارمسئولیت ناشی از اعمال زیانبارخود، شانه خالی نمایند بلکه درسطح فراملی و در ارزیابی‌های حقوق بشری به حکومت‌های غیردمکراتیک شهره خواهندشد. فلذا همانطوری که فقدان قانون داخلی مبنی برجرم‌انگاریِ آسیب‌های منتج ازپالایش، اعمال ضدحقوق بشری ناشی ازآن را توجیه نخواهدکرد، همچنین پیش‌بینی مصادیق مجرمانه پالایش شده درقانون، موجبات مصونیت دولت‌ها را فراهم نخواهدساخت.

ازاین‌روحکومتی که مدعی مردم‌سالاری است و به حقوق بنیادین بشری ارج می‌نهد، بایدجهت اعمال پالایش اصولی، علاوه براصل«قانون‌مندی»، همچنین به ضوابط دیگری که در اسناد حقوق بشری جهانی ومنطقه‌ای جهت تحمیل هرگونه محدودیت برحقوق بنیادین، لازم دانسته شده است، پایبند باشد تا به ناقض حقوق بشرشهره نگردد. براساس اسنادفوق، اعمال محدودیت برحقوق بنیادین و ازجمله پالایش، باید واجد جامع شرایط زیرباشد: به موجب قانون شفاف و قابل فهم مقررشود. مبنای وضع قانون بیشتر برضابطه ضرر استوار باشد و برضوابط دیگرچون پدرسالاری قانونی و اخلاق‌گرایی جز درشرایط استثنایی تکیه نشود. در واقع مداخله قانون‌گذار باید حداقلی باشد. یک یا چندمورد از اهداف مشروعی را که دراسناد بین‌المللی یا قوانین داخلی تصریح شده است، دنبال نماید. از قبیل احترام به حقوق دیگران، حفظ نظم یا امنیت ملی، پیشگیری ازجرم، حمایت از اخلاق وسلامت جامعه. ضرورت داشته باشد. یعنی ازمیان تدابیرمتعددی که می‌تواند اهداف مشروع مورد نظر را تأمین نماید، بایدکمترین لطمه را به آزادی‌های افراد بزند. بدین منظور، باید میزان تأثیر پالایش برحقوق بنیادین روشن شود و محدودیت‌های تحمیل شده براین حقوق، بتواند با حفظ منافع ناشی ازپالایش جبران شود به‌طوری که ارزش منفعت موردحمایت، نسبت به حق مورد مداخله بیشترباشد و هیچ روش دیگری غیراز پالایش، که محدودیت کمتری درحقوق شهروندان ایجادکرده و برای رسیدن به هدف مورد نظر مطلوب‌ترباشد، وجود نداشته است.

پالایشِ ضروری، باید مناسب با هدف مورد نظر باشد.بدین معنا که هم معلوم گرددکه حقوق خاصی درخطراست و تضمین آن جز با اعمال پالایش ممکن نیست و هم احرازشود پالایش ازلحاظ فنی قابلیت تأمین هدف موردنظر را دارد.چنانچه مشخص شودکاربران بانصب ضدپالایش یا ازطریق توسل به پروتکل‌های دیگر، به محتواهای فیلتر شده دست پیدا خواهندکرد، پالایش باوجود داشتن دوشرط اول، به علت عدم کارآیی، غیرضروری و نامتناسب قلمدادخواهد شد.

بدیهی است به منظور احراز این شرط، دربیشتر موارد باید مطالعات و بررسی‌های کارشناسانه‌ای انجام شود تا ازکارکرد 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 ازکارکرد پالایش درتأمین اهداف مورد نظراطمینان 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 قلمدادشدن 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 کارشناسی‌ارشد 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 آشکارحقوق بشر»، ترجمه حامدصفایی 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 صابرنژاد، 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 اسنادحقوق بشری»، **آموزه‌های حقوق کیفری**، دوره هفدهم، شماره ۱۹، صص. ۳۵-۶۷ .

حسین پور، پری و صابرنژاد، 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. ۱۹۹-۲۱۸.

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

روث،داون 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.۶۷-۹۸.

سلیمی، احسان (۱۳۹۷)، «**آسیب اجتماعی‌شناختی پیشگیری ازجرایم سایبری درایران**»، 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. ۸۴-۹۷.

فردریش، دیوید (۱۳۹۶)، «به سوی جرم‌شناسی جنایات بین‌المللی: ارائه چهارچوب مفهومی و مبنایی»، ترجمه مهدی کاظمی جویباری، در: **جرم شناسی فراملی به سوی جرم‌شناسی جنایات بین‌المللی**، به کوشش حمیدرضا نیکوکار، چاپ اول، تهران: میزان.

فرهادی‌آلاشتی، زهرا (۱۳۹۵)، **پیشگیری وضعی از جرایم سایبری: راهکارهاو 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. ۳۲۴-۳۰۴.

کلارک، آر.وی.جی (۱۳۸۸)، **جرم‌شناسی پیشگیری**، ترجمه مهدی مقیمی و مهدیه تقی‌زاده، تهران: نشر زرد.

کوچ‌نژاد، عباس (۱۳۸۳)، «محدودیت‌های حقوق بشردر اسناد بین‌المللی»، **حقوق اساسی**، سال دوم، شماره سوم، صص. ۱۶۹-۱۷۸.

کوزلاریچ، دیوید؛ مائتو،ریک؛ جی‌میلر، ویلیام (۱۳۸۹)، «بزهدیده‌شناسی جرایم دولت»، ترجمه قورچی‌بیگی، مجید، **فصلنامه اطلاع رسانی حقوقی**، معاونت تحقیقات، آموزش و حقوق شهروندی، شماره ۲۲-۲۱، صص. ۱۱۷-۱۳۸.

گرین، پنی؛وارد، تونی (۱۳۹۸)، **جرم‌حکومتی، دولت‌ها، خشونت‌وفساد**، 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 نوربها، **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 ازجرم»، در:علوم جنایی، **مجموعه مقالات تجلیل از دکتر محمد آشوری**، چاپ چهارم، تهران: سمت. صص. ۵۵۹-۵۹۸.

نجفی ابرندآبادی، علی حسین (۱۳۹۵)، «ازجرم‌شناسی حقیقی تا جرم‌شناسی مجازی»، دیباچه در:**جرم‌شناسی**، ژرژ، پیکا، ترجمه علی‌حسین نجفی ابرندآبادی، چاپ چهارم، تهران: میزان. صص.۹-۱۷.

نجفی ابرندآبادی، علی حسین (۱۳۹۵)، «جرم‌شناسی درآغازهزاره سوم»، دیباچه در:**دانشنامه جرم‌شناسی** از:علی‌حسین نجفی‌ابرندآبادی و حمید هاشم‌بیگی، چاپ‌چهارم، تهران: انتشارات گنج دانش. صص. ۱۳-۲۸.

ون هام، فرانسواز (۱۳۹۵)، «آسیب اجتماعی‌شناسی :رشته‌ای جدید،توسعه قلمرو جرم شناسی؟»، 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 & Ziekenheiner,Hein (2009), **Internet blocking balancing cybercrime responses in democratic societies,** Open socity Institute, Action internet solutions.

Jaishankar, Karupannan (2008), " Space transition theory of cyber crimes,in book: **crime of the internet,chapter: space Trasition 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)، «پالایش فضای سایبری به مثابه جرم یـا ابـزار پیشـگیری ازآن؟»، **پژوهشـــنامه حقوق کیفری**، دوره ۱۳، پیاپی ۲۶، صص. ۱۶۳-۱۸۷. DOI:10.22124/jol.2022.18816.2078