Modern Technologies Law

University of Science and Culture

http://10.22133/mtlj.2025.468669.1354

The Confluence of Human Rights, Technology and National Security in the Light of the Case-Law of the European Court of Human Rights

Mohammadreza Shakib[1*] **Abbasali Kadkhodaei**[2]

[1] Ph.D. in International Law, Faculty of Law and Political Science, University of Tehran, Tehran, Iran.

[2] Prof., Department of Public Law, Faculty of Law and Political Science, University of Tehran, Tehran, Iran.

Article Info

Original Article

Received:
20-07-2024
Accepted:
13-10-2024

Key Words:
National Security
Margin of Appreciation
Human Rights
European Court of Human Rights
Communication Technologies

Abstract

During its activity, the Strasbourg court has tried to take care in the decisions issued while protecting human rights, in order to play an intermediary role in critical situations when the national security of the member countries of the convention is in danger, so as to be on the side of " human rights " and do not ignore the "national security" of governments. However, what makes the care of human rights a challenge is the complex and advanced "communication technologies" that, on the one hand, allow dangerous criminals (domestic and international) to communicate, coordinate, avoid detection, etc.; and on the other hand, such a possibility deems as a threat to countries security and causes to expand their "discretion" and result in marginalize human rights. The question is, how has the Strasbourg court been able to protect human rights while paying attention to the national security concerns of countries in the challenging issue of the intersection of human rights, technology and security In response, It can be said that The court through the submitted cases, on the one hand, has taken care of, so that governments do not abuse advanced technologies to control people's communications and information or violate their privacy, and on the other hand, according to the possibility Abusing the capacity of technology by law-breaking groups, especially cyber attackers and terrorists, the Court has rushed to the aid of the governments and given them Certain Margin of appreciation to interception to protect their national security.

***Corresponding author**
e-mail: shakib.mohammadreza@gmail.com

How to Cite:
Shakib, S.M., & Kadkhodaei, A. (2025). The Confluence of Human Rights, Technology and National Security in the Light of the Case-Law of the European Court of Human Rights. *Modern Technologies Law*, *6*(12), 309-325.

Published by University of Science and Culture https://www.usc.ac.ir
Online ISSN: 2783-3836

1. Introduction

It is obvious that the protection of human rights is the most important application of the European Court of Human Rights, known as the Strasbourg Court, and the Court has tried to protect European human rights with its brilliant performance in numerous cases. Despite this, one of the issues that leads to the functional limitation of the court is the issue of the security of the member states, which in articles (6, 8 to 11) allow them to take necessary measures when "national security" is endangered. and has given them a degree of "discretion" or "margin of Appreciation" to detect the threat and necessary measures to deal with it. One of the important issues facing the Court is the efforts of member states to deal with threats related to their security interests and possible violations of human rights, and the Court has tried to protect human rights against the excesses of countries in various cases. However, in recent years, due to the growth and development of communication technologies, the security threats facing countries have expanded, and the same issue has had an impact on the Court's approach.

Maybe in the past it was obvious that the threat to a country's security is understood in the context of foreign military threats; But the passage of time and the developments that have taken place have changed this mentality and the scope of the threat to the security of a country has become much wider; In such a way that even the United Nations Security Council approved such a development. In Resolution 1308, the Security Council considers the AIDS virus as a possible threat to stability and security if the necessary care is not taken; or in Resolution 2177 considers the unprecedented spread of the Ebola virus in Africa as a threat to international peace and security; And in Resolution 2565, it declares that the unprecedented spread of the COVID-19 virus may endanger the maintenance of international peace and security. However, according to some, such resolutions are more based on desirable rights than existing rights and their recommendatory nature prevails over their mandatory nature. However, with the emergence of new technologies, the scope of fundamental security interests should be expanded to include cyber, communication and information threats, and as the International Court of Justice has also acknowledged, the concept of fundamental security interests is definitely not limited to armed attack but it is beyond that.

Communication technologies is a word that should not be limited to the Internet and its main role should be to facilitate the reception, transmission, storage, processing and collection of information, which means radio, television, satellite transmitters, e-mail, network Social... can also be considered as an example that such characteristics include positive and negative effects. Among the positive effects of technology, we can mention the provision of suitable solutions for various issues, informing people of their rights, guaranteeing human rights claims, informing about human rights violations, etc., and on the other hand, the negative effects of communication technologies; can count the direction of people's ideas and information or the misuse of its capacities by dangerous groups for subversive actions. Therefore, countries have tried to expand their surveillance-interception field so that the misuse of technological capacities does not harm their national security interests.

In this article, we are looking for an answer to the question of how the Court of Strasbourg can protect human rights in the challenging issue of the intersection of human rights, technology and national security. And what effect has technology had on the court's approach? For this purpose, first (in the second paragraph) we will have a reflection on the narrow and strict approach of the Court; In the following (third paragraph) we will examine the modification of the court's procedure under the influence of the development of communication technologies and after that (fourth paragraph) we will evaluate and analyze the court's procedure.

In domestic law, despite the fact that there are a number of articles and books on human rights, technology and national security separately, there is no work that specifically looks at all three categories together, and it has been the same in foreign research. with the difference that in some articles, human rights and national security have been considered in the procedure of the European Court of Human Rights.

2. Methodology

In this research, we tried to collect and gather information from the primary sources (including laws, regulations, directives, bylaws, judicial decisions, etc.) and secondary sources (such as books and articles, theses, research reports, etc.) in scientific research data centers, official and reputable websites, libraries, and similar resources. At first, we will have a reflection on the narrow and strict approach of the Court; In the following, we will examine the modification of the court's procedure under the influence of the development of communication technologies, and after that (Finally) we will evaluate and analyze the court's procedure.

3. Results and Discussion

Communication technology is not limited to information transfer and one of its important applications is to introduce and guide different topics. If we measure such features in the age of technology, along with issues such as the spread of dangerous people and organizations domestically and internationally, we conclude that strengthening the precautionary approach to technology is a necessity for living in today's world.

In the cases where technology, national security and human rights conflict, the court has not forgotten its position to create a balance. In other words, the court takes care of the passing of the cases so that governments do not abuse advanced technologies to control people's communications and information or violate their privacy or their freedom and other human rights, and on the other hand, in the decisions has shown that the court is not indifferent to the sovereignty of countries, and in cases where law-breaking groups, especially the most dangerous ones, i.e. cyber attackers and terrorist groups, may threaten the security of countries by using technology, it rushes to help the governments. And it did not let them use the capacity of technology to achieve sinister goals and hide themselves under the protection of human rights.

In addition, in all cases, the court has maintained its legal-supervisory role regarding the whole case and has carefully evaluated the challenging actions of the government and has repeatedly stated that it is necessary to provide sufficient guarantees by the governments in order for the court to It should be noted that they have used all their efforts to prevent arbitrary behavior as well as abuse of their supervisory capacity through technology. Also, their actions to reach a legitimate goal and within the framework of the convention were necessary for a democratic society.

Therefore, by considering the public interests and interests of the society on the one hand and individual interests and freedoms on the other hand, the court tries to create a balance between the two and issue a decision depending on the case and according to the facts and circumstances of each case; which has provided the protection of human rights and assured the governments of their national security.

4. Conclusions and Future Research

In general, it seems that the Court, unlike some international courts, has tried to adopt a balanced approach and does not have a strict and one-sided view of the protection of human rights and does not forget its duty to fully comply with the provisions of the Convention, which in some articles, care has considered national security as one of the important duties of the member states.

حقوق فناوری‌های نوین، ۱۴۰۴، ۶(۱۲) https://www.mtlj.usc.ac.ir

حقوق فناوری‌های نوین

http://doi.org//10.22133/mtlj.2025.468669.1354

تلاقی حقوق بشر، فناوری و امنیت ملی در پرتو رویهٔ دیوان اروپایی حقوق بشر

محمدرضا شکیب[1]*، عباسعلی کدخدایی[2]

[1] دانش‌آموختهٔ دکتری حقوق بین‌الملل، دانشکدهٔ حقوق و علوم سیاسی، دانشگاه تهران، تهران، ایران.

[2] استاد، گروه حقوق عمومی، دانشکدهٔ حقوق و علوم سیاسی، دانشگاه تهران، تهران، ایران.

اطلاعات مقاله

مقالهٔ پژوهشی

تاریخ دریافت:
۱۴۰۳/۰۴/۳۰

تاریخ پذیرش:
۱۴۰۳/۰۷/۲۲

واژگان کلیدی:
امنیت ملی
حاشیهٔ صلاحدید
حقوق بشر
دیوان اروپایی حقوق بشر
فناوری‌های ارتباطی

چکیده

دیوان استراسبورگ در طول فعالیت خود تلاش کرده در آرای صادره ضمن پاسداری از حقوق بشر، مراقبت کند تا در مواقع حساس، که امنیت ملی کشورهای عضو کنوانسیون با خطر مواجه می‌شود، نقشی بینابین ایفا کند تا از این رهگذر هم جانب «حقوق بشر» را بگیرد هم به «امنیت ملی» دولت‌ها بی‌توجه نباشد. بااین‌حال، آنچه مراقبت از حقوق بشر را با چالش مواجه ساخته، «فناوری‌های ارتباطی» پیچیده و پیشرفته‌ای است که از یک طرف به جنایتکاران (داخلی و بین‌المللی) امکان ایجاد ارتباط، هماهنگی، اجتناب از شناسایی و... می‌دهد و همچنین، چنین امکانی موجبی است برای کشورها تا به عنوان تهدید امنیت، «دامنهٔ صلاحدیدی» خود را گسترش و حقوق بشر را به حاشیه ببرند. پرسش این است که دیوان استراسبورگ در موضوع چالش‌برانگیز تلاقی حقوق بشر، فناوری و امنیت ملی چگونه می‌تواند به پاسداری از حقوق بشر بپردازد؟ در پاسخ می‌توان گفت که از یک طرف، دیوان از رهگذر پرونده‌های مطروحه مراقبت نموده تا دولت‌ها از فناوری‌های پیشرفته برای کنترل ارتباطات و اطلاعات افراد و تجاوز به حریم خصوصی آن‌ها سوءاستفاده نکنند. از طرف دیگر، با توجه به امکان سوءاستفادهٔ گروه‌های قانون‌شکن (به‌ویژه حمله‌کنندگان سایبری و گروهک‌های تروریستی) از ظرفیت فناوری، دیوان به کمک دولت‌ها شتافته و حاشیهٔ صلاحدید نظارتی کافی به آن‌ها جهت حفاظت از امنیت ملی‌شان اعطا کرده است.

***نویسندهٔ مسئول**

رایانامه: shakib.mohammadreza@gmail.com

نحوهٔ استناددهی:

شکیب، سید محمدرضا، و کدخدایی، عباسعلی (۱۴۰۴). تلاقی حقوق بشر، فناوری و امنیت ملی در پرتو رویهٔ دیوان اروپایی حقوق بشر. حقوق فناوری‌های نوین، ۶(۱۲)، ۳۰۹-۳۲۵.

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

شاپای الکترونیکی: ۳۸۳۶-۲۷۸۳

مقدمه

آشکار است که پاسداری از حقوق بشر مهم‌ترین کاربست دیوان اروپایی حقوق بشر معروف به دیوان استراسبورگ است و دیوان با عملکرد درخشان خود در پرونده‌های متعددی تلاش کرده از حقوق بشر اروپایی صیانت کند. با وجود این، یکی از مسائلی که تا حدی به محدودیت عملکردی دیوان منجر می‌شود، بحث امنیت کشورهای عضو است که در مواد (۶، ۸ الی ۱۱) به آن ها اجازه داده در مواقع به‌خطرافتادن «امنیت ملی»[1]، اقدامات ضروری را اتخاذ کنند و به آن‌ها میزانی از «صلاحدید»[2] یا «حاشیهٔ صلاحدید»[3] برای تشخیص تهدید و اقدامات ضروری برای مقابله با آن اعطا کرده است.[4] یکی از موضوعات مهم پیش روی دیوان، تلاش کشورهای عضو برای مقابله با تهدیدات مربوط به منافع امنیتی‌شان و نقض احتمالی حقوق بشر است و دیوان در پرونده‌های مختلفی تلاش کرده تا از حقوق بشر در مقابل زیاده‌خواهی کشورها محافظت کند. بااین‌حال، در سال‌های اخیر و با توجه به رشد و توسعهٔ فناوری‌های ارتباطی تهدیدات امنیتی که متوجه کشورهاست گسترش یافته و همین موضوع بر رویکرد دیوان نیز بی‌تأثیر نبوده است.

شاید در گذشته بدیهی می‌نمود که تهدید امنیت یک کشور در چهارچوب تهدیدات نظامی خارجی معنا پیدا می‌کند، اما گذر زمان و تحولات صورت گرفته این ذهنیت را تغییر داد و گسترهٔ تهدید امنیت یک کشور به‌مراتب وسعت بیشتری یافت؛ به نحوی‌که حتی شورای امنیت نیز بر چنان توسعه‌ای صحه گذاشت. در قطعنامهٔ ۱۳۰۸ (2000) شورای امنیت ویروس ایدز را درصورت بی‌توجهی به مراقبت‌های لازم، تهدیدی احتمالی علیه ثبات و امنیت تلقی می‌کند (Resolution 1308, 2000, p. 2)؛ یا در قطعنامهٔ ۲۱۷۷ (2014) شیوع بی‌سابقهٔ ویروس ابولا در آفریقا را تهدیدی علیه صلح و امنیت بین‌المللی می‌داند (Resolution 2177, 2014, p. 1). همچنین در قطعنامهٔ ۲۵۶۵ (2021) اعلام می‌دارد که شیوع بی‌سابقهٔ ویروس کووید-۱۹ ممکن است حفظ صلح و امنیت بین‌المللی را به خطر اندازد (Resolution 2565, 2021, p. 2)؛ هرچند به نظر برخی، چنین قطعنامه‌هایی بیشتر مبتنی بر حقوق مطلوب[5] است تا حقوق موجود[6] و ماهیت توصیه‌ای آن‌ها بر ماهیت الزامی‌شان غلبه دارد (Sadat meidiani, 2005, p. 95). بااین‌حال، با ظهور فناوری‌های نوین، دامنهٔ منافع اساسی امنیتی را باید به تهدیدات سایبری، ارتباطی و اطلاعاتی نیز گسترش داد (Farshasaid & Jalali, 2022, p. 175-176) و همان‌طور که دیوان بین‌المللی دادگستری نیز اذعان داشته، مفهوم منافع اساسی امنیتی[7] بی‌شک به حملهٔ مسلحانه محدود نیست و فراتر از آن است (Military and Paramilitary Activities in and against Nicaragua Case, 1986, p. 224).

فناوری‌های ارتباطی واژه‌ای است که نباید آن را به اینترنت محدود دانست و نقش اصلی آن را باید تسهیل دریافت، انتقال، ذخیره، پردازش و جمع‌آوری اطلاعات بدانیم. با این وصف، رادیو، تلویزیون، فرستنده‌های ماهواره‌ای، پست الکترونیک، شبکه‌های اجتماعی و غیره نیز از مصادیق آن تلقی می‌شود (Solhchi & Biparva, 2018, p. 100). چنین ویژگی‌هایی متضمن آثاری مثبت و منفی است. برخی از تأثیرات مثبت فناوری عبارت‌اند از: ارائهٔ راهکارهای مناسب دربارهٔ مسائل متنوع (Shahbazi & Shabani Kolahi, 2024, p. 223)، آگاه‌کردن افراد از حقوق خود، تضمین مطالبات حقوق بشری، اطلاع‌رسانی دربارهٔ نقض‌های حقوق بشری. در مقابل از تأثیرات منفی فناوری‌های ارتباطی

1. National Security
2. Discretion
3. Margin of Appreciation

٤. اصطلاح حاشیهٔ صلاحدید برای اولین بار در گزارش کمیسیون اروپایی حقوق بشر (۱۹۵۸) در دعوای قبرس علیه پرتغال به کار رفت (Greer, 2000, p. 5). لازم به ذکر است که در ادبیات دیوان استراسبورگ بیشتر از عبارت «حاشیهٔ صلاحدید یا حاشیهٔ ارزیابی یا حاشیهٔ تشخیص» (Margin of Appreciation) استفاده می‌شود و در برخی موارد هم واژهٔ «صلاحدید» (Discretion) به کار رفته است و به عقیدهٔ نگارنده، نباید تفاوتی میان این دو قائل بود و علت اینکه عبارت Margin of Appreciation را حاشیهٔ صلاحدید ترجمه کرده‌ایم نیز به‌دلیل آن است که تصور نشود با واژهٔ Discretion تفاوتی دارد. در معنای خاص آن نیز دکترین صلاحدید یا حاشیهٔ صلاحدید به‌طور خلاصه بیانگر اختیار تعیین و تشخیص و آزادی عمل دولت در اتخاذ اقدامات لازم برای حفاظت از منافع ملی‌اش است.

5. Lex ferenda
6. Lex lata
7. Essential Security Interests

می‌توان جهت‌دهی به تصورات و معلومات افراد یا سوءاستفادهٔ گروه‌های خطرناک از ظرفیت‌های آن برای اقدامات خرابکارانه را برشمرد؛ ازاین‌روی، کشورها تلاش کرده‌اند حوزهٔ نظارتی ـ مداخلاتی خود را گسترش دهند تا مبادا سوءاستفاده از ظرفیت‌های فناوری به منافع ملی ـ امنیتی آن‌ها آسیب وارد کند.

در نوشتار حاضر، در پی پاسخ به این پرسش هستیم که دیوان استراسبورگ در موضوع چالش‌برانگیز تلاقی حقوق بشر، فناوری و امنیت ملی چگونه به پاسداری از حقوق بشر می‌پردازد؟ و فناوری چه تأثیری در رویکرد دیوان داشته است؟ بدین منظور، ابتدا (در بند دوم) رویه و رویکرد مضیق و سختگیرانهٔ دیوان بررسی می‌کنیم. سپس (بند سوم) تعدیل رویهٔ دیوان تحت‌تأثیر گسترش فناوری‌های ارتباطی را بررسی می‌کنیم و در ادامه (بند چهارم) به ارزیابی و تحلیل رویهٔ دیوان می‌پردازیم.

۱. ورود فناوری‌های ارتباطی به بررسی‌های دیوان؛ رویکرد سخت‌گیرانه

کنوانسیون اروپایی حقوق بشر[1] را باید سند اصلی پیش روی دیوان استراسبورگ دانست که مفاد آن متضمن رعایت حقوق اساسی و بنیادین بشر است[2]. بااین‌حال، کنوانسیون از واقعیت جامعهٔ بین‌المللی، که بازیگران نقش اول آن را کشورها برعهده دارند، غافل نبوده و در برخی مواد خود (۶، ۸ الی ۱۱) سوپاپ اطمینانی برای کشورها برای تضمین رعایت «امنیت ملی‌شان» پیش‌بینی کرده است. در مادهٔ ۶ استثنایی درخصوص (علنی‌بودن محاکمات)؛ در مادهٔ ۸ استثنایی بر (حق احترام به زندگی خصوصی و خانوادگی)، در مادهٔ ۹ استثنایی بر (آزادی اندیشه، وجدان و مذهب)، در مادهٔ ۱۰ استثنایی بر (آزادی بیان) و در مادهٔ ۱۱ استثنایی بر (آزادی احزاب و تجمعات)، درج شده است و مقررهٔ مربوطه بدین‌نحو نگارش یافته است: «...محدودیتی برای اعمال حقوق [مندرج در مواد ۶، ۸ الی ۱۱] نباید اعمال شود، مگر آنچه در قانون مقرر شده و در یک جامعهٔ دموکراتیک به نفع امنیت ملی، ایمنی جمعی، رعایت نظم عمومی، حفاظت از سلامت و اخلاق عمومی یا برای حمایت از حق آزادی دیگران ضرورت داشته باشد...»

بااین‌حال، مبنای صریح‌تر «حاشیهٔ صلاحدید»[3] دولت در مسائل حقوق بشری اتحادیهٔ اروپا را باید در مادهٔ ۱۵ کنوانسیون اروپایی حقوق بشر جست‌وجو کرد که اشعار می‌دارد: «۱- در زمان جنگ یا سایر وضعیت‌های اضطراری که حیات ملت را تهدید می‌کند، هر دولت معظم متعاهد می‌تواند تا حدی که وضعیت مزبور عمیقاً ایجاب می‌نماید برای تخطی از تعهدات خود اقداماتی را اتخاذ کند؛ مشروط بر آنکه چنین اقداماتی در تعارض با سایر تعهدات بین‌المللی آن دولت نباشد...۳- هر طرف متعاهدی که از مجوز عدول مقرر در این ماده استفاده می‌کند، دبیرکل شورای اروپا را به طور کامل از اقدامات اتخاذی و دلایل مربوطه مطلع خواهد ساخت... .» گفتنی است به موجب این ماده می‌توان از تمامی مواد مندرج در معاهده «تاحدی که به شدت لازم است»[4] عدول کرد و درج چنین عبارتی حاکی از آن است که ضروری‌بودن اقدام دولت با سخت‌گیری بسیار بیشتری ازطریق دیوان ارزیابی می‌شود.

بررسی پرونده‌های دیوان استراسبورگ حاکی از آن است که در اکثر پرونده‌های دیوان، به‌نحوی موضوع حاشیهٔ صلاحدید دولت در حفاظت از امنیت ملی و تقابل آن با حقوق بشر مطرح بوده است. بااین‌حال، رویهٔ حاکم گویای این است که دیوان ضمن تأیید صلاحدید و حق دولت بر

1. Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights), 1950.

۲ کنوانسیون اروپایی حقوق بشر اولین سند منطقه‌ای در راستای حمایت از حقوق بشر است که در ۴ نوامبر ۱۹۵۰ به تصویب رسید و در ۳ سپتامبر ۱۹۵۳ لازم‌الاجرا شد و در آن شهر استراسبورگ (فرانسه) به‌عنوان مقر اصلی مشخص شده است. یکی از ارکان کنوانسیون، دیوان اروپایی حقوق بشر (تأسیس: ۱۹۵۹) است و نظر به محل استقرار به دیوان استراسبورگ نیز مشهور است. حق دادخواهی فردی از نوآوری‌های کنوانسیون است و دیوان مستقیم به ادعاهای نقض حقوق و آزادی‌های مندرج در کنوانسیون رسیدگی می‌کند و بدین‌ترتیب، درجهٔ بالایی از حمایت و حفاظت فردی در کنوانسیون مقرر شده است. نظر به عملکرد درخشان دیوان در طول فعالیت خود، باید آن را یکی از نهادهای پیشرو و اثرگذار منطقه‌ای تلقی کرد که در زمینه‌های حقوق بشری تأثیری فرامنطقه‌ای و جهانی داشته است و در بسیاری از رسیدگی‌های بین‌المللی، به نقطه‌نظرات دیوان توجه شده است.

۳ رک: پانویس شماره ۴.

4. to the Extent Strictly Required

تأمین امنیت ملی‌اش، رویکردی سخت‌گیرانه به این موضوع داشته و بارها به نقش نظارتی خود بر این موضوع تأکید داشته است. دیوان در قضیهٔ مانوساکیس[1] و دیگران علیه یونان بیان داشت:

«حاشیهٔ صلاحدید [دولت] همراه با نظارت اروپایی بوده که هم قانون و هم تصمیمات مربوط به اعمال [صلاحدید] را دربر می‌گیرد. وظیفهٔ دیوان این است که تعیین کند آیا اقدامات اتخاذشده در سطح ملی اساساً و به‌نحو متناسبی موجه بوده است یا خیر» (ECHR, 1996, p. 44). دیوان در قضیهٔ لیلا شاهین عیناً این تحلیل را تکرار و تأیید کرد (ECHR, 2005, p. 110).

در قضیهٔ کاسادو کوکا[2] علیه اسپانیا نیز دیوان ضمن اینکه تأیید نمود وفق رویهٔ دیوان، دولت‌های عضو کنوانسیون از صلاحدید قابل توجهی برخوردار هستند، اظهار داشت «چنان حاشیهٔ صلاحدیدی همراه با نظارت اروپایی بوده که هم قانون و هم تصمیمات مربوط به اعمال [صلاحدید] را دربر می‌گیرد» (ECHR, 1994, p. 50).

تعداد چشمگیری از فعالان حقوق بشر در نقاط مختلف دنیا معتقدند که دیوان استراسبورگ یک دادگاه بین‌المللی موفق بوده که پتانسیل اثرگذاری مثبت بر زندگی مردم را دارد (McKenzie, 2014, p. 5). دیوان از یک طرف با حقوق بشر مندرج در کنوانسیون اروپایی حقوق بشر و اسناد مرتبط با آن، که متضمن اصول و قواعد و حقوق بدیهی و اساسی بشری هستند، مواجه است که وظیفهٔ ذاتی دیوان حمایت از آن‌هاست. همچنین دیوان با کشورهایی با حاکمیت برابر و مستقل مواجه است که تمام تلاش خود را برای پیشبرد منافع ملی و حفاظت از اموری همچون امنیت ملی، نظم عمومی، بهداشت عمومی و... خود به عمل می‌آورند و دیوان باید تمام تلاش خود را برای مراقبت از حقوق بشر در برابر حاکمیت مقتدر و به‌موازات آن احترام به وظیفهٔ ذاتی دولت‌ها در حفاظت از منافع اساسی‌شان را به عمل آورد. حال این مناقشه با عنایت به ورود فناوری و تأثیر آن در حقوق بشر و امنیت ملی کشورها پررنگ‌تر شده است و لزوم دقت نظر بیشتر دیوان را می‌طلبد.

در موضوعات مربوط به امنیت ملی، دیوان صلاحدید قابل توجهی را برای دولت‌های عضو به‌رسمیت می‌شناسد و احترام زیادی که دیوان برای نقش دولت درمورد مسائل مربوط به منافع ملی قائل است، بدین جهت است که دولت در بطن امور است و بهتر از هر نهاد دیگری امکان بررسی امور و تشخیص اقدام لازم برای مواجهه با آن‌ها را در اختیار دارد. بااین‌حال، بررسی رویهٔ دیوان حاکی از آن است که دیوان در طول سال‌ها ضمن توجه به حاشیهٔ صلاحدید دولت‌ها، رویکردی سخت‌گیرانه در قبال توسل به امنیت ملی به‌منظور توجیه نقض حقوق بشر داشته است. در قضیهٔ کلاس[3] و دیگران علیه آلمان، دیوان از عبارت «صلاحدید خاص»[4] درخصوص حق نظارت دولت برای حفاظت از امنیت ملی استفاده کرده و اظهار داشت:

«دربارهٔ تعیین شرایط مربوط به نحوهٔ عمل سیستم نظارتی، دیوان خاطرنشان می‌سازد که قانون‌گذار داخلی از صلاحدید خاصی برخوردار است و قطعاً دیوان جایگزین مقامات ملی در ارزیابی اتخاذ بهترین تدبیر در این زمینه نمی‌شود. با وجود این، بدان معنا نیست که دولت‌های متعاهد از صلاحدیدی نامحدود[5] به‌منظور نظارت مخفی بر شهروندان برخوردارند... و دولت‌های متعاهد نمی‌توانند به نام مبارزه با جاسوسی و تروریسم هر اقدامی را که مناسب می‌دانند اتخاذ کنند» (ECHR, 1978, p. 49).

1. Manoussakis and others
2. Casado Coca
3. Klass and others

٤. به نظر می‌رسد استفاده از عبارت «Certain Discretion» را می‌توان به این دلیل دانست که از منظر دیوان، دولت واجد میزانی از صلاحدید است که بسته به مورد، کم یا زیاد می‌شود. برای مثال درخصوص تنظیم مقررات و امور مشابه آن، دولت از صلاحدید قابل توجهی برخوردار است؛ بااین‌حال نباید تصور شود چنین صلاحدیدی نامحدود است. به همین خاطر دیوان از واژهٔ «Certain» استفاده می‌کند که هم بیانگر میزان درخور توجهی از صلاحدید است و درعین‌حال گویای حد ومرز داشتن چنین صلاحدیدی است؛ ازاین‌روی هم می‌توان آن را «صلاحدید خاص» و هم می‌توان «میزانی از صلاحدید» ترجمه کرد.

5. Unlimited Discretion

در قضیهٔ سی‌جی[1] و دیگران علیه بلغارستان، دیوان بیان داشت که «امنیت ملی مفهومی است بسیار گسترده که دامنهٔ صلاحدید زیادی را در اختیار مقامات اجرایی قرار می‌دهد که تشخیص دهند چه اقدامی به نفع چنان امنیتی است؛ اما این امر بدان معنا نیست که اختیار دولت آنچنان گسترده است که به"ورای معنای طبیعی"[2] این مفهوم گسترش یابد» (ECHR, 2008, p. 43).

در قضیهٔ زابو و ویسی[3] علیه مجارستان، دیوان با تأیید استدلال شعبهٔ دیوان در قضیهٔ رومن زاخاروف علیه روسیه (با کمی تغییر) بیان داشت:

«این یک نگرانی جدی است که مفهوم "افراد مرتبط شناسایی شده... به عنوان طیفی از افراد" ممکن است به واقع شامل هر فردی گردد و به‌مثابهٔ همراه ساختن راه برای نظارت نامحدود بر تعداد زیادی از شهروندان تعبیر گردد و عدم وجود هرگونه توضیحی در قوانین داخلی درخصوص چگونگی اعمال این مفهوم [نیز دلیلی بر این یافتهٔ دیوان است]» (ECHR, 2016, p. 65).

دیوان مذکور در خصوص استفاده از فناوری‌های پیشرفته اظهار داشت:

«با توجه به... پتانسیل فناوری‌های نظارتی پیشرفته جهت تجاوز به حریم خصوصی شهروندان، دیوان معتقد است که شرط "ضروری بودن در یک جامعهٔ دموکراتیک" باید در این خصوص یک "ضرورت محض"[4] تلقی شود» (ECHR, 2016, p. 73).

در پروندهٔ ایورداشی و دیگران علیه مولداوی، شعبهٔ بدوی دیوان بند ۹۴ دیگر رأی دیوان در قضیهٔ وبر و ساراوییا[5] علیه آلمان را عیناً تکرار و تأیید کرد که آمده بود:

ازآنجاکه اجرای اقدامات نظارت مخفی بر ارتباطات در عمل قابلیت بررسی توسط افراد ذی‌نفع یا عموم مردم را ندارد، صلاحدید قانونی اعطایی به قوهٔ مجریه یا قاضی، در قالب قدرتی نامحدود، با حاکمیت قانون مغایر خواهد بود؛ درنتیجه قانون باید دامنهٔ هرگونه صلاحدید اعطایی به مقامات و نحوهٔ اعمال آن را به‌وضوح مشخص کند تا از فرد در برابر مداخلهٔ خودسرانه حمایت کند (ECHR, 2009, p. 39). همین دیدگاه را دیوان اروپایی در قضیهٔ زابو و ویسی علیه مجارستان تأیید کرد (ECHR, 2016, p. 67).

در قضیهٔ مالون[6] علیه انگلیس دیوان اظهار کرد:

«بدون تردید وجود برخی قوانین که اختیارات شنود ارتباطات را به منظور کمک به پلیس در امر تحقیقات و کشف جرم اعطا می‌کند، می‌تواند ذیل عبارت مقرر در بند ۲ مادهٔ ۸ [کنوانسیون یعنی] "در یک جامعهٔ دموکراتیک... برای پیشگیری از اختلال در نظم و ارتکاب جرم... ضروری باشد" قرار گیرد. بااین‌حال، اعمال چنین اختیاراتی به‌دلیل محرمانه‌بودن ذاتی آن خطر سوء استفاده ... را در پی دارد ... و تنها درصورتی می‌توان آن را برای یک جامعهٔ دموکراتیک ضروری تلقی کرد که سیستم نظارت مخفی اتخاذی، دارای تضمین‌های کافی در برابر سوء استفاده باشد» (ECHR, 1984, p. 81).

در قضیهٔ وبر و ساراوییا علیه آلمان، درنهایت دیوان به این نتیجه رسید که «تضمین‌های کافی و مؤثر در برابر سوء استفاده از اختیارات نظارتی وجود دارد ... و با عنایت به اینکه خوانده صلاحدید نسبتاً گسترده‌ای در خصوص موضوع پرونده دارد، حق مداخله در محرمانه‌بودن ارتباطات از راه دور ... بنا به دلایل مربوط به امنیت ملی و به منظور پیشگیری از وقوع جرم را داشته است ... و بنابراین مادهٔ ۸ کنوانسیون نقض نشده است» (ECHR, 2006, p. 137-138).

بنابراین، دیوان سال‌ها با مسئلهٔ فناوری و ارتباط آن با حقوق بشر و امنیت ملی کشورها مواجه بوده است و بررسی رویهٔ دیوان گویای سخت‌گیری زیاد درخصوص استناد دولت‌ها به امنیت ملی تحت‌تأثیر فناوری‌های ارتباطی ـ اطلاعاتی به‌منظور توجیه نقض حقوق بشر است و توجه به «ضرورت محض» را باید اوج سخت‌گیری دیوان تلقی کرد. بااین‌حال، پیچیدگی و پیشرفت روزافزون فناوری، دیوان را قانع ساخت تا

1. C. G. and others
2. Natural Meaning
3. Szabó and Vissy
4. Strict Necessity
5. Gabriele Weber and Cesar Richard Saravia
6. Malone

کمی از نگاه سختگیرانه و مضیق خود فاصله گرفته و با تعدیل رویکرد خود به نفع امنیت ملی کشورها، خود را همسو با تغییروتحولات سریع جامعهٔ بین‌المللی وفق داد. در ادامه به بررسی تعدیل در رویهٔ دیوان می‌پردازیم.

۲. پیشرفته و پیچیده‌شدن فناوری های ارتباطی؛ تعدیل رویکرد دیوان

دولت‌ها به علت یا به بهانهٔ تهدیدات تروریستی و به‌ویژه پس از وقایع ۱۱ سپتامبر، نظارت زیادی بر ارتباطات الکترونیکی افراد داشته‌اند و اسنادی که اسنودن[1] افشا کرد مؤید آن است (Christakis & Bouslimani, 2019, p. 1). از زمان اولین رأی دربارهٔ «قوانین نظارت»[2] در سال ۱۹۷۸ و در پروندهٔ کلاس علیه آلمان، دیوان اروپایی حقوق بشر رویهٔ قضایی مستحکمی درمورد نظارت مخفی توسعه داده است (Christakis & Bouslimani, 2019, p. 3). موضع مستمر دیوان این بوده که اقدامات نظارتی می‌تواند در مبارزه با تروریسم ضروری باشد. برای مثال در رأی زابو و ویسی علیه مجارستان، دیوان تأکید کرد که «این نتیجهٔ طبیعی اشکال [متفاوت و متنوع] تروریسم در دوران کنونی است که دولت‌ها برای پیشگیری از چنین حملاتی به فناوری‌های پیشرفته، ازجمله نظارت گسترده بر ارتباطاتی که بالقوه حاوی نشانه‌هایی از حوادث قریب‌الوقوع است، متوسل شوند» (ECHR, 2016, p. 68).

از سال ۲۰۱۸ و در دو قضیهٔ معروف سنتروم فور راتویسا[3] علیه سوئد (زین پس سنتروم) و بیگ برادر واچ[4] و دیگران علیه انگلیس (زین پس بیگ برادر) و همچنین رأی شعبهٔ عالی در هر دو قضیه، که در سال ۲۰۲۱ صادر شد، شاهد بودیم که تهدید روزافزون امنیت کشورهای عضو توسط فناوری، موجب تعدیل رویکرد سختگیرانهٔ دیوان شد. به‌عبارت‌دیگر دیوان، که نگاهی مضیق به «حاشیهٔ صلاحدید» دولت برای اتخاذ تصمیم درخصوص «وجود وضعیت اضطراری» داشت و در سال ۲۰۱۶ و با معیار «ضرورت محض» این سخت‌گیری به اوج خود رسیده بود، از سال ۲۰۱۸ و در دو قضیهٔ سنتروم و بیگ برادر رویکرد خود را کمی منعطف کرد و با فاصله از معیار ضرورت محض تأیید داشت که سیاست نظارت گسترده به‌عنوان «ابزاری ارزشمند»[5] برای حفاظت از امنیت ملی تلقی می‌شود (ECHR, 2018a, p. 112; ECHR, 2018b, p. 385). شعبهٔ عالی دیوان در قضیهٔ بیگ برادر همسو با شعبهٔ بدوی، به‌طور گسترده ماهیت تهدیدهای مدرنی را که ناشی از فناوری‌های جدید و پیشرفت‌های مربوط به آن است توصیف کرد و توضیح داد که رهگیری گسترده تا چه حد ممکن است در شناسایی و پیشگیری از چنین تهدیداتی مفید واقع شود (ECHR, 2021a, p. 168).

قضیهٔ بیگ برادر مربوط به برخی جنبه‌های برنامهٔ نظارتی انگلستان بود که به نقض حق بر حریم خصوصی و حق بر آزادی بیان مشکوک بود. این برنامه دولت انگلیس را قادر می‌ساخت تا داده‌های ارتباطی را به‌صورت وسیع رهگیری کند، داده‌هایی را از ارائه‌دهندگان خدمات ارتباطی به دست آورند و مطالبی را از سرویس‌های اطلاعاتی خارجی دریافت کنند و همهٔ این موارد درحالی بود که برنامهٔ مذکور صلاحدید گسترده‌ای به دولت اعطا کرده بود. در قسمت مهمی از رأی که بیانگر صلاحدید گسترده به‌ویژه با توجه به پیچیدگی فعالیت‌های خطرناک با بهره‌گیری از فناوری است، شعبهٔ عالی بیان داشت: «دیوان می‌پذیرد که رهگیری انبوه برای کشورهای متعاهد در شناسایی تهدیدات امنیت ملی آن‌ها اهمیت حیاتی[6] دارد... و موضع اتخاذی دولت خوانده و دولت‌های وارد ثالث مانند فرانسه و هلند نیز چنین بود.» در ادامه دیوان با تأیید ضمنی رهگیری انبوه ارتباطی ـ اطلاعاتی بیان داشت: «شناسایی تروریست‌ها، جنایتکاران و سرویس‌های اطلاعاتی متخاصم خارجی توسط ابزارهای سنتی به‌نحو فزاینده‌ای پیچیده [و سخت] شده است؛ مضاف بر اینکه ماهیت اینترنت جهانی بدان معناست که مسیری که یک ارتباط خاص طی می‌کند به‌شدت پیش‌بینی‌ناپذیر است» (ECHR, 2021a, p. 424).

1. Edward Snowden
2. Surveillance Laws
3. Centrum för Rättvisa
4. Big Brother Watch and others
5. Valuable Means
6. Vital Importance

همچنین در این قضیه[1] دیوان اظهار داشت:

«[در قضیهٔ وبر و ساراوییا] (European Court of Human Rights, 2006, p. 106) دیوان صراحتاً تأیید کرد که مقامات ملی در انتخاب بهترین روش جهت نیل به هدف مشروع امنیت ملی، از حاشیهٔ صلاحدید گسترده‌ای برخوردار هستند. علاوه‌براین، در دو قضیهٔ وبر و ساراوییا و همچنین لیبرتی[2] و دیگران، دیوان پذیرفت که نظام‌های رهگیری انبوه فی‌نفسه خارج از چهارچوب حاشیهٔ صلاحدید دولت قرار نمی‌گیرند. با اینکه از عمر هر دو پروندهٔ اشاره شده بیش از ده سال می‌گذرد، اما با توجه به استدلال دیوان در آن احکام و با توجه به تهدیدات فعلی که بسیاری از کشورهای متعاهد با آن مواجه هستند (ازجمله مصیبت تروریسم جهانی و سایر جرائم مهم مانند قاچاق مواد مخدر، قاچاق انسان، بهره‌کشی جنسی از کودکان و جرائم سایبری) [و با توجه به] پیشرفت‌های فناوری، که امکان فرار تروریست‌ها و مجرمان از شناسایی در اینترنت را آسان کرده است و [همچنین] پیش‌بینی‌ناپذیربودن مسیرهایی که ازطریق آن ارتباطات الکترونیکی منتقل می‌شود، دیوان معتقد است که تصمیم اجرای یک نظام شناسایی وسیع به‌منظور شناسایی تهدیدهای ناشناخته برای امنیت ملی، نظامی است که همچنان در محدودهٔ حاشیهٔ صلاحدید دولت‌ها قرار می‌گیرد» (ECHR, 2021a, p. 314).

همسو با قضیهٔ بیگ برادر، در قضیهٔ سنتروم، شعبهٔ عالی دیوان بیان داشت: «شکایت مطروحه مربوط به رهگیری وسیع ارتباطات فرامرزی توسط سرویس‌های اطلاعاتی است ... در عصر کنونی ... اکثر قریب به اتفاق ارتباطات شکل دیجیتالی پیدا می‌کنند ... و به شکلی سریع و ارزان و بدون توجه به مرزهای ملی منتقل می‌شوند؛ بنابراین نظارت و رهگیری که مستقیماً افراد را هدف قرار نمی‌دهد ... می‌تواند دامنهٔ وسیعی داشته باشد ... و برخلاف رهگیری هدفمند، که موضوع پرونده‌های زیادی در دیوان بوده و اغلب برای تحقیق در خصوص جرم بوده است، رهگیری انبوه عمدتاً برای جمع‌آوری اطلاعات خارجی و شناسایی تهدیدهای جدید ... می‌باشد ... و [طبیعی است] دولت‌ها اطلاعات کم و مبهمی در این خصوص در دسترس عموم قرار دهند» (ECHR, 2021b, p. 236). در توضیح کامل‌تر حق دولت بر مراقبت‌های امنیتی، دیوان اظهار داشت:

«قابلیت‌های فناوری حجم ارتباطات منتقل‌شده از اینترنت جهانی را گسترش داده است و متعاقب آن، تهدیدهایی که متوجه دولت‌ها و شهروندانش است نیز افزایش یافته است؛ ازجمله تروریسم جهانی، قاچاق انسان و مواد مخدر، بهره‌کشی جنسی و... . بسیاری از این تهدیدها با دسترسی به فناوری پیچیده امکان‌پذیر است... و قابلیت‌های فناوری باعث شده حتی عملکرد صحیح فرایند دموکراتیک ازطریق حملات سایبری نیز مختل گردد» (ECHR , 2021b, p. 237). در ادامه، شعبهٔ عالی ضمن لزوم وجود تدابیری که از خودسری و سوءاستفاده جلوگیری کند، حق دولت‌ها برای استفاده از ظرفیت فناوری به‌منظور شناسایی تهدیدهای جدید را به رسمیت می‌شناسد.

شعبهٔ بدوی و شعبهٔ عالی دیوان در قضیهٔ سنتروم در خصوص اینکه مداخلهٔ دولت به منظور دستیابی به یک هدف مشروع امری «ضروری برای یک جامعهٔ دموکراتیک» تلقی می‌شود یا خیر نیز به صلاحدید گستردهٔ دولت در انتخاب بهترین روش جهت حفاظت از امنیت ملی به عنوان یک هدف مشروع اشاره نمود (ECHR, 2018a, p. 104, 112; ECHR, 2021b, p. 252). در این راستا شعبهٔ عالی اظهار داشت: سیستم نظارتی سوئد واجد مبنا در قوانین داخلی این کشور است و در پرتو منافع امنیت ملی قابل توجیه می‌باشد. به واقع، با توجه به تهدیدات امروزی تروریسم جهانی و جنایات مهم فرامرزی و همچنین با عنایت به پیشرفت روزافزون فناوری ارتباطات، به زعم دیوان سوئد دارای صلاحدید قابل توجهی (حاشیهٔ صلاحدید گسترده[3] برای تصمیم‌گیری در خصوص راه‌اندازی چنین سیستم رهگیری انبوهی می‌باشد ... هرچند دیوان باید قانع شود تضمین‌های لازم برای جلوگیری از سوء استفاده نیز تعبیه شده است. همچنین شعبهٔ عالی در قسمتی از رأی خود تأکید نمود که رهگیری

---

۱. به‌زعم برخی قضات دیوان، هدف از این قضیه چنین بود که منافع مشروعی که توسط دولت‌ها دنبال می‌شود باید با حقوق بشر و آزادی‌های اساسی، به‌ویژه آن‌هایی که توسط ماده ۸ کنوانسیون حمایت می‌شود، سنجیده شود و از این رهگذر تعادل به وجود آید (Big Brother Watch and others Case, Joint Partly Concurring of Judges Lemmens, Vehabovic and Bosnjak, 2021, p. 168).

2. Liberty and Others

3. Considerable Power of Discretion (“a Wide Margin of Appreciation”)

انبوه فی‌نفسه خارج از دامنهٔ حاشیهٔ صلاحدید دولت نیست [به ویژه آنکه] ... فناوری‌های پیچیده به بازیگران [خطرناک] در عدم شناسایی کمک می‌کند (ECHR, 2021b, pp. 178, 254) .

در پروندهٔ یوزون[1] علیه آلمان نیز دیوان اظهار داشت: «نظارت بر خواهان ازطریق جی‌پی‌اس که به دستور دادستان عمومی فدرال [آلمان] به‌منظور تحقیق درمورد چندین فقره قتل که یک جنبش تروریستی مسئولیت آن را بر عهده گرفته بود و برای پیشگیری از حملات بیشتر، پیشگیری از وقوع جرم و حفاظت از حقوق قربانیان صورت گرفته است، در راستای منافع ملی امنیتی و ایمنی عمومی تلقی می‌گردد. دیوان در تعیین اینکه آیا نظارت بر خواهان ازطریق جی‌پی‌اس در یک جامعهٔ دموکراتیک ضروری بوده است یا خیر، تصریح کرد که مفهوم ضرورت دلالت بر این دارد که با یک نیاز فوری اجتماعی مطابقت داشته و به‌ویژه با هدف مشروع دنبال شده تناسب داشته باشد... و رفتار خواهان نیز بیانگر آن است که سایر روش‌های تحقیق که نسبت به نظارت بر خواهان توسط جی‌پی‌اس از مزاحمت کمتری برخوردار باشند، از کارایی کمتری برخوردار بوده‌اند و بنابراین نقض مادهٔ ۸ کنوانسیون منتفی است» (Uzun v. Germany case, 2010, pp. 77-78, 80).

۳. بررسی و تحلیل رویهٔ دیوان استراسبورگ

با مداقه در رویهٔ دیوان، شاهد تعدیل رویکرد مضیق دیوان، به‌ویژه در دو پروندهٔ سنتروم و بیگ برادر به نفع امنیت ملی کشورها و تحت تأثیر پیچیده و پیشرفته‌ترشدن فناوری‌های ارتباطی، بودیم.

هرچند آرای صادره در قضایای سنتروم و بیگ برادر که توسط شانزده روزنامه‌نگار و سازمان مردم‌نهاد در پی افشاگری‌های ادوارد اسنودن رهبری می‌شد، با احراز نقض کنوانسیون در برخی جنبه‌ها به نبردی هشت‌ساله (از سال ۲۰۱۳ تا ۲۰۲۱) خاتمه داد؛ با این حال، به زعم برخی در بطن خود تجویزی برای حق دولت بر نظارت را نیز در برداشت و همین امر انتقاداتی را متوجه دیوان استراسبورگ نمود (Zalnieriute, 2022, pp. 585 – 592).

قاضی آلبوکوئرک[2] هشدار داد که:

«...در برخی نقاط اروپا سرویس‌های مخفی جسور به‌شدت وسوسه می‌شوند که از شیوهٔ بسیار سست دیوان در تدوین استانداردهای قانونی استفاده کنند و افراد بی‌گناه دیر یا زود بهای آن را خواهند پرداخت.» وی همچنین اظهار داشت: «این رأی به‌طرز چشمگیری تعادل موجود میان حق احترام به زندگی خصوصی و منافع امنیت عمومی را در اروپا تغییر می‌دهد؛ چرا که نظارت غیرهدفمند بر محتوای ارتباطات الکترونیکی و داده‌های ارتباطی مرتبط را می‌پذیرد و بدتر از آن تبادل اطلاعات با کشورهای ثالثی را که از حمایت قابل مقایسه با کشورهای شورای اروپایی برخوردار نیستند نیز تأیید می‌نماید...» (ECHR, 2021a, pp. 179, 200).

همچنین قضات دیوان (لِمنس[3]، وهابوویچ[4] و بوسنیاک[5]) در نظر مشترک خود و در نقدی تلویحی اظهار داشتند:

«شعبهٔ عالی دیوان در رأی خود مجموعه‌ای جامع از اصولی را که با هدف حمایت از حقوق بشر و آزادی‌های اساسی، به‌ویژه آن‌هایی که در مواد ۸ و ۱۰ کنوانسیون ذکر شده‌اند، ترسیم نمود. بااین‌حال، بنا به دلایلی که در این نظر جداگانه توضیح داده شد، اکثریت [قضات] در اعمال تعادل [میان حقوق فردی و منافع اساسی دولت] ارزش مناسبی برای زندگی خصوصی افراد و مکاتباتشان قائل نشدند... می‌توان امیدوار بود در پرونده‌های آتی، که مسائل مربوط به مداخلهٔ جدی در حقوق افراد خاص مطرح می‌گردد، دیوان اصول را به‌نحوی تفسیر و توسعه دهد که به درستی از جامعهٔ دموکراتیک و ارزش‌های آن، که اساس و مبنای وجودی دیوان هستند، حمایت کند» (ECHR, 2021a, p. 168).

1. Uzun
2. Pinto De Albuquerque
3. Lemmens
4. Vehabovic
5. Bosnjak

به عقیدهٔ ما، هشدار قضات دیوان قابل تأمل و از برخی زوایا صحیح است؛ اما با تغییر و تحولات جهان امروز همسو نیست. به‌عبارت‌دیگر، هرچقدر دست دولت‌ها در نظارت بر ارتباطات بسته باشد، دامنهٔ عمل گروه‌های جنایتکار مانند تروریست‌ها گسترده‌تر خواهد شد. مضاف بر آنکه، نباید به نگرانی‌های امنیتی دولت‌ها بی‌اعتنا بود و تنها مراقب دغدغه‌های حقوق بشری بود و دیوان دیر یا زود باید نشان می‌داد که در کنار حقوق بشر، مراقب منافع امنیتی کشورهای متعاهد نیز هست و در قضایای بیگ برادر و سنتروم، این موضوع به‌درستی نشان داده شد. به‌واقع، دیوان در آرای خود به‌دنبال توازن بوده است و در آرای اخیر، ایجاد توازن در شرایطی که تلاقی میان امنیت، حقوق بشر و فّناوری صورت گرفته بود، به امری مناقشه‌برانگیز تبدیل شد و دیوان سربلند از آن بیرون آمد و از رهگذر این آرا، دیوان در عین مراقبت از حقوق بشر، با شناخت پیچیدگی‌های فناوری، به دغدغه‌های امنیتی کشورها نیز پاسخ مناسب داد.

رویهٔ دیوان به‌سوی بازگذاشتن دست دولت در مقابله با تهدیدات سایبری و گروه‌های خطرناک پیش رفته است؛ اما نباید فراموش کرد که وفق مادهٔ ۸ کنوانسیون، اقدامات دولت در نیل به «هدف مشروعی» که به دنبالش است بایستی «برای یک جامعهٔ دموکراتیک ضروری» باشد و این ضرورت ازطریق دیوان به دقت بررسی می‌شود تا دولت از حاشیهٔ صلاحدید خود فراتر نرفته باشد. به‌واقع دیوان باز هم نقش متوازن‌ساز خود را، که به نفع حقوق بشر سنگینی می‌کند، کنار نگذاشته است و صرفاً به‌دنبال این بوده تا از تغییرات سریع صورت‌گرفته در جامعهٔ بین‌المللی که تحت‌تأثیر فناوری‌های جدید و پیشرفته است غافل نباشد؛ بنابراین دیوان سعی کرده به حاکمیت کشورها احترام گذاشته و تدبیر امور مربوط به منافع ملی را بر عهدهٔ خودشان بگذارد. درعین‌حال نظارت‌های حقوقی لازم را نیز به عمل آورد تا از نقض حقوق بشر نیز جلوگیری کند.

همچنین باید توجه داشت که حقوقی مانند منع شکنجه، منع برده‌داری، آزادی عقیده (نه ابراز آن) از حقوق مطلق بشری به‌شمار می‌روند؛ ازاین‌روی، شکنجه یا بازخواست عقاید افراد به بهانه‌هایی چون حفظ نظم عمومی یا امنیت ملی، مجاز نیست (Ghari S Fatemi, 2003, pp. 187, 189). بنابراین، آنچه در سطور گذشته از رویهٔ دیوان اروپایی درخصوص امنیت ملی از نظر گذشت، صرفاً متوجه حقوق بشری مشروط یا مقید است؛ چراکه نقض حقوق مطلق بشری، حتی به دلایل امنیت ملی، اساس و بنیان حقوق بشر را زیر سؤال می‌برد.

ارزیابی آرای دیوان نشان‌دهندهٔ این است که محکمهٔ مذکور، هم به این مهم توجه داشته که فناوری‌های جدید ممکن است به تهدیدهای جدید و پیچیده منجر شوند و از طرف دیگر تهدیدهای جدید و پیچیده ممکن است بر فناوری‌های پیشرفتهٔ کشورها، که حاصل سال‌ها تلاش و صرف هزینه‌های هنگفت است، اثر منفی بگذارد؛ بنابراین لازم است از هر دو زاویه به فناوری نگاه کرد. یک زاویه، احتیاط در برابر فناوری‌ها و احتمال استفاده از آن‌ها به‌منظور تهدید کشورهاست و زاویهٔ دیگر، حفاظت از خود فناوری‌های پیشرفته است.

همچنین باید مراقب بود کشورها نیز از فناوری‌های پیشرفته علیه حقوق بشر استفاده نکنند. ازاین‌روی، دیوان بارها بر اهمیت تضمین‌های کافی در برابر سوءاستفاده و خودسری صحه گذاشته است و تعدیلِ صورت‌گرفته در دو قضیهٔ سنتروم و بیگ برادر خلاف رویهٔ متوازن دیوان نیست. در همین دو پرونده نیز سخت‌گیری و اختلاف نظر میان شعب بدوی و عالی دیوان ملاحظه می‌شود. در قضیهٔ سنتروم شعبهٔ بدوی درنهایت بیان داشت:

«...با عنایت به حاشیهٔ صلاحدید دولت در حفاظت از امنیت ملی... و [با توجه به اینکه] در قوانین سوئد تضمین‌های کافی و مؤثر در برابر خودسری و سوءاستفاده موجود بوده... [بنابراین] اقدامات صورت‌گرفته ضروری در یک جامعهٔ دموکراتیک تلقی می‌گردد و... نقض مادهٔ ۸ منتفی است» (ECHR, 2018a, p. 181).

بااین‌حال، شعبهٔ عالی با توجه به اصل حاکمیت قانون که صراحتاً در مقدمهٔ کنوانسیون ذکر شده است و به زعم دیوان ذاتیِ موضوع و هدف مادهٔ ۸ است و همچنین با توجه به اینکه تضمین‌های کافی و مؤثر توسط سوئد در برابر خودسری و احتمال سوء استفاده تعبیه نشده است، رأی به نقض مادهٔ ۸ توسط این کشور صادر نمود (ECHR , 2021b, p. 373).

یا اینکه در قضیهٔ بیگ برادر هم دیوان بدوی (ECHR, 2018b, p. 184) و هم شعبهٔ عالی (ECHR , 2021a, p. 156) درنهایت اعلام داشتند که دولت خوانده مادهٔ ۸ کنوانسیون حقوق بشر اروپایی را با توجه به وقایع پرونده نقض کرده است. شعبهٔ عالی قضیهٔ بیگ برادر قانع نشد

که اقدامات نظارتی وسیع انگلیس به آستانهٔ «ضروری بودن برای یک جامعهٔ دموکراتیک» رسیده است (ECHR, 2021a, p. 426). همچنین شعبهٔ عالی به اتفاق آراء اعلام داشت که دستیابی انگلیس به داده‌های ارتباطی از ارائه‌دهندگان خدماتی ناقض مادهٔ ۸ کنوانسیون است؛ زیرا انگلیس ثابت نکرد دسترسی به داده‌ها را صرفاً به‌منظور مبارزه با جرائم مهم تحصیل کرده است. همچنین شنود انبوه ارتباطات و تحصیل داده از ارائه‌دهندگان خدمات به‌دلیل فقدان تدابیر محافظتی از منابع روزنامه‌نگاری و مطالب محرمانهٔ روزنامه‌نگاری موجب نقض مادهٔ ۱۰ کنوانسیون بوده است (ECHR, 2021a, pp. 458, 524-525, 528). بنابراین، نظام اشتراک‌گذاری اطلاعات، که از رهگذر آن مقامات انگلیس مواردی را از سرویس‌های اطلاعاتی خارجی تحصیل می‌کردند، نقض مادهٔ ۸ و ۱۰ کنوانسیون تلقی نشد (ECHR, 2021a, pp. 514, 516).

همچنین در پروندهٔ لیبرتی و دیگران علیه انگلیس دیوان باوجود اینکه صلاحدید فوق‌العاده گستردهٔ[1] دولت را فی‌نفسه مغایر کنوانسیون ندانست؛ اما با توجه به اوضاع و احوال پرونده و به‌دلیل نبود تضمین‌های کافی و مناسب برای جلوگیری نسبت به سوءاستفاده از چنین صلاحدیدی و اینکه نحوهٔ برخورد دولت با اشتراک‌گذاری، ذخیره‌سازی و ازبین‌بردن مطالب رهگیری شده رویه‌ای مشخص نداشته و در دسترس عموم نبوده، به این نتیجه رسید که مادهٔ ۸ کنوانسیون نقض شده است (Liberty and Others v. the United Kingdom Case, 2008, p. 64, 69).

همچنین در قضیهٔ وبر و ساراوییا علیه آلمان، که درخصوص نظارت بر ارتباطات اینترنتی ـ مخابراتی و تأثیر آن در نقض برخی حقوق ازجمله آزادی مطبوعات، محرمانه‌بودن ارتباطات از راه دور و... بود اظهار داشت:

«دیوان مجدداً تأکید می‌کند که هنگام ایجاد توازن میان منافع دولت خوانده در حفاظت از امنیت ملی خود ازطریق اقدامات نظارتی مخفی و شدت مداخلهٔ آن بر حریم خصوصی خواهان، مکرراً مقرر داشته که مقامات ملی از حاشیهٔ صلاحدید نسبتاً گسترده‌ای[2] در انتخاب ابزار [لازم] برای دستیابی به هدف مشروع حفاظت از امنیت ملی هستند... هرچند باید تضمین‌های کافی برای جلوگیری از سوءاستفاده از چنین ظرفیتی توسط دولت وجود داشته باشد ... [مضاف بر این‌که] بررسی چنین مسائلی بستگی به اوضاع و احوال هر پرونده دارد و [و نمی‌توان از قبل قضاوتی نمود یا چهارچوب دقیقی مشخص نمود]» (ECHR, 2006, p.106).

باید خاطرنشان ساخت که این اولین رأی دیوان استراسبورگ است که اشتراک‌گذاری اطلاعات بین‌المللی را قانونی تلقی می‌کند و اهمیت زیادی دارد (Zalnieriute, 2022, p. 592)؛ بنابراین آنچه در این چهار رأی حائز اهمیت است رأی نهایی دیوان‌های رسیدگی‌کننده نیست؛ بلکه استدلال و توضیحات تکمیلی آن‌ها در خلال رأی است که چراغ راه دولت‌ها و دیوان استراسبورگ برای مشروعیت‌بخشی به رهگیری گستردهٔ ارتباطات افراد است.

نتیجه‌گیری

فناوری‌های ارتباطی به انتقال اطلاعات منحصر نیست و از کاربست‌های مهم آن، می‌توان به معرفی و جهت‌دادن به موضوعات مختلف اشاره کرد چنین ویژگی‌هایی را اگر در عصر فناوری در کنار مسائلی مانند گسترش افراد و سازمان‌های خطرناک داخلی و بین‌المللی بسنجیم، به این نتیجه می‌رسیم که تقویت رویکرد احتیاطی در قبال فناوری، لازمهٔ زیست در جهان امروز است.

دیوان در پرونده‌هایی که به‌نحوی تقابل فناوری، امنیت ملی و حقوق بشر مطرح بوده است، موقعیت خود را برای ایجاد توازن فراموش نکرده است. به‌عبارتی، دیوان از رهگذر پرونده‌های مطروحه مراقبت کرده تا دولت‌ها از فناوری‌های پیشرفته برای کنترل ارتباطات و اطلاعات افراد یا تجاوز به حریم خصوصی آن‌ها و یا آزادی و سایر حقوق بشری آن‌ها سوء استفاده نکنند و همچنین در آرای صادره نشان داده که به حاکمیت کشورها نیز بی‌توجه نیست و در مواردی که ممکن است گروه‌های قانون‌شکن، به‌ویژه خطرناک‌ترین آن‌ها یعنی حمله‌کنندگان سایبری و گروهک‌های تروریستی با استفاده از فناوری امنیت کشورها را تهدید کنند، به کمک دولت‌ها شتافته و نگذاشته از ظرفیت فناوری به‌منظور نیل به اهدافی شوم استفاده و خود را زیر چتر حمایتی حقوق بشر پنهان کنند.

1. Extremely Broad Discretion
2. Fairly Wide Margin of Appreciation

مضاف بر آن‌که دیوان در تمامی قضایا نقش حقوقی ـ نظارتی خود نسبت به کلیت پرونده را حفظ کرده و اقدامات چالش‌برانگیز دولت را به‌دقت ارزیابی کرده است و به‌کرات اظهار داشته، ارائهٔ تضمین‌های کافی توسط دولت‌ها لازم است تا برای دیوان محرز شود که آن‌ها تمام تلاش خود برای جلوگیری از رفتارهای خودسرانه و همچنین سوءاستفاده از ظرفیت نظارتی خود را، که از رهگذر فناوری صورت می‌گیرد، به کار گرفته‌اند. همچنین اقداماتشان برای رسیدن به هدفی مشروع و در چهارچوب کنوانسیون برای جامعه‌ای دموکراتیک ضروری بوده است.

بنابراین دیوان با درنظرگرفتن منافع و مصالح عمومی جامعه از یک‌سو و منافع و آزادی‌های فردی از سوی دیگر، تلاش کرده توازنی میان این دو ایجاد کند و بسته به مورد و با توجه به وقایع و اوضاع و احوال هر پرونده، رأیی صادر کند که هم حمایت از حقوق بشر را تأمین کرده باشد و هم به دولت‌ها اطمینان دهد به امنیت ملی آن‌ها بی‌توجه نیست.

منابع

سادات میدانی، سیدحسین (۱۳۸۴). صلاحیت قانون‌گذاری شورای امنیت. تهران: دفتر مطالعات سیاسی و بین‌المللی. مرکز چاپ و انتشارات وزارت امور خارجه.

شهبازی، آرامش و شبانی کلاهی، ساناز (۱۴۰۳). چالش‌های حقوقی حفظ حریم خصوصی در شهرهای هوشمند با نگاهی به حقوق بین‌الملل و حقوق ایران. حقوق فناوری‌های نوین، ۵(۹)، ۲۲۱-۲۳۴. https://doi.org/10.22133/mtlj.2024.407318.1226

صلح‌چی، محمدعلی و بی‌پروا، علی (۱۳۹۷). فناوری‌های جدید ارتباطی و تضمین حقوق بشر، پژوهش حقوق عمومی، ۲۰(۶۰)، ۱۲۴-۹۹. https://doi.org/10.22054/qjpl.2018.23789.1579

فرشاسعید، پرویز و جلالیان، محمود (۱۴۰۱). مسئولیت بین‌المللی دولت‌ها در قبال حملات سایبری عوامل غیردولتی. حقوق فناوری‌های نوین، ۳(۶)، ۱۷۳-۱۸۴. https://doi.org/10.22133/mtlj.2023.367059.1136

قاری سیدفاطمی، سیدمحمد (۱۳۸۲). حقوق بشر در جهان معاصر - دفتر اول: در آمدی بر مباحث نظری (مفاهیم، مبانی، قلمرو و منابع). تهران: انتشارات دانشگاه شهید بهشتی.

Christakis, T., & Bouslimani, K. (2019). National security, surveillance and human rights. In R. Geiss & N. Melzer (Eds.), *Oxford handbook on the international law of global security*. Oxford University Press.

Council of Europe. (1950). *Convention for the protection of human rights and fundamental freedoms (European Convention on Human Rights)*. Link

European Court of Human Rights (ECHR). (1978). *Klass and Others v. Germany* (Application no. 5029/71). Chamber Judgment. Link

European Court of Human Rights (ECHR). (1984). *Malone v. the United Kingdom* (Application no. 8691/79). Chamber judgment. Link

European Court of Human Rights (ECHR). (1994). *Casado Coca v. Spain* (Application no. 15450/89). Chamber Judgment. Link

European Court of Human Rights (ECHR). (1996). *Manoussakis and Others v. Greece* (Application no. 18748/91). Chamber Judgment. Link

European Court of Human Rights (ECHR). (2005). *Leyla Sahin v. Turkey* (Application no. 44774/98). Grand Chamber. Link

European Court of Human Rights (ECHR). (2006). *Gabriele Weber and Cesar Richard Saravia against Germany* (Application no. 54934/00). Judgment. Link

European Court of Human Rights (ECHR). (2008). *C. G. and Others v. Bulgaria* (Application No. 1365/07). Chamber Judgment. Link

European Court of Human Rights (ECHR). (2009). *Iordachi and Others v. Moldova* (Application No. 25198/02). Chamber Judgment. Link

European Court of Human Rights (ECHR). (2016). *Szabó and Vissy v. Hungary* (Application no. 37138/14). Chamber judgment. Link

European Court of Human Rights (ECHR). (2018a). *Big Brother Watch and others v. the United Kingdom* (Applications nos. 58170/13, 62322/14 and 24960/15). Chamber Judgment. Link

European Court of Human Rights (ECHR). (2018b). *Centrum för Rättvisa v. Sweden* (Application no. 35252/08). Chamber Judgment. Link

European Court of Human Rights (ECHR). (2021a). *Big Brother Watch and others v. the United Kingdom* (Applications nos. 58170/13, 62322/14 and 24960/15). Grand Chamber. Link

European Court of Human Rights (ECHR). (2021b). *Centrum för Rättvisa v. Sweden* (Application no. 35252/08). Grand Chamber. Link

European Court of Human Rights (ECHR). (2008). *Liberty and Others v. the United Kingdom*, (Application no. 58243/00), Chamber judgment. Link

European Court of Human Rights (ECHR). (2010). *Uzun v. Germany*, (Application no. 35623/05), Chamber Judgment. Link

Greer, S. (2000). *The margin of appreciation: Interpretation and discretion under the European Convention on Human Rights*. Council of Europe Publishing.

International Court of Justice. (1986). *Military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986*. Link

McKenzie, M. J. (2014). The influence of the European Court of Human Rights on the behavior of national courts in terrorism and national security cases: A case study of supreme courts in Denmark, the U.K., and Spain. *APSA 2014 Annual Meeting Paper*, p. 5. Link

Security Council Resolution 1308. (2000, July 17). Link

Security Council Resolution 2177. (2014, September 18). Link

Security Council Resolution 2565. (2021, February 26). Link

Zalnieriute, M. (2022). Big brother Watch and others v. the United Kingdom. *American Journal of International Law*, *116*(3), 585-592. https://doi.org/10.1017/ajil.2022.35

Lemmens, J., Vehabovic, F., & Bosnjak, D. (2021). Joint partly concurring opinion. In *Big Brother Watch and others v. the United Kingdom* (Applications nos. 58170/13, 62322/14 and 24960/15). Grand Chamber. Link

Pinto de Albuquerque, P. (2021). Partly concurring and partly dissenting opinion. In *Big Brother Watch and others v. the United Kingdom* (Applications nos. 58170/13, 62322/14 and 24960/15). Grand Chamber. Link

[in Persian]

Farshasaid, P., & Jalali, M. (2022). International Responsibility of States for Cyber Attacks of Non-State Actors. *Modern Technologies Law*, 3(6), 173-184. https://doi.org/10.22133/mtlj.2023.367059.1136

Ghari S Fatemi, S M. (2003). *Human rights in the contemporary world - the first book: an introduction to theoretical issues (concepts, foundations, territory and sources)*, First edition, Tehran, Publications of Shahid Beheshti University.

Sadat meidiani, S H. (2005). *Legislative Jurisdiction of the Security Council*, Tehran, Office of Political and International Studies, Printing and Publishing Center of the Ministry of Foreign Affairs.

Shahbazi, A., & Shabani Kolahi, S. (2024). Legal Challenges of Privacy Protection in Smart Cities Considering International and Iranian laws. *Modern Technologies Law*, 5(9), 221-234. https://doi.org/10.22133/mtlj.2024.407318.1226

Solhchi, MA., & Biparva, A. (2018). Effect of Communication Technologies in Respect of Human Rights, *Public Law Research*, 20(60), 99-124. https://doi.org/10.22054/qjpl.2018.23789.1579