Republic of Bulgaria
ECONOMIC
AND SOCIAL COUNCIL

R E S O L U T I O N

on

"Challenges Facing Bulgarian Citizens Due to the Risks of the Global Digital Environment"

(own-initiative resolution)

Sofia, 2019

The President's Board of the Economic and Social Council has decided to develop a resolution on "Challenges Facing Bulgarian Citizens Due to the Risks of the Global Digital Environment".

Bogomil Nikolov, a member of ESC Group III - other organizations, was appointed rapporteur.

At its meeting of 11 July 2019, The Plenary Session adopted the resolution.

ABBREVIATIONS USED

EESC - European Economic and Social Committee

EC - European Commission

EU - European Union

EP - European Parliament

OECD - Organization for Economic Co-operation and Development

AI - Artificial Intelligence

NSI - National Statistical Institute

1. CONCLUSIONS AND RECOMMENDATIONS

1.1. The Economic and Social Council (ESC) notes that in the last 5 years internet usage in Bulgaria has increased, and during this period the number of users of mobile broadband has increased more than 4 times. Children are entering the Internet at an earlier age, and this age is steadily decreasing in our country. At the same time, data show that by the age of 11, nearly 90% of them have already become Internet users.

1.2. ESC finds that the positive trend of penetration and development of Internet access and related technologies create a number of challenges related to the lack of skills for using digital technologies and expose Bulgarian citizens to unknown risks and threats. The latter include: threats to physical safety, especially that of children, to privacy and personal information, card theft and payment fraud; fake news, negative influences and radicalism, etc.

1.3. ESC is concerned that children are exposed to the greatest risk when using social networks. A serious problem, according to ESC, is also the excessive use of the Internet and modern children's addiction to digital devices.

1.4. In this context, ESC recommends that the problems arising from the digitalization and growth of Internet usage in Bulgaria should become the subject of constant targeted attention and implementation of specific measures and integrated policies by the state. These measures should, as a matter of priority, target the socially vulnerable population groups, such as children and senior citizens, who are facing significant risk.

1.5. According to ESC, the opportunities offered by digitization can only be fully realized if the efforts of all concerned national institutions, social partners and civil society structures as well as citizens are united. At the same time, every initiative must pay particular attention to organizing information campaigns in order to create a digital security culture.

1.6. It is a fact that the Internet provides a fertile ground for the application of numerous frauds that are not restricted to any country. The most significant of these are related to e-commerce, false identity and investment fraud.

1.7. In this context, ESC offers a set of measures and initiatives that are far from exhaustive but focus on essential measures and actions that can lead to tangible results.

1.8. In order to limit the risks during shopping from non-EU online merchants, ESC recommends conducting extensive campaigns by control authorities and consumer organizations among consumers about the risks of shopping from non-EU websites. The aim is to inform and educate citizens on how to identify risky websites, how to prevent fraud, how to protect computers and electronic devices from unauthorized access in online commerce, etc.

1.9. ESC emphasizes the importance of concluding agreements between national / European market surveillance authorities and similar authorities in third countries where online shops

are predominantly registered - China, USA, etc., with a view to reaching agreements protecting the consumers when using these shops.

1.10. ESC calls for more robust controls on the safety of products imported from non-EU traders, which implies greater cooperation with customs authorities, online platforms, business and consumer training on product safety issues, etc.

1.11. With regard to cybersecurity, ESC believes that Bulgaria can be actively involved in the work of the European Center for Industrial, Technological and Research Expertise in the Field of Cybersecurity and the Network of National Focal Points established within the EU. According to ESC, it is important to define clear conditions for cooperation and relations between the European Center and the national centers. At the same time, national centers need to be funded by the EU in order to work to reduce existing disparities between European countries.

1.12. ESC believes that any cyber security strategy should also include measures to raise citizens' awareness and increase safe behavior. Therefore, in every initiative, particular attention should be paid to organizing information campaigns in order to build a culture of digital security.

1.13. In this regard, ESC draws attention to the potential of the new Digital Europe Programme in the period 2021-2027 and calls on the Bulgarian institutions to actively explain the opportunities for participation to the social partners and civil society organizations, especially in the priority areas of cybersecurity and deep digital skills. It also emphasizes the importance of developing digital skills and competences to enhance the ability to adapt human resources to changing job and labour market demands.

1.14. ESC also pays special attention to the level of consumer knowledge and skills in dealing with digital technologies, taking into account the particularities of age and social environment. In addition to being aware of their rights, obligations and responsibilities, citizens must have adequate skills to handle digital content. In this sense, ESC believes that the digital literacy initiatives should be encouraged.

1.15. ESC underlines the crucial importance of education and digital skills and recommends that institutions, in collaboration with social partners, work to integrate online literacy and skills into curricula at all stages of education with a focus on risks and appropriate behavior in an online environment.

1.16. According to ESC, financial literacy and education can play an important role in enhancing consumer protection, raising awareness and awareness of digital finances, enhancing financial literacy in the use of digital finance and enhancing overall consumer confidence in it.

1.17. ESC has also in other acts expressed its support for the development of mobile healthcare, which can achieve more equal access to healthcare for people in remote areas. At

the same time, ESC calls for compliance with the safety requirements of mobile healthcare solutions, which would create greater confidence among citizens.

1.18. Artificial intelligence (AI) is rapidly entering the modern economy and is often replacing people in the multiple logistics and customer services sectors. At the same time, there is concern and distrust on the part of citizens whether they will retain control of the machine and control over their own lives. In this regard, ESC calls for the development and adoption of a national AI strategy in the context of the Artificial Intelligence for Europe strategy and as provided for in the Coordinated AI Plan.

2. INTRODUCTION

2.1. The problems and challenges facing citizens and arising from the use of digital and internet technologies in Bulgaria have not been the subject of specialized documents of the Economic and Social Council. Understanding that the primary function and concern of the state is to improve the quality of life of every Bulgarian citizen and to provide adequate social protection for vulnerable groups, ESC believes that the rapid development of digital technologies poses serious challenges for a significant part of Bulgarian citizens.

2.2. In recent years, internet usage in Bulgaria has been increasing systematically. If in 2014 56.7% of households had internet access by 2018 their share reached 72.1%. At the same time, the proportion of people who have never used the Internet is decreasing in the country - 26.7% in 2018, compared to 37.1% in 2014, and 70.6% in 2006.

2.3. In Bulgaria, the growth and development of broadband internet access over the last 5 years is particularly impressive, with the number of mobile broadband users increasing over 4 times during this period. At the same time, the relative share of households with internet access (72.1%) is almost exactly the same as that of broadband access (71.5% for 2018).

2.4. ESC recognizes that these processes are a consequence of both the intensive technological development and the action of a number of state policies outlined in the National Broadband Development Strategy in the Republic of Bulgaria (2012-2015), the National Broadband Infrastructure Plan for the following a generation developed as a programming document for the use of EU funds for the programming period 2014-2020, the National Programme "Digital Bulgaria 2015" and others.

2.5. The high speed of propagation and development of Internet access and related technologies poses a number of challenges for Bulgarian citizens related to the lack of skills in using digital technologies. ESC expresses its concern that for many citizens the use of these technologies is new and they do not even have the minimum qualifications and experience to use them effectively and safely.

2.6. According to ESC, particular attention should be paid to socially vulnerable population groups, such as children and senior citizens, for whom the use of these technologies poses a

greater challenge and/or poses significant risks related to physical safety, economic interests in shopping, exposure to malevolent influences, security of personal data, etc.

2.7. ESC is concerned that children are exposed the greatest risk when using the Internet. While the moderate use of digital technologies may be beneficial for the mental well-being of children, their overuse leads to negative consequences and addiction, not so much to digital devices, but to digital content (video and internet games, forums, etc.), which, when used purposefully, can be used to educate children and acquire knowledge. In this sense, a serious problem, according to ESC, is the excessive use of the internet for the wrong purpose. This creates a danger to the physical and mental integrity of children and leads to a serious limitation of their physical activity.

2.8. In this regard, ESC believes that the problems arising from the digitalization and growth of Internet usage in Bulgaria need to be the subject of constant targeted attention and implementation of specific measures and policies.

3. IDENTIFICATION OF RISKS FACING BULGARIAN CITIZENS AS A RESULT FROM THE USE OF DIGITAL AND INTERNET-BASED TECHNOLOGIES

3.1. The rapid proliferation and development of digital and internet-based technologies have led to the emergence of many new, unknown risks and threats to citizens regarding:

3.1.1. physical safety, especially in the case of children (e.g. instances of threat or assault by those they contact online);

3.1.2. fake news, ideological influences and radicalism;

3.1.3. property (e.g. rental via an online platform);

3.1.4. personal information - Internet technologies have turned personal data into a highly sought-after commodity that threatens privacy;

3.1.5. financial risks - theft of card details, payment fraud, payment for a service they never receive, etc.

3.2. Risks related to online shopping outside the EU

3.2.1. ESC takes a positive view of the trend of expanding remote shopping opportunities in the online environment, because consumers are offered the opportunity to shop online not only from Bulgarian or European (EU) traders, but also from traders anywhere in the world. ESC emphasizes that in Europe consumers have clearly regulated online shopping rights, including:

• the right to pre-contractual information;

• protection against unfair terms;

• protection against unfair commercial practices (incl. misleading and aggressive);

• protection of the user's personal data;

• the right to obtain full compliance of the goods with what was agreed through a legal and commercial guarantee;

• the right of return (refusal), without stating the reason, without owing compensation or penalty, within 14 days;

• the right to alternative dispute resolution arising from the relationship with a trader.

3.2.2. At the same time, ESC reminds that this is not the case with the protection of consumers and their rights when shopping from online stores outside the EU. The main reason is that EU consumer protection does not apply to these purchases. Moreover, enforcement is difficult because control bodies (national or European) cannot impose sanctions and exercise their control functions and powers outside the EU.

3.2.3. ESC pays special attention to the main risks and problems of shopping from non-EU traders:

3.2.3.1. Provision of incomplete or misleading information about the product and its price (offered under extremely attractive conditions, which raises suspicion of a defective product, a fake product or a false offer).

3.2.3.2. Delivery of counterfeit goods (imitation) - are usually recognized at a suspiciously low price; cheap packaging that does not correspond to the expected expensive product; the lack of characteristic holograms that some brands use to protect their products.

3.2.3.3. Shopping from unknown merchants is a prerequisite and risk for the delivery of counterfeit goods - if a merchant we first meet online offers fashion accessories from the latest collection for half the price, it probably delivers imitations.

3.2.3.4. Malevolent fake reviews create the risk of unconditional trust of honest online customer reviews, which can be misleading - the customer may be incentivized to write something positive in return for payment or the merchants themselves post false reviews.

3.2.3.5. Payment of the price of the goods without the necessary trust in the other party, which may make it difficult or impossible to repay the amount paid in case of problem with the purchased goods or when they are not delivered.

3.2.3.6. Unfair terms and conditions (no warrantee, no right of return, etc.).

3.2.3.7. Missing, incomplete or misleading information about the merchant, which makes it impossible to communicate with them.

3.2.3.8. When shopping from non-EU merchants, it is very difficult and often impossible to resolve disputes and problems. Even when the website is in Bulgarian or the address ends with .bg, there is no guarantee that it is registered in Bulgaria.

3.3. Internet Connected Security - The Internet of Things

3.3.1. ESC believes that with the growing in popularity service "Internet of Things", defined as interconnecting via the Internet, computing devices embedded in everyday objects, allowing them to send and receive data, provide new opportunities for users, but at the same time generate hitherto unknown security and safety risks.

3.3.2. The Internet can connect devices from different manufacturers, retailers, or software developers. This can make it much more difficult to determine who is responsible when something goes wrong. Therefore, ESC believes that a clear and stable product liability framework must be worked on. It should be clear which entity is responsible for the implementation and security during the full life of the connected product.

3.3.3. Following numerous scandalous revelations around the world of data leaks through connected devices, it has become clear that measures must be taken to guarantee the principle that the owner of a device must control how and by whom the data it generates is used. The settings of each connected product should be set by default to the highest level of privacy protection, and consumers should be aware of the implications of how data collected through the Internet can be used.

3.3.4. Users should have access to high quality and high-speed internet connection. According to ESC, particular attention should be paid to providing access for marginalized or vulnerable groups of users, incl. in remote geographical areas and in compliance with the principle of net neutrality.

3.3.5. It should also be ensured that consumers receive clear, concise and easily understandable information about related products, and in particular what a product can or cannot do without being connected, instead of the widespread "I agree with general terms ". Critical information must be prominently displayed before purchase.

3.3.6. Digital technologies have changed the nature of many products because of connected software. ESC believes that the functionality of the products should not be limited by software rights or lack of updating and maintenance, and that it must be guaranteed to work offline.

3.3.7. The Internet of Things gives hackers more vulnerabilities. Existing legislation and product safety standards are limited to the safety of physical devices. ESC is of the opinion that in order to ensure security, the concept of 'security' should be revised and legislation should be updated to take account of new issues related to cybersecurity, data security and product safety.

3.4. Security of online payments

3.4.1. The successful development of an Internet-based economy requires advanced online payment systems and high consumer confidence in them. ESC notes that Bulgaria is currently at the forefront of using cash payments for the delivery of products ordered online by 62% compared to the EU average of 18%.

3.4.2. According to OECD data in 2015, about 2.5% of French and UK nationals have suffered financial losses as a result of unauthorized or fraudulent online payments over a three-month period. In the absence of such statistics for Bulgaria, the size of this problem in our country cannot be categorically determined, even more so in the context of the aforementioned prevailing cash payments.

3.4.3. When considering the security of online payments, the security features of different payment mechanisms should be taken into account. Overall, credit card protection is higher than debit cards and bank transfers, as consumers have the ability to dispute payments for delivery issues. According to ESC, efforts should be made to inform consumers about existing measures and procedures for different types of payments, which can also help reduce cash payments.

3.4.4. Without adequate security of payments, data provided in the context of e-commerce payments may be lost, stolen or otherwise misused, especially when using mobile devices, because of the higher risk of loss, theft or compromise. In this regard, ESC believes that encryption and dynamic data authentication could help address potential problems and increase consumer confidence in mobile payments.

3.5. Application of artificial intelligence in online services

3.5.1. Algorithms based on artificial intelligence (AI) rapidly enter the modern economy. They often completely replace people in providing multiple logistics and customer services, which often creates distrust and concern for their users. Moreover, AI is systematically used to profile and personalize clients, which requires the processing of personal and/or non-personal data.

3.5.2. Lack of sufficient knowledge and understanding of what artificial intelligence means is probably at the root of the anxiety and distrust of how much people will retain control of the machine and control of their lives.

3.5.3. ESC notes that following the adoption of a strategy on Artificial Intelligence for Europe, published in April 2018, the European Commission (EC) has proposed a Coordinated Artificial Intelligence Plan, which formulates measures at the EU and national levels in the context of world competition. In addition to measures to increase investment, improve data availability and accessibility, provide support for talents and skills, the EC proposes to formulate confidence-building measures as well.

3.5.4. In this regard, ESC calls for the timely adoption of a national AI strategy as foreseen in the Coordinated AI Plan.

3.5.5. ESC recalls that in its opinion the EESC calls for better statistics and more research on the implications of AI for employment and work, including studies on sector-specific impacts. More knowledge and understanding of the nature and functioning of AI are also needed to increase people's confidence based on critical thinking.

3.5.6. ESC fully endorses the EESC's position and believes that measures to tackle the mistrust of AI should take into account both the promotion of technology opportunities and the ethical, environmental and social aspects of their implementation.

3.6. Responsibility of online platforms

3.6.1. The development of online information and commerce platforms has also raised a number of questions and raised concerns among citizens. According to a 2016 Eurobarometer survey 72% of users have concerns about their data being collected. At the same time, 56% admit that they have not read the terms of use of the online platforms. On the other hand, 75% of citizens believe that more transparency is needed in ordering search results, identifying the actual provider of a good or service, or false reviews.

3.6.2. ESC welcomes the EU's efforts to develop and adopt an Online Platforms Regulation (Regulation), which created the preconditions for a level playing field for comparable digital services, responsible online platform behavior, transparency and impartiality, open and non-discriminatory markets in a data-driven economy.

3.6.3. ESC also stresses the need to strengthen coordination between national supervisory authorities in EU Member States in order to ensure the effective application of the requirements of the Regulation.

3.6.4. ESC also believes that a broader information campaign is needed to inform Bulgarian citizens and SMEs of the requirements adopted for online platforms in order to effectively protect the rights of citizens and businesses when using them.

3.7. Social challenges - risks in social networks

3.7.1. The Internet provides a fertile ground for the application of numerous scams that are not restricted to any country. The most significant of these are:

3.7.1.1. E-commerce fraud when consumers pay for goods that then turn out to be false, defective or of poor quality. In some cases, the goods are never delivered.

3.7.1.2. Investment fraud when advertising too good investment opportunities, using news and ads that appear to come from genuinely existing sources. Consumers who are tempted to invest in such investment scams can lose a significant portion of their money.

3.7.1.3. False identity when there is a representation as an authentic brand, real friends or relatives in order to gain consumer trust and are offered to buy goods, send money or download malware on their computer.

3.7.2. Social networks, in turn, are a field for many risks, mainly related to:

3.7.2.1. Illegal use of personal information by third parties that might, for example, find a way to copy and aggregate profiles, collect personal financial information or copy personal information and use it for their own purposes.

3.7.2.2. Identity theft when someone illegally obtains and uses another person's personal data in a manner that involves fraud or deception, usually for economic gain.

3.7.2.3. Cyber bullying and harassment when there is targeted, deliberate, unbalanced and criminal use of digital technology to offend, publicly humiliate, spread rumors and lies, and harass a person in his or her real life through digital technology.

3.7.3. Consumers suffer the most scams that penetrate WhatsApp and Facebook, followed by Instagram and Twitter.

3.8. Social challenges - risks for children

3.8.1. According to a national representative survey from the Applied Research and Communications Foundation of 2016, almost all Bulgarian children (97%) aged between 9 and 17 use the Internet, while having children in the family significantly increases the likelihood of having broadband at home. The age at which children go online for the first time is steadily falling, with the youngest being 4 years old (3%) and 5 years old (6.8%). Almost a quarter (24.3%) of children had their first contact with the Web at the age of seven, and by the age of 11, nearly 90% had already become Internet users. The average age at which children first go online in 2016 is 8 years, while in 2010 it was 9.

3.8.2. The survey also found that children use the Internet the most for watching videos 68.8%, using social networks (64.9%), playing games online (55.3%) and listening to music (54.2%). ESC draws attention to the finding that the greatest risks for children lie in the use of social networks. The most prominent of them include contacts with strangers, inappropriate content, virtual or sexual harassment. According to ESC, internet use and addiction are also a serious problem.

4. PROPOSALS FOR INCREASING THE OPPORTUNITIES RESULTING FROM DIGITALIZATION

4.1. Developing digital literacy

4.1.1. Emphasizing the crucial importance of education and digital skills, ESC agrees with OECD's recommendation to governments that they should raise awareness and support education as essential tools for empowering parents and children, for example by:

• integrating online literacy and skills into curricula with a focus on risks and appropriate behavior in an online environment;

• training and encouraging other stakeholders to educate and raise the awareness of children and parents;

• regularly measure the development of their internet literacy.

4.1.2. ESC calls for digital literacy training at all stages of education. It should focus on online safety, internet security, critical understanding and evaluation of information, online etiquette and other social skills.

4.2. Digital literacy in financial services

4.2.1. Digital financial services are technologies, including electronic money, mobile financial services, online financial services, banking without face-to-face contact with customers, etc., which are a global phenomenon. They offer unlimited opportunities to integrate the poorer and financially excluded sections of the population who have not previously banked by: extending access, including to new types of financial services, to overcome physical infrastructure barriers; reducing costs and providing more affordable finances for all; offering more convenient, faster, secure and timely transactions; and providing a seamless user experience tailored to individual needs.

4.2.2. Consumer challenges in accessing and using digital finance can stem from a general lack of awareness and knowledge of financial concepts or digital technologies. Accordingly, they may be due to: a lower level of general literacy; limited general financial literacy; lack of knowledge or lack of knowledge of financial services and related regulation; lack of specific awareness or knowledge of digital finance; inadequate digital skills and competences; and lack of knowledge of technology and/or finance.

4.2.3. ESC believes that financial literacy and education can play an important role in enhancing consumer protection, raising awareness and awareness of digital finances, increasing financial literacy for the use of digital finance and enhancing overall consumer confidence in them.

4.3. Digital literacy in healthcare

4.3.1. Expert estimates show that approximately 15% of healthcare costs can be saved by remote monitoring using mobile healthcare solutions. ESC shares the view that mobile healthcare can contribute to achieving more equal access to healthcare, as technologies cover remote areas and groups of people who may have difficulty accessing healthcare.

4.3.2. In this regard, ESC believes that an information campaign is needed to help inform citizens about the available eHealth options for e-access to their data on medical manipulations performed, in order to personally control the abuse of the National Health Insurance Fund.

4.3.3. At the same time, ESC is concerned about ensuring the safety of mobile health solutions and applications affecting lifestyles and well-being, which explains the potential

lack of trust in citizens. According to ESC, on the other hand, safety can be demonstrated using consumer safety standards or special quality marks.

4.3.4. Concerns may also be raised where citizens might use the results of a technical solution or application in the field of mobile healthcare to make a stand-alone decision that could endanger their own health, or where a technical decision in the field of mobile healthcare wrongly indicates that the person is in good health.

4.4. Digital exclusion

4.4.1. ESC pays special attention to the fact that the needs of marginalized or vulnerable consumers as well as disadvantaged consumers must be taken into account when developing online trading platforms and e-commerce processes such as payments and deliveries in order to reduce the danger of further marginalization and social exclusion.

4.4.2. In view of the growing popularity of the sharing economy, it should be noted that a steadily increasing group of users remains unaffected by the benefits of internet technology in terms of sharing and leasing a functional resource. This is of utmost importance not only in the context of the ageing population in Bulgaria, but also in view of increasing prices of resources around the world.

4.5. Protection of privacy and correspondence

4.5.1. ESC calls for strict application of the high standards of personal data protection and privacy set out in European legislation, both in substantive and procedural law. Citizens should be able to exercise full control over their personal data - how they are collected, used and shared, and be able to protect their privacy.

4.6. Network neutrality in Bulgaria

4.6.1. Network neutrality is a principle whereby all electronic communications transmitted over the Internet are treated equally without discrimination, restriction or interference, regardless of the sender, recipient, type, content, device, service or application.

4.6.2. Bulgaria is among the seven EU countries that have set a relatively low fine (EUR 100,000) for net neutrality offenses. In ESC's view, in order to be dissuasive and proportionate to the infringement, the penalty should be based on the annual turnover of the infringing company.

Prof. Lalko Dulevski, Ph.D.

PRESIDENT OF THE ECONOMIC AND SOCIAL COUNCIL