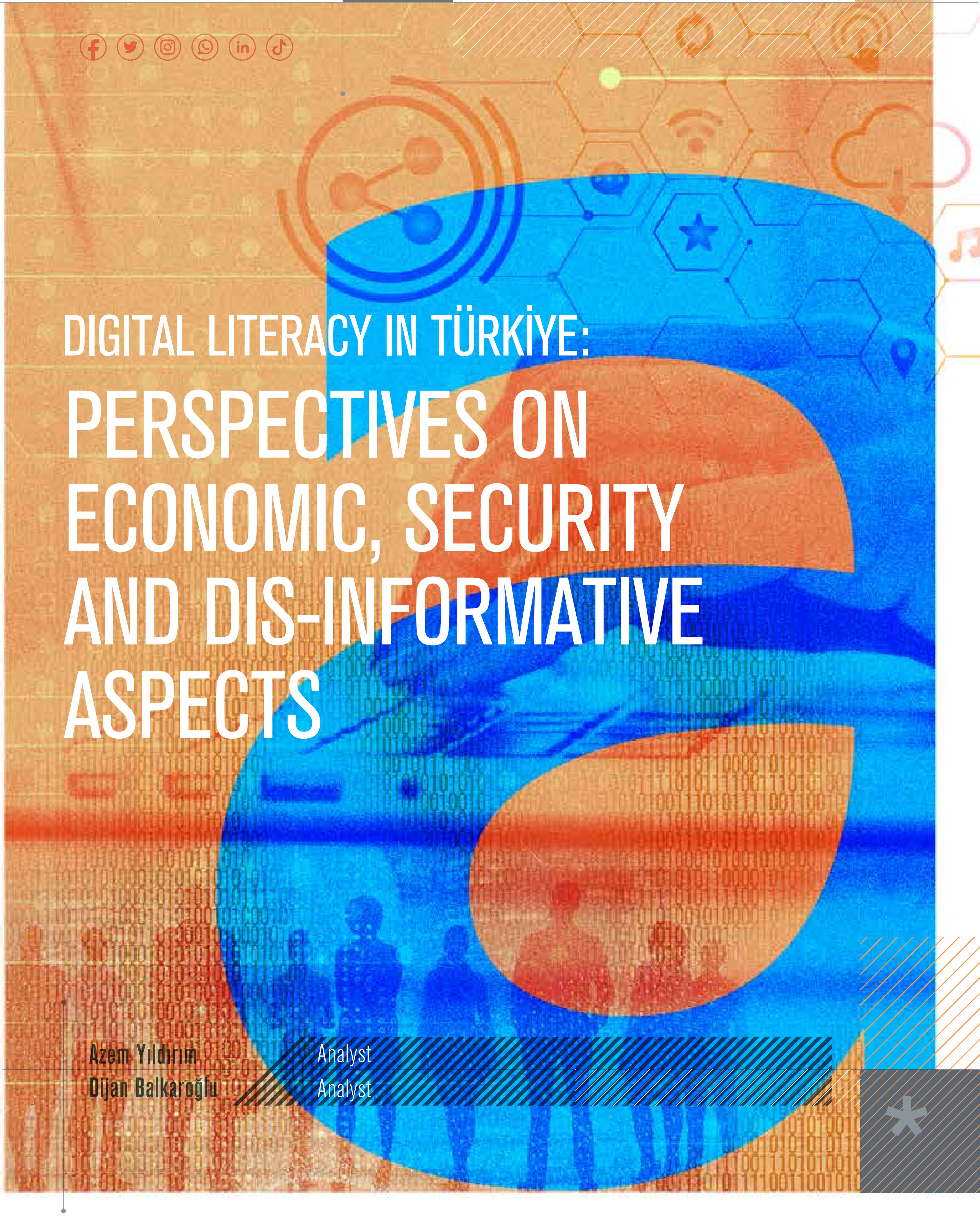
edam
Centre for Economics
and Foreign Policy Studies

01 // 2023

SUBJECT CYBER GOVERNANCE & DIGITAL DEMOCRACY 2023/01/EN



DIGITAL LITERACY IN TÜRKİYE: PERSPECTIVES ON ECONOMIC, SECURITY AND DIS-INFORMATIVE ASPECTS

Azem Yıldırım Analyst
Dijan Balkaroğlu Analyst

Digital Literacy in Türkiye: Perspectives on Economic, Security and Dis-Informative Aspects

JANUARY // 2023

Azem YILDIRIM	Analyst
Dijan BALKAROĞLU	Analyst

This report has been prepared by the Centre for Economics and Foreign Policy Studies (EDAM) for TikTok Turkiye.

EXECUTIVE SUMMARY

Digital literacy is generally defined as ability to navigate our digital world using reading, writing, technical skills, and critical thinking. In other words, it is about using technology to find, evaluate, and communicate information. In line with this definition, the report provides an insight in areas that are at the core of the challenge of digital literacy, namely the ability to participate in the digital economy, the state of play regarding online privacy and digital and social media disinformation.

DIGITAL ECONOMY

The digital economy can be defined as the sum of economic activities in which digitized information is used as the main factor of production. According to the Financial Times Omdia Digital

Economies Index - which makes its evaluation based on five criteria: connectivity (and communications), devices (and the internet of things), enterprise computing, entertainment and payments- Türkiye ranks twentieth in the overall ranking and yet it ranks seventh in credit card transaction volume, eighth in monthly active Facebook users and eleventh in the population of YouTube users. In the same vein, the increasing volume of the digital economy points also to an increase in digital literacy as people have been transacting online more and more. But gaps remain with developed countries. The deviation can be explained not only by differences in financial and infrastructural capacity, but also by the level of educational attainment which correlates strongly with the use of digital services. According to a report by Ingev and Oxford University on Digital Citizenship in Türkiye, while 72% of university or above graduates indicate that they use e-commerce, the number falls to 52%, 33%, 23% and for high school, middle school and primary school graduates respectively.

One area that Türkiye has been particularly successful in terms of digital services adoption has been digital public services. For instance, in 2021, 68.7% of Turkish citizens used the e-government platform. Accordingly, the 2022 UN E-Government Survey identifies Türkiye as one of the twelve upper-middle income countries that are in the very high segment of the online services index "by capitalizing on very high levels of human capital development and moderate to very high levels of infrastructure development".

Policy Recommendations

Digital literacy will be deeply tied with the wellbeing of millions of families in the coming period. In line with our previous recommendation, the report shows that an increasing share of the Turkish workforce will require higher levels of education. Among the needed skills are higher cognitive, social and technological ones. It is estimated that the demand for technological skills will rise by 63%. Higher cognitive skills such as critical thinking are connected to digital literacy, and so are technological ones which include basic digital skills. It is imperative for both the government, through national education, and employers, through reskilling programs, to ensure that the workforce is ready for this transition. The OECD recommends that strengthening vocational education and adult learning in digital areas would help the productive sector better tap the potential of technological change". A more fundamental solution is integrating digital solutions in all areas of education. As mentioned, digital literacy includes skills that are not necessarily technical such as critical thinking, reading, and writing. Modes of instruction that use digital methods to teach these skills would increase students' digital literacy just as, after some point, traditional literacy instruction advances from letters and syllables to understanding texts and writing compositions. This should not be limited to national education, either. Any instruction on business or other economic activities should consider digital applications of the materials taught.

ONLINE SAFETY

Aspects of digital literacy such as critical thinking and basic knowledge of how digital systems work are connected to cybersecurity. Knowing that one should not click on every link since some links automatically download things, or that passwords comprising only of numbers are easier to break in are a few examples of how foundational digital knowledge can enhance security. Moreover, critical thinking in the broader sense can help with evaluating which link is suspicious or whether the person communicating with can be an imposter or not. An LSE study looking at children's digital literacy and safety skills found out for instance that safety skills and critical literacy skills were positively correlated and potentially mutually reinforcing. A key barrier to the improvement of online safety practices is socio economic disparities. As digital skills develop with use, inequalities such as socio-economic status, age and gender still affect their development. A study of high school students in Gaziantep and Kilis found that male students scored significantly higher than females in terms of digital security awareness.

Policy Recommendations

Firstly, there is a need to have a culture of digital safety where consciousness and basic skills about it are second nature. This can be achieved through simultaneous action by all stakeholders: the government, public and private organizations and digital citizens in general. Implementing public awareness campaigns through public and civil society channels, complemented by platform-initiated reminders by social media providers, could help to introduce the stakes to the user concerning the damages that can be inflicted in case of poor security measures.

Secondly, inequality in digital literacy correlated with other inequalities such as socio-economic status and gender. The uneven distribution of net infrastructure may have a role but nevertheless, but the lower levels of digital literacy renders disadvantaged groups more vulnerable to digital security threats exposing the whole digital ecosystem to a higher level of vulnerabilities. Therefore, public programs designed to bridge gaps of inequality would be instrumental in overcoming deficiencies in digital literacy.

In the same vein, it has to be underlined that gender inequality also takes shape in the digital world. There is a significant discrepancy between women's and girls' digital adoption and that of men's and boys'. However, the data revealing the underlying causes of these discrepancies is still nascent, especially among young generations, consequently, current research is not permissible to introduce extensive policy suggestions. Comprehensive data-based research to determine the contribution levels of the previously mentioned factors among females from different socioeconomic and geographic backgrounds is strongly advised so that necessary policies can be applied in a tailored fashion.

COMBATING DISINFORMATION

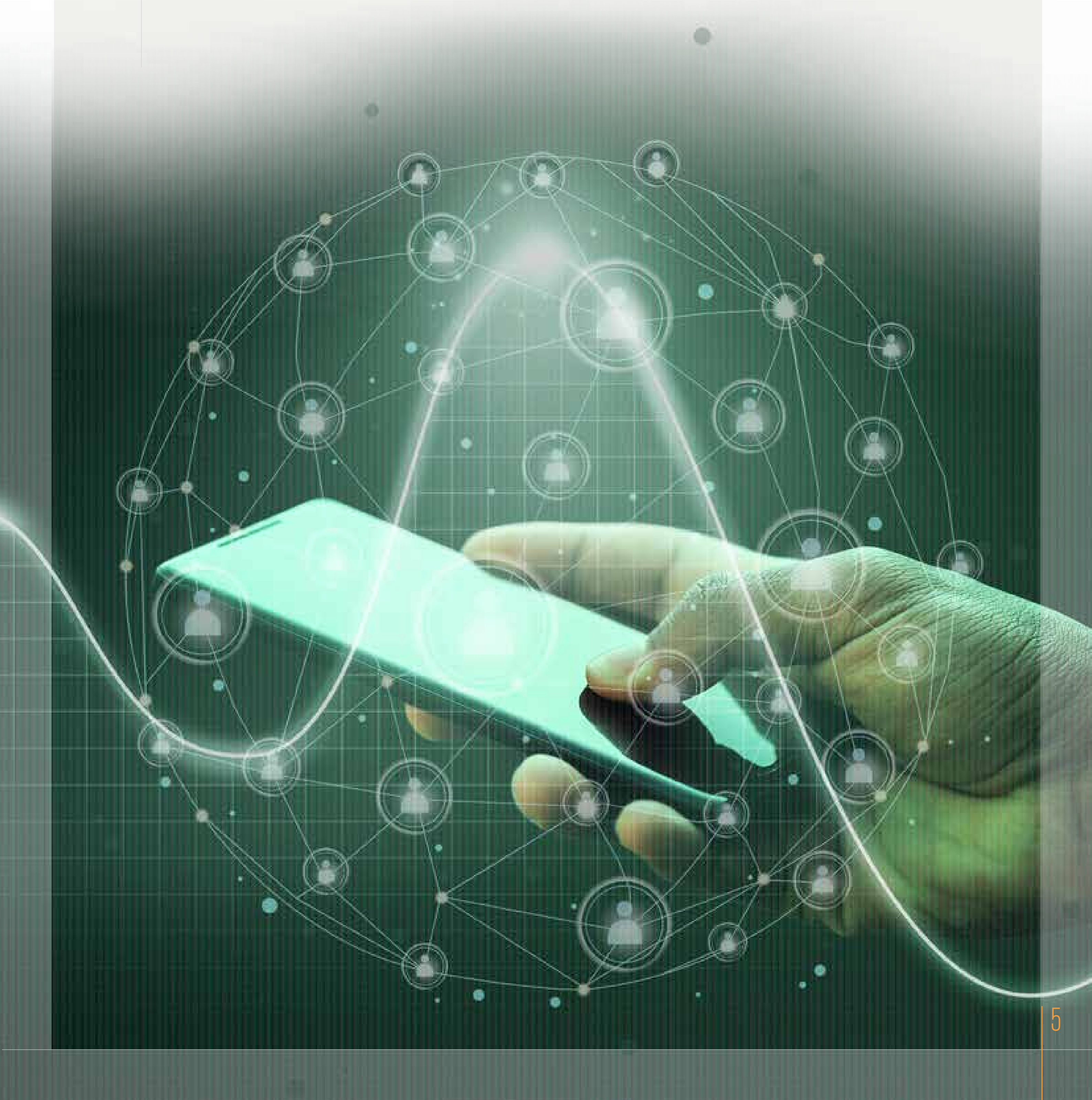
The ways of spreading false information are diverse, and combatting each of them requires different techniques and interventions. Moreover, new channels appear as technology and society evolves further. Though disinformation is spread with a myriad of personal or other motives, its socio-political dimension poses a significant threat to both democracy and social cohesion. This is also why governments and international organizations are particularly interested in fighting this phenomenon. Türkiye has not been an exception to this trend. Türkiye's Omnibus Law number 7428, also known as the 'Disinformation Law', entered into force on the 18th October, 2022 subsequent to its publication in the Official Gazette. In addition to extra regulations and requirements for social media platforms, over-the-top platforms such as messaging apps, and online newspapers, a controversial aspect of the law is the way it criminalizes disinformation. According to the law, 'spreading misleading information' becomes a criminal act if four essential criteria are fulfilled simultaneously: Publicly disseminating false information, relating to the country's internal and external security, with intent to cause worry, fear or panic, in a way that disrupts public order and general health.

The law has thus far been criticized for severely limiting freedom of speech and privacy. Organizations and bodies such as Human Rights Watch , the Venice Convention , and Article 19 have voiced concerns based on the observation that the state assumes the responsibility for determining truth and intent, and criminalizes behavior based on vague criteria.

Policy Recommendations

For governments that want to combat disinformation and its destructive effects, the main issue can be defined as trying to prevent disinformation on the one hand, and creating solutions that enable societies to be more resilient to disinformation on the other. The approach adopted by democratic countries in the fight against fake news and disinformation is instructive. In these countries, penal sanctions on sources of disinformation or fake news are very limited and only valid for extreme (terrorist) cases. On the other hand, it was also preferred to impose obligations on the platforms that carry the news. A similar approach is adopted by the European Commission, which acts as a Europe-wide rule maker to combat disinformation.
Strengthening the information ecosystem is another pillar of the measures taken at the public level to combat disinformation in Western democracies. In this framework, objectives such as strengthening digital literacy, supporting the so-called "fact checker" and trying to detect fake news, ensuring pluralism in the media and protecting freedom of expression are at the forefront.

As a result, it is now clear that new rules and mechanisms are needed to protect the information ecosystem. In this context, the legislator must also make a choice. As a matter of fact, a clear distinction has emerged between democratic countries and authoritarian systems in the fight against fake news. In authoritarian systems the laws give weight to the measures in which the public is at the forefront, coercive and police-dominated, harming the freedom of the press and expression, while democratic countries, on the contrary, are based on the guiding principle of the state and essentially oppose this manipulation of information. has embraced solutions where civil society, journalists, fact-checkers and platforms bear greater responsibility. This critical choice has been made in order to preserve the balance of security and freedom in the social contract at the core of democracies. It would be useful to remember this general framework in the context of the implementation of the newly adopted disinformation law in Türkiye.



WHAT IS DIGITAL LITERACY?

While the traditional definition of literacy is the ability to read and write in one's mother tongue, this definition began to be questioned in the mid-twentieth century[1]. The fear developing countries had of falling behind in technological competence, combined with the rapid growth and development of technology, led Paul Gilster to introduce the concept of 'Digital Literacy' in 1997. Gilster defined digital literacy as the ability to understand and use information presented in a variety of formats via computer from a wide range of sources[2]. Today, a variety of other internet-enabled devices can be added alongside computers as mediums of digital information. Thus, the concept of literacy extends beyond traditional literacy. Another, more recent definition by Microsoft is stated as "the ability to navigate our digital world using reading, writing, technical skills, and critical thinking. It's using technology– like a smartphone, PC, e-reader, and more—to find, evaluate, and communicate information"[3] Notice that differently from Gilster who draws attention to understand and use information presented through digital media, here the emphasis is on 'navigating' an entire digital world with the help of certain skills. This definition also gives way to a more economic or commercial understanding of the term. The interconnectivity enabled by digital literacy and accessibility also brings about economic possibilities either through benefitting from the digitalization of traditionally physical services, or by opening up new avenues for completely digital new opportunities.

Another aspect that has been related to digital literacy is its importance in dealing with digital and social media. Digital media, unlike traditional media, does not have a one-way connection. Content is only delivered unidirectionally in traditional media. In digital media, however, the user is no longer the last link in a chain, but rather a node in the middle of a near-infinite network; everyone and everything is interlinked. As a result, unlike in traditional media, the barriers to participation are much lower, and anyone can publish content and find an audience whether they desire to or not. Accordingly, TikTok's perspective on digital literacy, for example, has focused on personal privacy, internet protection and countering disinformation[4].

Based on these definitions and recent developments, we decided to focus this report on three areas relating to digital literacy. First, we focus on the ability to participate in the digital economy. From the point of view of consumers, we look at how awareness of access to online services such as those provided by the government and others such as e-banking and e-commerce is enabled by digital literacy. We complement this section with a brief overview of the state of digital skills in the context of the digitalization of work in Türkiye. Indeed, in addition to facilitating the use of services, digital

[1] Kurt, Adile, Derya Orhan Göksün, Fatih Yaman, Mehmet Solak, and Fatih Türkan. "Bilgi ve İletişim Teknolojileri Işığında Türkiye'de Yapılan Okuryazarlık Çalışmalarındaki Eğilim" Eğitim Teknolojileri Araştırmaları Dergisi, June 2014.

[2] Lankshear, Colin, and Michele Knobel. "Digital Literacy and Digital Literacies:" Nordic Journal of Digital Literacy, January 2015, 13.

[3] Microsoft. "Digital Literacy Courses, Programs & Resources | Microsoft Digital Literacy." Accessed October 27, 2022. https://www.microsoft.com/en-us/digital-literacy.

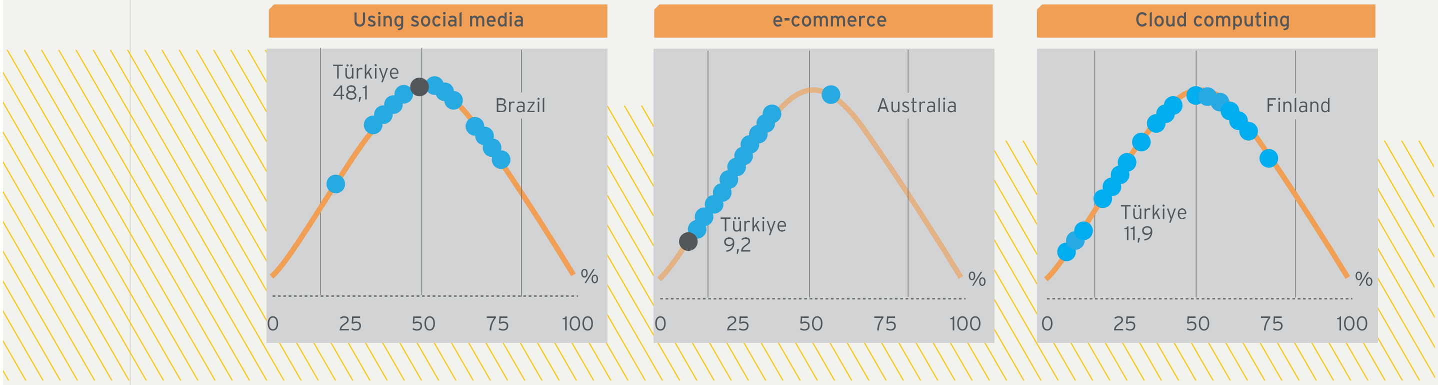
[4] Newsroom | TikTok. "TikTok Unveils Digital Literacy Edition of Its Wellness Hub to Reinforce Commitment to Online User Safety and Education," May 13, 2022. https://newsroom.tiktok.com/en-sg/tiktok-unveils-digital-literacy-edition-of-wellness-hub.

literacy also plays a key role on the supply side as well, given the continuously digitalizing nature of Turkish economy. We then look at internet security and privacy to determine where Türkiye is at with regards to the consciousness and ability of users in this regard. Finally, we dedicate a significant portion of the report on disinformation as it currently occupies a key spot on the national legislative and policy agenda. In that section, we point out digital literacy as a way of overcoming it.

ABILITY TO PARTICIPATE IN THE DIGITAL ECONOMY

Although the digital economy is a frequently used concept, it can be difficult to provide a concise definition for it. Essentially, the digital economy can be defined as the sum of economic activities in which digitized information is used as the main factor of production. Digital connections between individuals and businesses, data, internet-enabled machines and the internet of things form the backdrop of the digital economy in this context[5].

According to the FT Omdia Digital Economies Index, which uses a similar methodology, Türkiye ranks 20th out of 51 countries compared in 2022[6]. This index makes its evaluation based on five criteria: connectivity (and communications), devices (and the internet of things), enterprise computing, entertainment and payments. Although Türkiye ranks 20th in the overall ranking, it ranks 7th in credit card transaction volume, 8th in monthly active Facebook users and 11th in YouTube users. It ranks 20th in online net advertising turnover. Although these indicators suggest that Türkiye is in a relatively advantageous position in terms of digital consumption, the fact that the index does not include factors such as e-commerce usage or access to e-government services prevents a comprehensive analysis.



[5] Atici, Gonca. Digital and Digitalized Economy in EMs: A Focus on Türkiye. Emerging Markets. IntechOpen, 2020. https://doi.org/10.5772/intechopen.94494.

[6] Omdia. "FT Omdia Digital Economies Index 2022-26," June 23, 2022.

The Türkiye section of Statista's 2021 Digital Markets Outlook[7] report measures the volume of the digital economy based on the annual turnover of the digital media, e-commerce and e-services sectors. According to this report, the digital economy volume, which was 5.58 billion dollars in 2018, reached around 13.1 billion dollars in 2021. E-commerce itself accounted for 89% of the volume in 2021.

The increasing volume of the digital economy points also to an increase in digital literacy as people have been transacting online more and more. In the realm of e-commerce, this indicates that both consumers and SME owners operating digitally are developing the competency to trade online. But gaps remain with developed countries. An OECD report from 2021 asserts that Turkish SMEs have not yet fully embraced the digital revolution. The report presents the charts on social media use, e-commerce and cloud computing adoption portrayed to the left as indicators for this lag[8]. Though these factors are also related to financial and infrastructural capacity, it has to be conceded that digital literacy also plays a part. Here, it is possible to draw a connection between general level of education and digital literacy. A report by Ingev and Oxford University on Digital Citizenship in Türkiye illustrates that educational attainment correlates strongly with the use of digital services[9]. So much so that while 72% of university or above graduates indicate that they use e-commerce, the number falls to 52%, 33%, 23% and for high school, middle school and primary school graduates respectively. The same trend is at play for other digital services such as e-banking and even for the widely used e-government portal, E-Devlet, where there is a gap of 30% between university and middle school graduates. A straightforward solution that this implies is to invest in higher education overall with complementary programs for adults.

One area that Türkiye has succeeded in terms of digital services adoption has been digital public services, that is, e-government. Digitalization of public services lowers costs, makes them more transparent and accessible, and overall boosts government effectiveness[10]. While e-government services were once seen as the digital alternative, the 2022 UN E-Government Survey posits that with intense digitalization, the line between offline and online public services is disappearing[11]. The report claims that digital government is at a critical point in that it is no longer a "stand-alone or auxiliary" tool but rather integral for the functioning of public institutions and their delivery of services. The stakes for national governments are therefore higher as mismanagement in this are poses challenges for cybersecurity and data privacy, and overall development in general. Inaction is also perilous since it means missed opportunities in terms of economic and social development.

[7] Statista. "Digital Economy - Türkiye." Accessed August 09, 2022. https://www.statista.com/outlook/co/digital-economy/turkey. Using August 2022 exchange rate.

[8] OECD. "OECD SME and Entrepreneurship Outlook 2021 | En | OECD," June 28, 2021. https://www.oecd.org/publications/oecd-sme-and-entrepreneurship-outlook-2021-97a5bbfe-en.htm.

[9] "DİJİTAL VATANDAŞLIK: Erişim, Tutum ve Davranışlar - Sunum." Ingev, University of Oxford, October 2021. https://s.gazeteduvar.com.tr/storage/files/documents/2021/11/02/ingev-calistay-sunum-dijital-vata-tifw.pdf.

[10] Nam, Taewoo. "Does E-Government Raise Effectiveness and Efficiency?: Examining the Cross-National Effect." Journal of Global Information Management 27 (July 1, 2019): 120–38. https://doi.org/10.4018/JGIM.2019070107.

[11] "E-Government Survey - The Future of Digital Government." UN Department of Economic and Social Affairs, 2022. https://desapublications.un.org/sites/default/files/publications/2022-09/Report%20without%20annexes.pdf.

The aforementioned UN survey identifies Türkiye as one of the twelve upper-middle income countries that are in the very high segment of the online services index "by capitalizing on very high levels of human capital development and moderate to very high levels of infrastructure development"[12]. Digitalization of government services has been part of Türkiye's long-term digitalization policy as articulated by the National E-Government Strategy and Action Plan[13]. Türkiye also scored tenth highest E-Government Development Index among Asian countries. In 2021, 68.7% of Turkish citizens used the e-government platform according to Turkstat[14]. The platform that was launched in 2008 offers 6,665 digital services provided by 886 institutions, and has a user count of over 60 million[15]. Though Türkiye has achieved sufficient quality in terms of e-government, there is still room for improvement as the country would be fourth from last in terms of E-Government Development Index had it been compared with European countries. Keeping in mind the educational gap in access to e-government services, a straightforward solution can be to invest in higher education overall with complementary programs for adults.

Digital literacy on the part of users is only half the story on its effects on economy. In an increasingly digitalized world, digital literacy is as important for producers as traditional literacy was in the pre-digital era. The UN's view on digital public services can be generalized for the whole digital economy, in fact; mismanaging or not achieving to have a workforce equipped with ITC skills, for which digital literacy is necessary, means missing out on catching on to the new era of work. A McKinsey report from 2020 outlines clearly the opportunities and challenges Türkiye has in this regard[16]. It claims that with current technologies, six out of ten occupations could be automated by 30% by 2030. On one hand, automation will reduce the manpower needed in certain areas. On the other, adoption of new technologies is also expected to create new jobs. The tradeoff is between workers whose jobs will be automated, and those who can fill in the new technologically intensive ones. The latter category will need to possess the necessary digital literacy, and the ones in the former category need to acquire it so that they do not fall through the cracks. In the net, however, the report foresees 3.1 million additional jobs being created. 21.1 million workers will need to improve their digital skills to remain employed with their current employers. The authors predict that 7.6 million people will be affected by significant reskilling and job displacements and 7.7 million will join the workforce with the necessary skills by 2030.

There are not small numbers. Digital literacy will be deeply tied with the wellbeing of millions of families as digitalization intensifies in the coming decades. In line with our previous recommendation, the report shows that an increasing share of the Turkish workforce will require higher levels of education. Among the needed skills are higher cognitive, social and technological ones.

[12] "E-Government Survey - The Future of Digital Government." UN Department of Economic and Social Affairs, 2022, 13 https://desapublications.un.org/sites/default/files/publications/2022-09/Report%20without%20annexes.pdf.

[13] Ozan, Mehmet Seyda. "Türkiye'de Ulusal E-Devlet Stratejisi ve Eylem Planının Bilgi Ve İletişim Teknolojileri Üzerinden Değerlendirilmesi," 2020.

[14] TÜİK. "Hanehalkı Bilişim Teknolojileri (BT) Kullanım Araştırması, 2022," August 26, 2022. https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanim-Arastirmasi-2022-45587.

[15] Unal, Arife Yildiz. "E-Devlet Kapısı'nda Kullanıcı Sayısı 60 Milyonu Geçti." Anadolu Ajansi, November 8, 2022. https://www.aa.com.tr/tr/gundem/e-devlet-kapisinda-kullanici-sayisi-60-milyonu-gecti/2658630.

[16] McKinsey. "The Future of Work in Türkiye," February 28, 2020. https://www.mckinsey.com/featured-insights/future-of-work/the-future-of-work-in-Türkiye.

It is estimated that the demand for technological skills will rise by 63%. Higher cognitive skills such as critical thinking are connected to digital literacy, and so are technological ones which include basic digital skills. It is imperative for both the government, through national education, and employers, through reskilling programs, to ensure that the workforce is ready for this transition. The OECD Economic Survey of Türkiye in 2021 state that Turkish firms forego large dividends from digitalization due to a bottleneck caused by inadequate internet infrastructure and shortcomings in digital skills. The OECD recommends that strengthening vocational education and adult learning in digital areas would help the productive sector better tap the potential of technological change"[17]. Moreover, focusing on digital education for students would reduce the socioeconomic gap that is inherent in the digital economy, it says.

A more fundamental solution is integrating digital solutions in all areas of education. As mentioned, digital literacy includes skills that are not necessarily technical such as critical thinking, reading, and writing. Modes of instruction that use digital methods to teach these skills would increase students' digital literacy just as, after some point, traditional literacy instruction advances from letters and syllables to understanding texts and writing compositions. This should not be limited to national education, either. Any instruction on business or other economic activities should consider digital applications of the materials taught.

[17] Florence, GUERINOT. "OECD Economic Surveys: Türkiye 2021." OECD Economic Surveys, 2021, 78.

AWARENESS OF INTERNET SECURITY AND PRIVACY

As interaction with the digital world intensifies, the potential surface of cyber-attack also increases[18]. Put simply, the chances of a password getting breached increases as user has more passwords. Even worse, if the user does not take precautions in line with their increased use of internet services, their vulnerability increases. Identifying potential risks and taking precautions have become a necessity to effectively use the internet and related services. The awareness thereof and the ability to carry out digital hygiene practices come with digital literacy.

Types of cybersecurity threats that end-users face include[19] *:*

- *Malware Attacks:* Where different forms of software viruses infect the victim's device either through a compromised network or by the victim unintentionally downloading the malware, for example by clicking a suspicious link.
- *Phishing Attacks:* Where the attacker impersonates a trusted contact (such as an official, friend, or technical assistant) to make the victim deliver sensitive information.
- *Password Attack:* Where the attacker cracks the victim's password by using specialized software.
- *Man-in-the-Middle Attack:* Where the attacker eavesdrops on the victim's communication by intercepting data to acquire sensitive information from the victim.

These examples illustrate that aspects of digital literacy such as critical thinking and basic knowledge of how digital systems work are connected to cybersecurity. Knowing that one should not click on every link since some links automatically download things, or that passwords comprising only of numbers are easier to break in are a few examples of how foundational digital knowledge can enhance security. Moreover, critical thinking in the broader sense can help with evaluating which link is suspicious or whether the person communicating with can be an imposter or not. Indeed, an LSE study looking at children's digital literacy and safety skills found out that safety skills and critical literacy skills were positively correlated and potentially mutually reinforcing[20].

There are some indicators that there is awareness in Türkiye about these issues. This is made clear by a survey conducted by Ipsos in late 2020 with 15,700 responders in 31 countries. There is certainly anxiety as Türkiye tops the list in the "share of adults who think it is likely that their online accounts will be hacked into in 2021" with 50% of adults responding "likely" and only 33% responding "unlikely"[21]. To give more context, the survey was conducted by Ipsos in late 2020 15,700 responders in 31 countries. In total, 34% thought it was likely that they would get hacked, and 45% saw it as unlikely. Moreover, in the first half of 2022, 8.75% of Turks were using VPNs, putting the country at thirteenth place in the global comparison[22].

[18] Fortinet. "What Is an Attack Surface? Definition and How to Reduce It." Accessed October 28, 2022. https://www.fortinet.com/resources/cyberglossary/attack-surface.

[19] Jaiswal, Sarvesh. "Different Types of Cyber Security Threats & Attacks | Emeritus India." Emeritus - Online Certificate Courses | Diploma Programs (blog), June 30, 2022. https://emeritus.org/in/learn/different-types-of-cyber-security-threats/.

[20] Haan, J. de, E. Kuiper, Sonia Livingstone, and N. Sonck. "Digital Literacy and Safety Skills." LSE, 2011. http://eprints.lse.ac.uk/33733/1/Digital%20literacy%20and%20safety%20skills%20(lsero).pdf.

[21] Statista. "Share of Adults Who Think It Is Likely That Their Online Accounts Will Be Hacked into in 2021, by Country," December 2020. https://www.statista.com/statistics/1228062/opinion-online-security-worldwide/.

[22] AtlasVPN. "VPN Usage by Country 2022," 2022. https://atlasvpn.com/vpn-adoption-index.

However, the education level-based gap is also evident here as can be seen from the Ingev study :[23]

	I don't accept friend requests from strangers	I know how to protect my personal data on social media	I know how to use the privacy settings on social media sites.	I check the accuracy of the information I read on the internet from different sources.	I never share information like passwords with anyone.	I know how to create a strong password.	I use antivirus software
University and above	62%	72%	73%	70%	64%	67%	63%
High School	61%	64%	63%	57%	57%	55%	49%
Middle School	58%	54%	54%	50%	48%	49%	43%
Primary School	52%	38%	38%	38%	40%	30%	30%
No Education	44%	40%	40%	15%	26%	22%	19%

As was the case in the economic context, inequalities are also reflected here when it comes to digital literacy with respect to online safety. They are not limited to education levels either; the LSE study found that as digital skills develop with use, inequalities such as socio-economic status, age and gender still affect their development[24]. A study of high school students in Gaziantep and Kilis confirm this result. The authors found that male students scored significantly higher than females in terms of digital security awareness[25]. Bridging such gaps of inequality is key in overcoming deficiencies in digital literacy.

Awareness, skills and empowerment is the first of four fundamental principles that the OECD outlines for operational digital security risk management[26]. The Companion Document states that all stakeholders (that is, the government, public and private organizations and the individuals who, directly or indirectly, rely on the digital environment for all or part of their economic and social activities) should follow this principle as the ignorance of risks posed by one can be detrimental for others as well. A culture of digital literacy and awareness of online risks can be established if all stakeholders take action. Though national education is an essential component in building relevant skills and overcoming inequalities, the private sector as well as individuals should take initiative as internet security and privacy shortcomings in one spot can damage the integrity of other interconnected digital ecosystems.

[23] "DİJİTAL VATANDAŞLIK: Erişim, Tutum ve Davranışlar - Sunum." Ingev, University of Oxford, October 2021. https://s.gazeteduvar.com.tr/storage/files/documents/2021/11/02/ingev-calistay-sunum-dijital-vata-tifw.pdf.

[24] Haan, J. de, E. Kuiper, Sonia Livingstone, and N. Sonck. "Digital Literacy and Safety Skills." LSE, 2011. http://eprints.lse.ac.uk/33733/1/Digital%20literacy%20and%20safety%20skills%20(lsero).pdf.

[25] Talan, Tarık, and Cemal Aktürk. "Orta Öğretim Öğrencilerinin Dijital Okuryazarlık ve Bilgi Güvenliği Farkındalığı Seviyelerinin İncelenmesi." Kahramanmaraş Sütçü İmam Üniversitesi Sosyal Bilimler Dergisi 18, no. 1 (April 29, 2021): 158–80. https://doi.org/10.33437/ksusbd.668255.

[26] OECD. Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document. OECD, 2015. https://doi.org/10.1787/9789264245471-en.

DISINFORMATION AND DIGITAL LITERACY

What is disinformation and how is it connected to digital literacy?

One of the most relevant themes associated with digital literacy is disinformation. The purposeful spreading of false information has become an especially pressing issue in recent years.

The dictionary definition of disinformation is "false information deliberately and often covertly spread (as by the planting of rumors) in order to influence public opinion or obscure the truth"[27]. This definition also points out the difference between disinformation and misinformation. Misinformation is basically any incorrect information. Disinformation, on the other hand, covers also the intent behind spreading misinformation. Disinformation is usually targeted and has the goal of manipulating truth in line with certain interests. These interests may be political; disinformation can take the form of a covert smear campaign against an opponent. They can also be financial. Both traditional and digital media sources depend on audience engagement to monetize their services. Therefore, attracting a bigger audience via shocking or greatly exaggerated content may be beneficial for such actors. The blurring of the line between news and entertainment lately[28] has made this issue graver in particular.

It is almost impossible to think of disinformation and the digital sphere separately today, yet disinformation has a long history. In fact, its first documented occurrence can be traced back to 1274 BCE, when Ramesses II of Egypt deliberately portrayed his inconclusive battle as a great victory. He had scenes of triumph painted on numerous temple walls and circulated poems celebrating it[29]. More recently, after the advent of print media, fake news and hoaxes began to appear. The Great Moon Hoax of 1835, where a fabricated story about a moon civilization, helped catapult the New York Sun to a century of commercial success[30].

Therefore, it is possible to find examples of disinformation with the motives outlined above long before digital media became mainstream. These examples also provide us with the preliminary insight that simply restricting or banning channels of information dissemination, a response that many governments today are keen to jump to, is not an appropriate solution; temple walls were replaced with newspaper pages, and those in turn are being replaced by web pages and apps today. As long as channels of spreading information exist and evolve, so will those for disinformation.

Why digital disinformation causes so much concern today is its effectiveness, which is connected to its novelty. In a way, we are in a similar situation to when print media was booming in an environment of low literacy, before journalistic ethics were established. Digital social media is

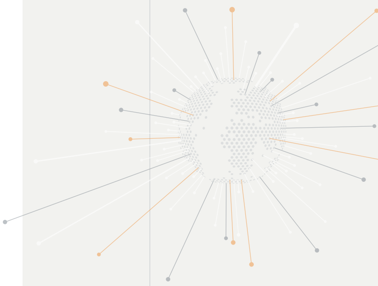
[27] Merriam-Webster. "Definition of Disinformation." Accessed October 18, 2022. https://www.merriam-webster.com/dictionary/disinformation.

[28] The Center for Digital Ethics and Policy. "From the Newsroom to the Television Screen: The Blurred Line between News and Entertainment," September 2019. https://digitalethics.org/essays/newsroom-television-screen-blurred-line-between-news-and-entertainment.

[29] Loktionov, Alex. "Ramesses II, Victor of Kadesh: A Kindred Spirit of Trump?" The Guardian, December 5, 2016, sec. Science. https://www.theguardian.com/science/blog/2016/dec/05/ramesses-ii-victor-of-kadesh-a-kindred-spirit-of-trump.

[30] Posetti, Julie, and Alice Matthews. "A Short Guide to the History of 'fake News' and Disinformation," n.d. https://www.icfj.org/sites/default/files/2018-07/A%20Short%20Guide%20to%20History%20of%20Fake%20News%20and%20Disinformation_ICFJ%20Final.pdf.

similarly expanding very fast today. Differently from the historical example, the ease of access to it is significant, yet low levels of digital literacy pose similar problems as the lack of actual literacy during the beginnings of print media. This is best evidenced by issues specific to digital media such as echo chambers and filter bubbles. Digital audiences have greater agency on the types of sources and channels they receive information from. In some cases, this customizability results in people creating an enclosed information environment unconducive to alternative or challenging opinions, reinforcing their pre-existing beliefs[31]. Echo chambers need not be created on purpose; sharing a digital social network with friends and family, generally people with similar worldviews, can result in an unnoticed echo chamber. A filter bubble, on the other hand, works similarly but is created by social media and search engine algorithms. Put simply, since most algorithms take input history as a basis for further recommendations and feed designs, they can also reinforce and amplify already held thoughts and beliefs. It is important to note that the evidence is mixed on the effects and prevalence of echo chambers and filter bubbles[32]. However, the identification of these phenomena points out that the disinformation problem has two layers. One is concerned with the technological and algorithmic side of disinformation where the choices of platforms and the functioning of algorithms affect the spread of false information. The other layer is about the agency of the audiences, their choices and overall interaction with online information, which points to the importance of digital literacy in overcoming the challenges posed by disinformation.



Types of disinformation

We have defined disinformation in relation to misinformation in the previous section. Before further breaking down the concept, it would be better to make clear the position of disinformation between misinformation and malinformation. As explained above, misinformation is the sharing of false information without any malicious intent. Malinformation, on the other hand, refers to the purposeful sharing of information that is accurate at its core but is presented in a way to serve personal or corporate interest rather than the interest of the public. Manipulating the context of a piece of information is a common method of malinformation[33].

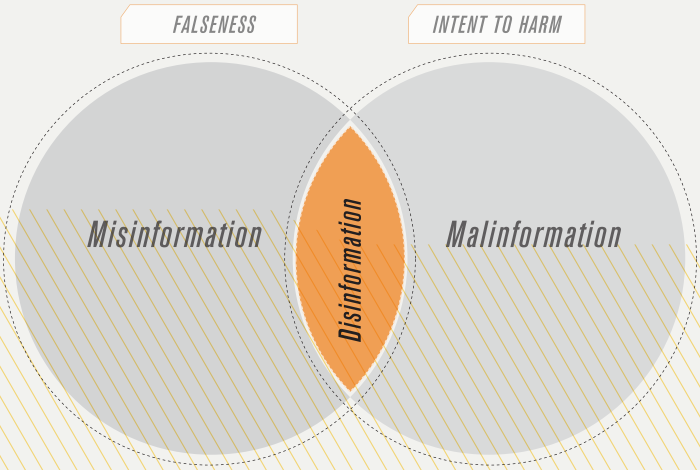
Disinformation can be situated at the intersection of misinformation and malinformation. It simultaneously involves the falsehood found in misinformation with the harmful intent of malinformation[34].

[31] Ross Arguedas, Amy, Craig T. Robertson, Richard Fletcher, and Rasmus Kleis Nielsen. "Echo Chambers, Filter Bubbles, and Polarisation: A Literature Review." Reuters Institute for the Study of Journalism, January 19, 2022. https://reutersinstitute.politics.ox.ac.uk/echo-chambers-filter-bubbles-and-polarisation-literature-review.

[32] Ibid.

[33] Staats, Beth. "Misinformation, Disinformation, Malinformation: What's the Difference?" Minitex, February 2021. https://minitex.umn.edu/news/elibrary-minnesota/2022-05/misinformation-disinformation-malinformation-whats-difference.

[34] Wardle, Claire. "Understanding Information Disorder." First Draft News. First Draft, September 2020. https://firstdraftnews.org:443/long-form-article/understanding-information-disorder/.



Misinformation sometimes follows from disinformation as the initial actor that shares the false information relies on an audience network that shares it without ill intentions. The example of intra-familial text message chains would be a good example of this. Moreover, the terms themselves are generally not mutually exclusive as it is not always easy to ascribe intent or to determine where factual truth ends and falsehood begins.

The 7 types of mis- and dis- information formulated by Claire Wardle is a good guideline that clarifies these concepts with greater detail[35].

Satire and parody: Though these are made purely for entertainment purposes, some may take them for reality and disseminate their content thinking it is true. Also, political satire and parody are sometimes part of disinformation efforts when it the veracity of the content is purposefully left blurry.

False connection: Sometimes, the headlines, visuals or quotes drawn from the content are intentionally misleading. This is mostly found in 'clickbait' content where the platform is interested in securing engagement with the content more than ensuring its truth.

Misleading content: Here, the information does not need to be false, yet its placement and presentation is done in a way to guide the audience towards embracing baseless perspectives or ideas regarding a person or subject. A particularly dangerous version of this is false truths where facts regarding a subject or person is mixed with speculation or theses presented as facts themselves. In those cases, it becomes even harder to separate fact from fiction.

False context: Genuine content is sometimes falsely contextualized to deceive audiences. This may be clipping a phrase mid-sentence to frame the speaker as supporting a view that they in fact do not. Another common example in Türkiye is the re-servicing of past news connected to current events to mislead people into thinking that they are happening simultaneously, or that there is a connection between them.

[35] Wardle, Claire, and Hossein Derakhshan. "Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making." Council of Europe Publishing, 2017. https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html.

Imposter content: Malicious actors sometimes pretend to be other, more credible sources to spread disinformation. During the pandemic, for example, there were many fake documents with the logos of public and international bodies pasted on them to give them an aura of authenticity. This is an especially pressing issue for Türkiye given the public's high levels of trust towards institutions perceived as serious and respectable.

Manipulated content: The means of manipulating information, images, and even sounds and videos are rapidly getting more advanced. Though a badly edited image may not be that hard to detect, new technologies such as deepfakes are particularly pernicious as they seek to bypass the basic human perception, which is the main way of determining truth.

Fabricated content: Lastly, there is the main channel of disinformation which is completely made-up content. We find this in fake news and conspiracy theories.

The ways of spreading false information are diverse, and combatting each of them requires different techniques and interventions. Moreover, new channels appear as technology and society evolves further. Though disinformation is spread with a myriad of personal or other motives, its socio-political dimension poses a significant threat to both democracy and social cohesion. This is also why governments and international organizations are particularly interested in fighting this phenomenon. Therefore, a discussion on how disinformation affects these subjects warrants its own section.

Implications for Democracy and Social Cohesion

The insidiousness of disinformation stems from the fact that it can reach its aims without necessarily convincing broad audiences. Thus far, we have mentioned echo chambers and filter bubbles as two examples through which people are informationally isolated from the broader digital public and subjected to one-sided and increasingly intense viewpoints which may cross over to false information. However, disinformation also carves space for itself by crowding out rational debate. When malignant actors disseminate disinformation in sufficiently high quantities, the amount of 'noise' within the debate may obscure true signals, hindering the communication of facts and ideas. In that case, audiences may simply decide not to consider any point of view, refusing to accord trust to any of the actors whether they are acting in the public interest or with the aim of spreading disinformation.

When applied to political discussions, this results in a 'retreat from politics' where citizens lose trust in institutions, not because they are convinced by the disinformation but because they simply do not know who to trust anymore[36]. The finding that 59% hesitate to express their views on the internet may be a sign that this is already taking place in Türkiye. In addition to the eroding effect that retreat from politics has on democratic institutions, by hindering fundamental features of democracy such as effective participation, informed electorate and citizen control of the agenda, it undermines the very idea itself[37]. Therefore, limiting freedom of speech and disincentivizing people from participating online would only amplify the effects of such disinformation.

In addition to depoliticizing more moderate groups, polarized political environments, such as those that appear during election campaigns, allow malevolent actors to deepen political cleavages through false information. In the US presidential elections of 2016, for example, it was found out that Russia-based groups founded social media pages catering disinformation to both sides with the aim of radicalizing them[38]. As it is illustrated in this example, foreign-sourced disinformation is also a big component of the broader issue as these actors can rely on the opacity of social networks to hide their origins.

Polarization does not invite disinformation only in the political sphere. The pandemic showed that social cohesion in general may be damaged by it. In Türkiye, multiple conspiracy theories regarding the virus, vaccines and 5G were fused to create a false narrative[39]. In short, proponents of disinformation spread stories that 5G network stations were instrumental in spreading the virus, and the vaccines included microchips that would be activated remotely through 5G. Paranoia of technology and vaccines was jointly introduced as a result[40].

[36] Butcher, Paul. "Disinformation and Democracy: The Home Front in the Information War." European Policy Centre, January 30, 2019.

[37] Dahl, Robert A. "Democracy - Features of Ideal Democracy." Britannica. Accessed October 21, 2022. https://www.britannica.com/topic/democracy/Features-of-ideal-democracy.

[38] K.N.C. "Digital Disinformation Is Destroying Society but We Can Fight Back." The Economist, January 17, 2020. https://www.economist.com/open-future/2020/01/17/digital-disinformation-is-destroying-society-but-we-can-fight-back.

[39] Yılmaz, Mert Can. "5G ile yeni koronavirüs arasında bağ olduğu iddiaları Türkiye'ye nasıl geldi?" Teyit, April 2020. https://teyit.org/5g-ile-yeni-koronavirus-arasinda-bag-oldugu-iddialari-turkiyeye-nasil-geldi.

[40] Yılmaz, Mert Can. "5G ile yeni koronavirüs arasında bağ olduğu iddiaları Türkiye'ye nasıl geldi?" Teyit, April 2020. https://teyit.org/5g-ile-yeni-koronavirus-arasinda-bag-oldugu-iddialari-turkiyeye-nasil-geldi.

By undermining a critical public health policy, this went beyond harming social bonds and in fact affected health and mortality. This example is also appropriate for bringing in the 'Big Disinformation' concept. Though it was not a central issue in Türkiye, the initial attempt in many countries to combatting pandemic-related disinformation was to attempt to limit debate around what was deemed as scientific truths. As the scientific consensus evolved so did the sanctioned narratives which were originally perceived as fixed, empirical truths. A good example is the WHO's recommendations regarding masks. It is argued that this approach of the establishment endorsing a narrative and forcing what it saw as disinformation out of the social sphere, only to recant and put forward a different one albeit with the same zeal actually boosted disinformation's traction by causing a loss of trust[41].

This is yet instance in which content-focused interventions are shown to be counterproductive. Before moving on to our policy recommendations that put debate-focused solutions at their center, a final discussion on Türkiye's recent Disinformation Law would help better situate our subsequent proposals.

Measures of disinformation in Türkiye

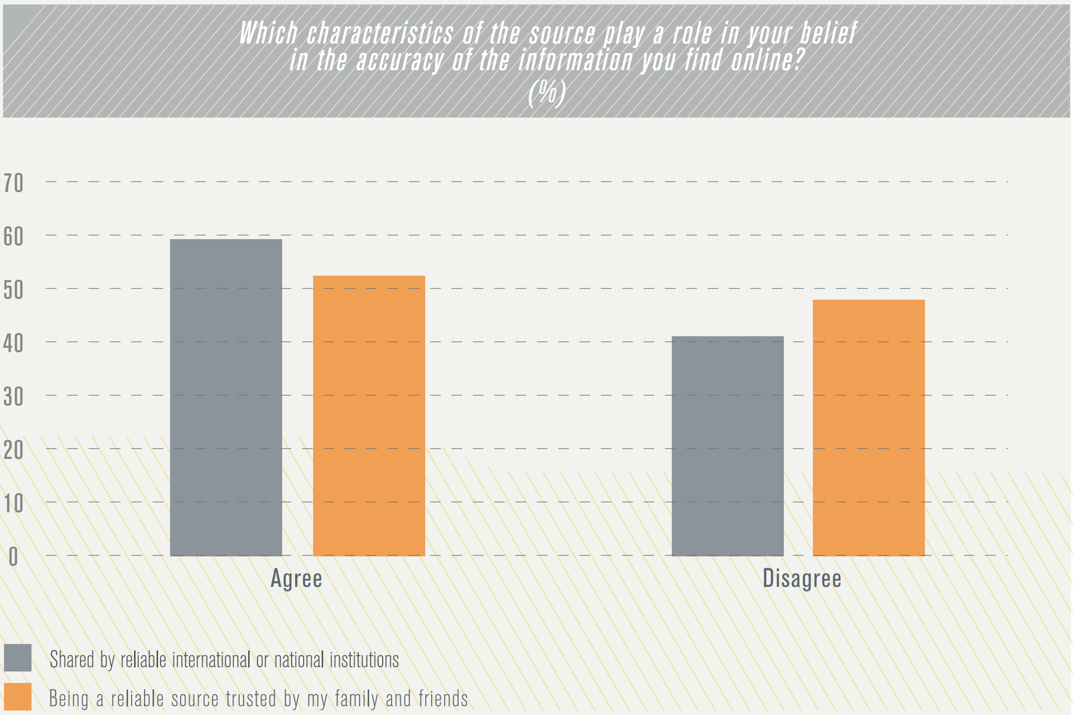
Before moving forward with the further analysis of disinformation in Türkiye, it will be better to provide an overview of the public's perspective of and interaction with this phenomenon. The following is a discussion of the research report titled 'New World, New Practices: Digital Literacy' by Türkiye Raporu[42]. The report is based on the findings of a survey with 1500 participants conducted in August 2022.

A vast majority of people in Türkiye are suspicious of the veracity of online information. 63% of the participants do not think that most of the information on the internet reflects truth. Skepticism towards digital information goes even beyond this as 58% think that trending topics on social media do not reflect reality. Here we get the first hint towards one aspect of disinformation which we will explore further in the following sections; though this figure may just be an extension of general distrust of online information, there may also be a tipping point where the perception that most information being encountered is false leads to the rejection of all online information.

Based on these results, it would not be an exaggeration to say that the majority of digitally active population assumes the worst when encountering new digital information. To overcome this, when forming a belief in the accuracy of online information, a majority of participants indicate that information is made more trustworthy when it is shared by a reliable international or national institution (59%) and when the source was seen as reliable by friends and family (52%).

[41] Friedersdorf, Conor. "How 'Big Disinformation' Can Overcome Its Skeptics." The Atlantic, Nisan 21, 2022. https://www.theatlantic.com/ideas/archive/2022/04/anti-disinformation-laws-social-media/629612/.

[42] "New World, New Practices: Digital Literacy." Türkiye Raporu, Ağustos 2022.



This illustrates how trust in institutions and social acceptance of a source influence its perceived trustworthiness. Therefore, we will look closer into the issue of fake/front organizations and experts, in addition to the echo chambers that can be catalyzed by close social circles. Indeed, it is not uncommon in Türkiye to receive a text message from a relative containing disinformation. Such family-based networks of information sharing are especially vulnerable to disinformation as the urge to inform and protect loved ones usually supersede rational concerns for verifying said information.

Another indicator of reliability may be the apparent popularity of the source that is spreading the information. However, 71% of the participants agree that the number of followers do not influence their trust in the information source. However, younger age groups are more influenced by the popularity of these actors. What's more, although 54% don't agree that information shared by a well-known person's account makes it more trustworthy, in the 18-24 age group this figure falls to %34.2. There is a similar dynamic with respect to the perceived trustworthiness of anonymous accounts. Though 71% overall say that they do not take such accounts seriously, this falls to 61.5% for those aged 18-24. The younger generations' interaction with online information is significantly different than that of the older ones. Therefore, special attention should be paid to the youth when analyzing disinformation.

In sum, Turks in general have a skeptical and cautious approach to digital information; at least that is how they self-perceive themselves to be. However, it should also be noted that 59% hesitate to express their views on the internet. The picture here points to some of the problems and solutions regarding disinformation. The majority of people do not take online information at face value yet they are also hesitant to express their opinions. Two inferences can be drawn from this. Either, disinformation is not that effective; it is widespread but not taken seriously, and people just do not act on countering the information. This is most likely not true, as disinformation has been proven to be influential in Türkiye (hate campaigns, racism etc.) The second, and more probable result is that though people are aware of the problem, and think they can insulate themselves from it, the lack of digital literacy, and the methods of disinformation prevents them from doing so. Hesitance to participating in the discussion online is just one example of this as it amplifies the vocal minority that spread disinformation.

Türkiye's New Disinformation Law

Türkiye's Omnibus Law number 7428, also known as the 'Disinformation Law', entered into force on the 18th October, 2022 subsequent to its publication in the Official Gazette. In addition to extra regulations and requirements for social media platforms, over-the-top platforms such as messaging apps, and online newspapers, a controversial aspect of the law is the way it criminalizes disinformation. According to the law, 'spreading misleading information' becomes a criminal act if four essential criteria are fulfilled simultaneously:

- Publicly disseminating false information,
- Relating to the country's internal and external security,
- With intent to cause worry, fear or panic,
- In a way that disrupts public order and general health.

The perpetrators face 1-3 years in prison if found guilty. Moreover, if they are found to have hidden their identities and/or if they operated within the framework of an organization, the penalty increases by 50%. Though the law defines disinformation as "the act of deliberately producing and disseminating false news", it does not provide legal definitions for 'misleading information', 'information that goes against the truth' or 'the motive to create anxiety, fear, or panic among the public' which are referenced throughout the law. Social network providers are obliged to provide user data to the legal authorities as part of the investigation, facing a 90% reduction in their bandwidth in the case of noncompliance[43].

The law has thus far been criticized for severely limiting freedom of speech and privacy. Organizations and bodies such as Human Rights Watch[44], the Venice Convention[45], and Article 19[46] have voiced concerns based on this evaluation. In the context of this report, the Disinformation Law contains shortcomings similar to those of other policy responses alluded to in the earlier sections. Essentially, the state assumes the responsibility for determining truth and intent, and criminalizes behavior based on vague criteria. This approach may prove to be counterproductive. Firstly, open-ended criteria such as 'the country's security' and 'public order' gives leeway to political interpretations, which is one reason why critics interpret this as a 'censorship law'. If the law's implementation is perceived as arbitrary, it may circumscribe the already shrunken space for public debate in the digital sphere. We mentioned that this is already one of the aims of disinformative actors. Combined with the fact that the state will also ascribe intent, increased hesitancy to participate on the part of well-meaning publishers of information, including most social media users, can also throttle the spread of accurate information. In the end, the counterbalance against disinformation stops being third-party fact-checkers, users and platforms, and becomes the organs of the central government. Until the necessary capacity and competence is built, it would not be surprising if state agencies and legal actors prove to be less efficient in combatting disinformation.

[43] Akkaş, Simge. "Dezenformasyon Yasası'nın Öngördükleri." Doğruluk Payı, June 8, 2022. https://www.dogrulukpayi.com/bulten/dezenformasyon-yasasi-nin-ongordukleri.

[44] Human Rights Watch. "Türkiye: Dangerous, Dystopian New Legal Amendments," October 14, 2022. https://www.hrw.org/news/2022/10/14/Türkiye-dangerous-dystopian-new-legal-amendments.

[45] Venice Commission. "Urgent Joint Opinion of the Venice Commission and the Directorate General of Human Rights and Rule of Law (DGI) of the Council of Europe on the Draft Amendments to the Penal Code Regarding the Provision on "false or Misleading Information" - Issued Persuant to Article 14a of the Venice Commission's Rules of Procedure," October 7, 2022. https://venice.coe.int/webforms/documents/?pdf=CDL-PI%282022%29032-e.

[46] ARTICLE 19. "Türkiye: Dangerous, Dystopian New Legal Amendments," October 14, 2022. https://www.article19.org/resources/Türkiye-dangerous-dystopian-new-legal-amendments/.

Moreover, since information (and by extension truth) is not static, criminalizing disinformation may exacerbate the issues related to 'Big Disinformation' as discussed before. Criminalization may foster deeper antipathy among people towards the government this way, even possibly increasing the attractiveness of conspiracy theorists.

POLICY RECOMMENDATIONS

For Participation in Digital Economy:

As Umberto Eco once said: "If you want to use television to teach somebody, you must first teach them how to use television." Today, the same is true for digital technologies in general, and the purpose of using them goes far beyond teaching. Digital literacy is essential so that Türkiye does not miss on the gains from digitalization. In addition to not taking advantage of potential benefits, failure in training the workforce to be digitally literate can also mean that millions of workers will be left with diminished opportunities when their jobs are automated. On the side of small businesses and retailers, digital literacy is still a bottleneck. The recent boom in e-commerce should therefore be seen as a glimpse of the success that can be achieved if this bottleneck is dealt with.

Improving digital literacy education is the first solution that comes to mind. This is essential for the retraining of the workforce and should be tackled by private firms, the public sector and non-governmental organizations alike, as its failure may have socio-economic effects of significant magnitude. However, this can only be a solution to one symptom that is visible today. A more fundamental solution is to integrate digital solutions in all areas of education. As mentioned, digital literacy includes skills that are not necessarily technical such as critical thinking, reading and writing. Modes of instruction that uses digital methods to teach these skills would increase students' digital literacy just as after some point the instruction of traditional literacy advances from letters and syllables to understanding texts and writing compositions. This should not be limited to national education, either. Any instruction on business or other economic activities should take into account digital applications of the materials taught.

For Internet Security and Privacy:

Our recommendations here share their spirit with to those for Digital Economy. The call for enhanced education also holds here. One thing that should be stressed, though, is that due to the high-impact nature of digital security breaches, digital literacy efforts in this area should go beyond education and formal training. Instead, we need to have a culture of digital safety where consciousness and basic skills about it are second nature. After all, we do not learn to lock our door at night at school. Daily security practices are so ingrained in culture that many pick them up intuitively. It should be the same in the digitalized world. As outlined in the appropriate section, this can be achieved through simultaneous action by all stakeholders: the government, public and private organizations and digital citizens in general.

Another thing that should be accorded special attention is that the inequality in digital literacy correlated with other inequalities such as socio-economic status and gender. The uneven distribution of net infrastructure may be playing a role in this. Nevertheless, this renders disadvantages groups more vulnerable to digital security threats. Since such threats can harm other people and systems than the victim, not mitigating such inequalities renders the whole ecosystems more vulnerable.

In the same vein, it has to be underlined that gender inequality also takes shape in the digital world. There is a significant discrepancy between women's and girls' digital adoption and that of men's and boys'. The International Telecommunications Union (ITU) reports that more than 50% of the world's women are offline. Beyond the accessibility issues due to the lack of smartphones and computers also lies the fact that women and girls do not engage in the full range of possibilities offered by the internet. In general, males use more digital services and platforms compared to females. However, the data revealing the underlying causes of these discrepancies is still nascent, especially among young generations; consequently, current research is not permissible to introduce extensive policy suggestions.Inequality in general education, lack of woman-friendly user design, abundant abuse on social platforms and vulnerable perception of females, and risk of being criticized by family members due to engaging usage of social platforms are all counted among contributing factors.

Comprehensive data-based research to determine the contribution levels of the previously mentioned factors among females from different socioeconomic and geographic backgrounds is strongly advised so that necessary policies can be applied in a tailored fashion.

For Disinformation:

For governments that want to combat disinformation and its destructive effects, the main issue can be defined as trying to prevent disinformation on the one hand, and creating solutions that enable societies to be more resilient to disinformation on the other. The approach adopted by democratic countries in the fight against fake news and disinformation is instructive. In these countries, penal sanctions on sources of disinformation or fake news are very limited and only valid for extreme (terrorist) cases. On the other hand, it was also preferred to impose obligations on the platforms that carry the news. For example, in Germany's NetZ law, platforms have an obligation to remove overtly false news within 24 hours. Likewise, in case of complaints, they have a one-week period. If they do not comply with this obligation, administrative fines are foreseen. There are also no measures such as access restriction. In France, sanctions for fake news only come into effect during election periods. In line with these restrictions, which started 3 months before the elections, responsibilities are brought to the platforms.

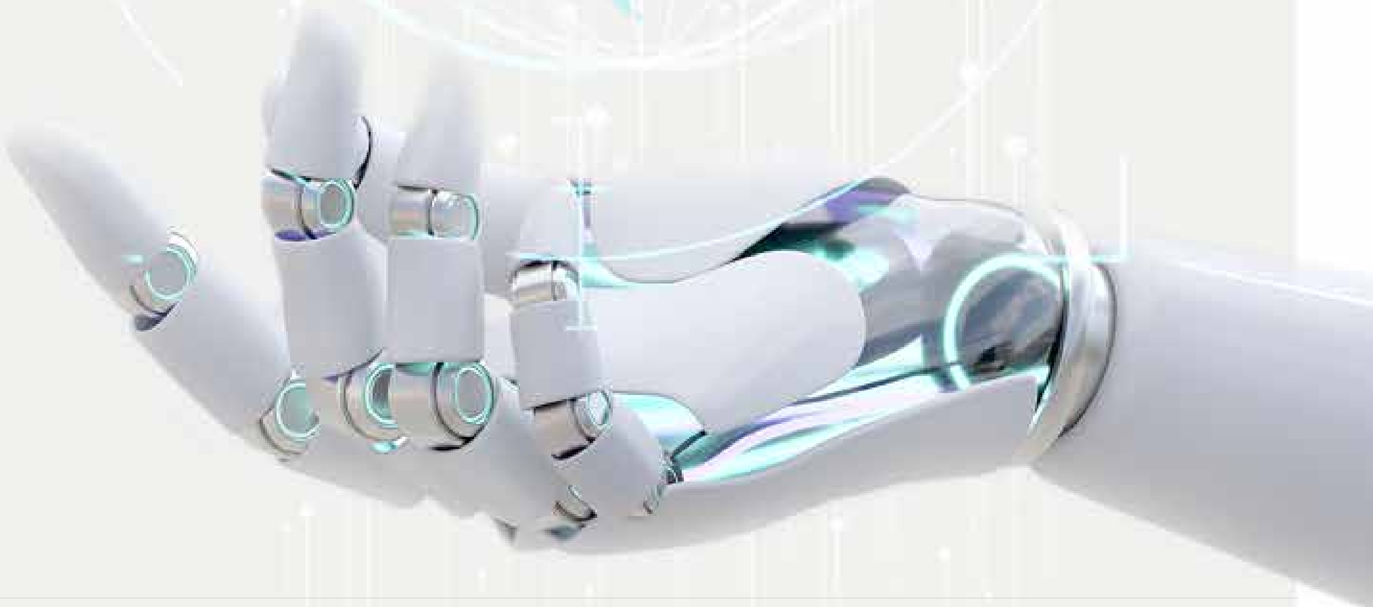
A similar approach is adopted by the European Commission, which acts as a Europe-wide rule maker to combat disinformation. As a result of the initiatives of the Commission, major digital platforms have become parties to a memorandum of understanding called "Code of Practice on Disinformation", which determines the principles of self-control in this field. In addition, with the “Digital Services Act” approved by the European Parliament this year, the responsibilities brought to major digital platforms in the name of combating disinformation have become valid at the level of all EU countries. The Commission has become the supervisory authority and, if necessary, the sanctioning authority of these responsibilities.

Strengthening the information ecosystem is another pillar of the measures taken at the public level to combat disinformation in Western democracies. In this framework, objectives such as strengthening digital literacy, supporting the so-called "fact checker" and trying to detect fake news, ensuring pluralism in the media and protecting freedom of expression are at the forefront. For example, in countries such as Sweden and Finland, the issue of digital literacy has been made a political target of great importance. In Finland, a curriculum for the development of media literacy has been created, and in Sweden, the theme of "digital skills" has been given as a compulsory subject in schools since July 2018.

As a result, it is now clear that new rules and mechanisms are needed to protect the information ecosystem. In this context, the legislator must also make a choice. As a matter of fact, a clear distinction has emerged between democratic countries and authoritarian systems in the fight against fake news. In authoritarian systems the laws give weight to the measures in which the public is at the forefront, coercive and police-dominated, harming the freedom of the press and expression, while democratic countries, on the contrary, are based on the guiding principle of the state and essentially oppose this manipulation of information. has embraced solutions where civil society, journalists, fact-checkers and platforms bear greater responsibility. This critical choice has been made in order to preserve the balance of security and freedom in the social contract at the core of democracies.

At their core, our policy recommendations depend on the fundamental belief that disinformation's criminalization is not a realistic or desirable solution. Conflating illegal content such as terrorist propaganda and child abuse, which is already criminalized, with disinformation opens the door to politically motivated limitations on free speech. The power to determine which content is false, dangerous for national security, is spread with an intent to cause panic in a way that disrupts public order and general health can be used to politicize the very scientific and rational methods of reaching truth. This, in turn, implies a state overreach as political and legal authorities not only determine what is true or false, but also ascribe intent to those who publish the (mis)information. Moreover, as stated before, disincentivizing people from participating online narrows the digital public space further, indirectly strengthening the 'retreat from politics' that disinformative actors want to achieve. Therefore, disinformation should have a policy definition instead of a legal one so that the issue can be solved through constructive policies instead of restrictions and bans.

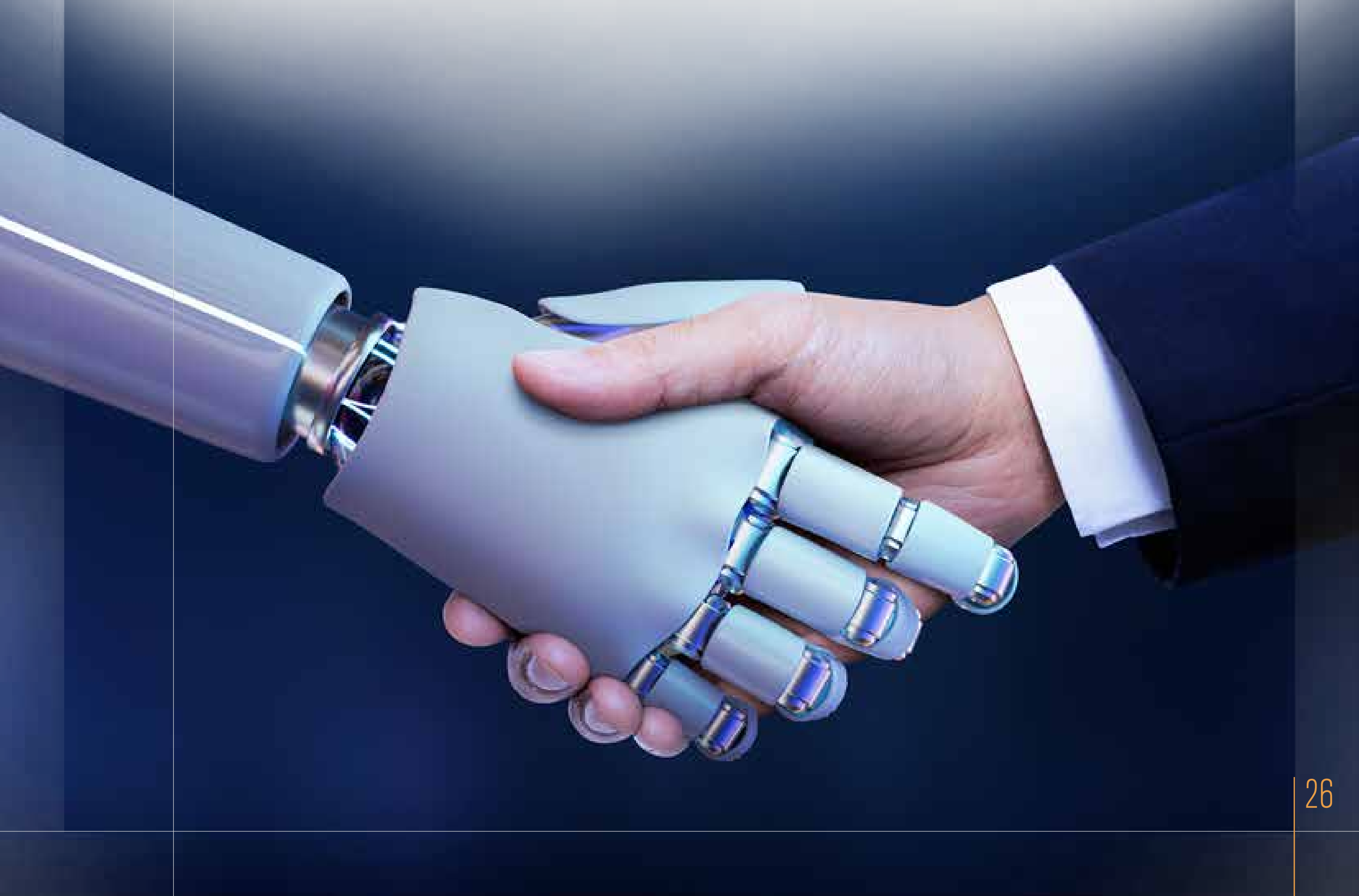
Finally, in addition to remedies targeting the symptoms of the problem, more general measures addressing the causes that make disinformation effective should be taken. Here, we return to the initial point made in this report; digital literacy through critical thinking is key to building consciousness towards all online information whether it be true and disinformative[47].



[47] Friedersdorf, Conor. "How 'Big Disinformation' Can Overcome Its Skeptics." The Atlantic, April 21, 2022. https://www.theatlantic.com/ideas/archive/2022/04/anti-disinformation-laws-social-media/629612/.

Separating objective facts from content targeting emotive responses, analyzing argumentative reasoning, and looking for evidence when evaluating information are key skills for both responding to digital content and information in general. This is also another reason why political/legal responses are inappropriate as they are inevitably based on the cultural and value judgements of the deciding authority. By focusing on digital literacy and critical thinking, the younger generations that we saw as the most vulnerable to disinformation can be educated to better respond to a world where false information is rife. Though the state is the main conduit for such education, civil society and platforms should also focus on building awareness on this.

In the end, the natural emotional response to shocking information and the financial incentive to publish marginal content stemming from this make it ultimately hard to overcome disinformation. Perhaps this is one reason why some governments have chosen the route of restriction and criminalization. However, top-down responses such as these can at best target the symptoms of disinformation. For disinformation to truly disappear, the demand characteristics of audiences, and the subsequent economic incentive of information suppliers to stay on the left edge of the policy line have to change. Enhancing digital literacy have a role to play on the demand side, yet the full solution to the problem needs policy measures that go beyond those that target disinformation specifically. It would be useful to remember this general framework in the context of the implementation of the newly adopted disinformation law in Türkiye.



01 // 2023

CYBER GOVERNANCE & DIGITAL DEMOCRACY 2023/01/EN

DIGITAL LITERACY IN TÜRKİYE:

PERSPECTIVES ON ECONOMIC, SECURITY AND DIS-INFORMATIVE ASPECTS

Centre for Economics
and Foreign Policy Studies

edam

Hare sokak No.16 Akatlar / İstanbul

T. +90 (212) 352 18 54
F. +90 (212) 351 54 65

info@edam.org.tr

// edam.org