TECHNOLOGY and MANAGEMENT CENTRE for DEVELOPMENT

UNIVERSITY OF OXFORD

ISSN 2045-5119

University of Oxford

Department of International Development

TMCD Working Paper Series

No. 083

Digital Citizenship in Turkey

Emre Eren Korkmaz[1], Türkay Salim Nefes[2], Aiden Slavin[3], Roxana Akhmetova[4],

Hüseyin Atakan Keskin[5], Johanna Bankston[6], Xiaolan Fu[1]

[1] Technology and Management Centre for Development, Oxford Department of International Development, University of Oxford; [2] Institute of Public Goods and Policies, Spanish National Research Council; [3] ID 2020 Alliance; [4] Oxford Department of International Development, University of Oxford; [5] Koç University, Turkey; [6] Artictic Freedom Initiative

Acknowledgement

The financial support from Facebook Inc. is gratefully acknowledged. The opinions and judgements expressed in the paper are the authors' views and do not necessarily reflect those of Facebook Inc. nor the University of Oxford.

Table of Contents

Chapter 1- Introduction to Digital citizenship

1.1 Digital Citizenship: The Concept

The digital age has created unprecedented opportunities for businesses and consumers, organizations and individuals. And yet, whilst modern technology has created unparalleled opportunities, it has also added new layers of complexity to persistent societal problems by giving them a digital dimension. Consequently, individuals and governments are being called upon to adapt old models of rights frameworks, regulations, and guidelines in order to keep pace with the societal changes brought on by the digital age. Importantly, the concept of citizenship itself, must adapt to reflect the increasing relevance of digital technologies to daily life in the modern era. The aim of efforts to apply citizenship principles and standards to the digital sphere – or a practice of 'Digital Citizenship– ' is to promote a fairer and more beneficial internet for all.

Digital citizenship can be defined as being an awareness and internalization of the standards and norms, rights and responsibilities associated with the use of digital technologies and the internet.[1] Most theorists who have attempted to adapt traditional citizenship principles to the digital era, base their adaptions on the ideals of kindness, respect, rights and responsibilities for all digital citizens. Concepts of digital citizenship can be categorized into three camps: educational, behavioral, and legal. *The educational category* corresponds to the requisite resources and skills necessary to participate in a digital society, including quality and consistent access to technology and basic internet literacy. *The behavioral category* is concerned with the norms associated with online interactions, such as treating others with respect when communicating online. The third category covers the *rights and responsibilities* belonging to all internet users as well as the legal norms which regulate business and data collection practices online.

While many of the topics in these categories - like etiquette, access, and responsibility in the public sphere - are as old as human civilization itself, societal changes brought on by rapid advancements in technology require citizenship concepts be made relevant to the digital age. As individuals, organizations, and government struggle to define fit-for-purpose principles for the digital era, many are looking to nine principles of digital citizenship – including access, commerce, communication, literacy, etiquette, law, rights and responsibilities, health and wellbeing, and security – developed by academics Mike Ribble and Gerald Bailey. Ribble and Bailey's nine principles are achieved through a multi-level approach which draws on legislation, policy, and advocacy to promote values of respect, education, and protection for all digital technology users.[2] For example, in order to foster values of respect in online communities, advocates and reformers highlight the need for standardized

[1] ISTE (2016) 'Digital Citizenship Defined.' Available at: https://otis.coe.uky.edu/DDL/Digital_Citizenship_Downloadable_10-2016_v11_web.pdf

[2] Ribble, M. (2017) 'Digital Citizenship in Schools,' Learning Network.' Available at: https://cpb-ca-c1.wpmucdn.com/learningnetwork.setbc.org/dist/d/592/files/2017/11/Digital-Etiquette-2mut8z0.pdf

etiquette and communication norms.[3] These values of respect are supported at the policy level through the promotion of programmes and requirements which guarantee digital access, literacy, and training on health and wellbeing online.[4] Efforts at the legislative level ensure the recognition of digital rights and standards for commerce and other conduct online. These approaches build upon each other and reinforce each other over time. In order to reach informed policy recommendations on how best to operationalize the above-described model of digital citizenship, it is important to understand the social and political issues which have stimulated the movement towards digital citizenship. Below, the tenuous relationship between digital technologies, the internet, and democratic principles is explained.

1.2 Acknowledging the Digital Divide

As an increasing number of political, social, and economic activities take place through digital technologies, access to these technologies can mean the difference between full and partial participation in the modern world. Inequalities in access to the internet and digital technologies, and the skills needed to use them, is popularly referred to as the 'digital divide'. The digital divide perpetuates inequalities between wealthy and impoverished nations, as well as between relatively advantaged and disadvantaged groups more generally. In this case, inequality is not necessarily determined by access to the internet alone, but also to the digital and information communication technologies (ICT) and competencies needed to go online. It also refers to the quality of access, technologies, and opportunities to develop digital literacies.

While global internet use has risen sharply in the past decade, disparities in access persist. As of 2020, only 50 percent of the global population have consistent, quality access to the internet.[5] The world economy is currently undergoing a new revolution characterized by increased digitization of both services and transactions. This revolution has fundamentally changed the way individuals socialize, conduct business, and organize their lives. Within the next decade, more than 30 percent of total economic activity is predicted to be mediated by digital platforms.[6] Inabilities to engage with the technologies that will facilitate growth will result in the exclusion of the digitally illiterate from the economy of the future. Lack of digital access will also stall development in the global south and widen wealth and education inequalities worldwide.

[3] Ribble, M. and Bailey, G. (2004) 'Digital Citizenship: Addressing Appropriate Technology Behavior.' Available at: https://eric.ed.gov/?id=EJ695788

[4] Georgetown ISD (2020) Digital Citizenship and Internet Safety Lessons for Students, Georgetown ISD, Available at: https://www.georgetownisd.org/Page/9780

[5] World Bank (2020) *Individuals using the internet (% of population) | data*. World Bank. Available at: https://data.worldbank.org/indicator/IT.NET.USER.ZS.

[6] Schenker, J. L. (2019) *The platform economy*, Medium, Available at: https://innovator.news/the-platform-economy-3c09439b56 (Accessed: 9 November 2020).

The digital divide also disproportionately affects marginalized groups. Intersectional factors, including race, class, and gender, further exacerbate inequalities in digital access. Obstacles to internet access, such as affordability and lack of education, may be compounded by sociocultural norms such as gender biases. Studies indicate that while the gender gap in digital interest is small at the elementary school level, it continuously widens throughout childhood, adolescence, young adulthood, and into adulthood.[7] The study found that in European tertiary education institutions, only 24 out of every 1,000 female university students graduate with a degree in ICT studies, of which a mere 6 out of those 1,000 female students go on to find employment in the ICT industry.[8] This gender disparity stems from negative and persistent stereotypes linked to young women's abilities in STEM, a lack of female leaders in the technology industry, and a lack of standardized technology education in secondary schools. As the global economy continues to digitize and automate, efforts to close the gender gap and other societal inequalities will be hampered by lack of investment in universal digital access and literacy.

1.3 Social Media, Democratic Principles, and Fundamental rights

Freedom House's 2019 'Freedom in the World' states that freedom of the media has deteriorated sharply since the beginning of the Twentieth Century.[9] While many early internet pioneers touted the potential of network technologies to extend access to freedoms of speech and expression to all, it has become increasingly clear that just as the internet can act as a democratizing force, it can also be abused to curtail individual expression.[10] One key avenue where this power struggle plays out in the digital age is social media.

In many ways, social media has helped the expansion of fundamental rights, such as access to information and free expression. In many countries social media offers an important outlet for activists and journalists to express opposition or to organize.[11] For example, the United States (U.S.) based activist group, Black Lives Matter, successfully used social media to organize protests despite alleged government attempts to block their mobilization.[12] In this and other instances, social media has proven an important tool for free speech and political mobilization. However, just as social media can offer a positive source of free expression, it can also be used to spread disinformation and

[7] Tarin Quiros, C. et al. (2018) *Women in the Digital Age*. European Commission.

[8] Tarin Quiros, C. et al. (2018) *Women in the Digital Age*. European Commission.

[9] Repucci, S. (2019) Media Freedom: A Downward Spiral, Available at: https://freedomhouse.org/report/freedom-and-media/2019/media-freedom-downward-spiral

[10] Repucci, Sarah (2019) Media Freedom: A Downward Spiral, Freedom House, Available at: https://freedomhouse.org/report/freedom-and-media/2019/media-freedom-downward-spiral

[11] Congressional Research Service (2019) Free Speech and Regulation of Social Media Content, Available at: https://fas.org/sgp/crs/misc/R45650.pdf

[12] Tufekci, Z. (2016) Technology in Global Activism, Uprisings and Social Movements, Available at: https://shorensteincenter.org/zeynep-tufekci/

bias.[13] One way this disinformation is spread is through the creation of internet bots which generate hundreds of fake social media profiles. The spread of disinformation by social media bots can be particularly harmful, because these profiles attempt to represent real interactions and can be difficult to detect as false.[14] By using these automated accounts to produce, or facilitate the spread of information, individuals and governments - can spread propaganda relatively easy.

A major rights issue related to free speech online is content moderation by social media companies. In a bid to deal with the rampant spread of inappropriate and harmful content online – such as cyberbullying - many countries are creating regulations which will hold social media and other internet service providers (ISP) liable for not efficiently removing this material from their platform. However, making ISPs liable for such content may cause them to excessively remove flagged content to avoid legal penalties. Content moderation by social media companies is thus plagued by an ethical dilemma – if content moderation is used too broadly and quickly, it may infringe many individuals' right to free speech, but if it is used too narrowly and without haste, disinformation or hate speech may spread widely to the detriment of many.[15] In order to realize an effective digital citizenship, governments must adopt and develop concepts of digital rights and responsibilities, security, and law in order to ensure that users are equipped to make informed, safe decisions about self-expression online and that their rights are protected.

1.4 User Data and Online Privacy

Privacy has long been a central issue in the theory and practice of governance. As a concept, privacy encompasses the respect and security of one's personal information, physical space, social life, and psychological well-being. On the internet, questions of privacy and security are extremely important - surveillance, data mining, unsolicited communications, harassment, and other undesirable behavior by organizations or individuals online may infringe a user's rights to privacy.[16]

The rapid and continued development of new digital technologies and internet features make questions of privacy and security difficult to answer. Many internet-users risk being surveilled and "identified" through data analysis. Identification refers to the determination of one's identity through the collection and analysis of data online; it is a process which can be performed without disclosure to the user through the triangulation of seemingly disconnected pieces of information related

[13] Repucci, S. (2019) Media Freedom: A Downward Spiral, Freedom House Available at: https://freedomhouse.org/report/freedom-and-media/2019/media-freedom-downward-spiral

[14] Caldarelli, G., Rocco, N., De Vigna, F. Del Petrocchi, M. and Saracco, F. (2020) The role of bot squads in the political propaganda on Twitter, Available at: https://www.nature.com/articles/s42005-020-0340-4.

[15] Rochefort, A. (2020) Regulating Social Media Platforms: A Comparative Policy Analysis, Available at: https://www.tandfonline.com/doi/abs/10.1080/10811680.2020.1735194?af=R&journalCode=hclw20

[16] Mekovec, R. (2010) Online privacy: overview and preliminary research, Available at: https://www.researchgate.net/publication/48371861_Online_privacy_Overview_and_preliminary_research/fulltext/02a6fe1e0cf2b4209299a340/Online-privacy-Overview-and-preliminary-research.pdf

to an individual across the internet. This data is difficult for users to control because most websites require the disclosure of personal information, which is collected and sold for a variety of purposes, ranging from personal use to targeted advertisements. Requesting and tracking of data has become so common on the internet and across digital technologies that users are often faced with byzantine privacy and use policies which ultimately force them to choose between preserving privacy or exchanging it for access to a service.

A major concern is that digital surveillance tools are used by companies to control, rather than benefit, users.[17] Findings of one study indicated that some surveillance practices influenced an individual long after engagement with the platform had ceased. Another major item of concern is the purchasing of external data by social media platforms to augment their own data collections. This level of data collection is alarming and calls into question the companies' abilities to respect user privacy in the absence of regulation.

Internet privacy is another source of concern for users and is regarded as an important rights issue. In a recent KPMG report, 97 percent of consumers stated that they considered data privacy important; 87 percent professed a belief in a human right to data privacy; 86 percent asserted that they believed data privacy to be a growing concern; and 54 percent stated that they did not trust private-sector companies to use their data ethically.[18] This mounting anxiety over online privacy is also reflected in the efforts of regulators, who are developing standardized rules and guidance to ensure user-data protection. Recent regulations from European Union (EU) and the U.S., including the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), are likely only the tip of the spear, signaling the coming of further data protection regulation from governments around the world.

1.5 Recognizing Digital Rights

Over the past several decades, calls have been made to adapt and harmonize existing rights frameworks with the features of the digital age by recognizing digital rights, or human rights related to the digital era or internet-use, through an official Declaration of Digital Rights.[19] Human rights can be understood as the full body of legal and ethical rights conferred to every person, derived solely from their personhood. As lived experiences increasingly overlap with digital technology use, the relevance and desirability of recognized digital rights only grows. However, conceptual and practical barriers have impeded their development. For example, rapid developments in technologies and digital practices seem to outpace efforts to codify digital rights, by making even the most recent

[17] Schyff, K., Flowerday, S., and Furnell, S. (2020) Duplicitous social media and data surveillance: AN evaluation of Privacy Risk, (Schyff, Flowerday, and Furnell 2020).

[18] KPMG (2020) New Imperative of Corporate Data Responsibility, Available at: https://advisory.kpmg.us/articles/2020/new-imperative-corporate-data-responsibility.html

[19] Mathiesen, K. (2020) Human Rights for the Digital Age, Available at: https://www.tandfonline.com/doi/abs/10.1080/08900523.2014.863124?journalCode=hmme20

digital rights concepts irrelevant with the creation of new applications and features. As digital media is relatively new, there are few long-term studies on the outcomes associated with internet-use, making most health and safety concerns unsubstantiated at present. This lack of data makes policies, let alone rights, difficult to formulate and realize.

Another important development in the field of human rights during the digital era is the entrance of digital evidence into human rights cases. There are documented cases of government actors using social media to collect information and facilitate arbitrary detentions and forced disappearances amounting to human rights violations. However, though social media interactions or data represents an important source of evidence in theory, the easily alterable nature of digital images or other media make evidence difficult to verify and accept in court.[20] As technologies continue to develop, digital rights will inevitably be pushed on the global agenda. While a Declaration of Digital Rights may be a way off, its creation is likely to be on the horizon. Until that time, digital citizenship provides a useful theoretical framework for ensuring fair and safe internet use.

Chapter 2: Digital Citizenship in Practice: Principles & Case Studies

In this section, the nine pillars of digital citizenship are developed. They are explored through case studies, and where possible, provide information and examples from Turkey.

2.1. Digital Access

Digital access is defined as "full electronic participation in society".[21] Access refers both to the resources (such as low-cost technology devices and broadband networks) which facilitate internet connection and the policies (such digital skills education, subsidies on digital devices for school, or initiatives to expand broadband connection to rural areas) that ensure equal and meaningful participation opportunities are available to all. Digital access is the most important principle of digital citizenship because it is the capstone upon which the other digital citizenship concepts are built.

The widening digital divide is one of the biggest factors influencing global inequality today. Traditionally, the digital divide has been articulated as the newest feature of the age-old dichotomy of the "have" and "have-nots" - in this case those with and without reliable internet connection and equipment. However, more contemporary discussions of the digital divide identify five factors symboli-

[20] Guberek, T. and Silva, R., (2014) "Human Rights and Technology:" Mapping the Landscape, Available at: https://www.fordfoundation.org/media/2541/prima-hr-tech-report.pdf

[21] Ribble, M. (2017) Digital Citizenship in Schools, Available at: https://cpb-ca-c1.wpmucdn.com/learningnetwork.setbc.org/dist/d/592/files/2017/11/Digital-Etiquette-2mut8z0.pdf

zing full digital access:[22]

* Quality of equipment, including devices and internet connection;

* Ability to use technologies autonomously, without supervision or intervention;

* Opportunities to develop digital skills;

* Systemic political and social support for equal access; and:

* Having purpose for technology, ability to identify new purposes for technology.

Despite the falling costs of mobile devices and greater coverage of broadband networks, women continue to have less access to mobile phones and internet technologies than men. This indicates that, additional factors – such as gender stereotypes which associate technology and digital skills with masculinity, or lack of educational requirements which ensure that girls stay in school long enough to develop digital skills – reduce women's abilities to participate meaningfully online.

The digital divide has become particularly evident in recent years with the rise of the platform economy.[23] The proliferation of mobile-operated, flexible jobs represents a so-called 'gig economy', or a triangular economic structure which links worker and customer through a digital platform. This change represents the integral role that digital technologies now play in the mediation of supply and demand.[24] It also signals that digital access will be a requisite for inclusion in the global economy of the future.

Digital divide should be addressed in Turkey, as well. ICT device access and ownership remain critically low in some parts of the country – as of 2018, only 50 percent of Turkish households reported having access to a computer or laptop at home.[25] While computer access remains relatively low in the country, mobile phone access is widespread and is reported to be the main device used to access the internet.[26] The digital divide in Turkey reflects wider inequalities which women, minorities, and low-income households face in the country. In particular, women in Turkey have been shown to access the internet and use computers at about half the rate of Turkish men, with the disparity growing wider with age.

[22] DiMaggio, P. and Hargittai, E., (2001) From the "Digital Divide" to "Digital Inequality": Studying Internet Use as Penetration Increases, Available at: https://culturalpolicy.princeton.edu/sites/culturalpolicy/files/wp15_dimaggio_hargittai.pdf

[23] Deloitte (2018) The rise of the platform economy, Available at: https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/humancapital/deloitte-nl-hc-reshaping-work-conference.pdf

[24] Deloitte (2018) The rise of the platform economy, Available at: https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/humancapital/deloitte-nl-hc-reshaping-work-conference.pdf

[25] 'Access to computers from home' (no date). OECD. doi: 10.1787/a70b8a9f-en.

[26] Yildiz, M. (2009) Digital Divide in Turkey: A general assessment' in Handbook of Research on Overcoming Digital Divides: Constructing an Equitable and Competitive Information Society. Information Science Reference.

Case Study on Digital Access

Digital access is a crucial determinant of overall economic inclusion, personal development, and upward mobility. For marginalized groups in particular, programmes supporting digital access are important equality initiatives. Turkey has seen the launch of many government-led and private-public sector partnership initiatives to expand digital access.

One tactic used to promote digital access is through the efforts to digitize government initiatives and policies, as well as to document, transfer, and process data more efficiently and effectively– the logic of this approach is that digitization will encourage individuals to learn new digital skills, or to laterally transfer digital skills they already possess. This technique contributes towards helping individuals to identify purposes for technology in their personal and professional lives. In recent years, the Turkish government has made major efforts to digitize its services by launching an 'E-Government' initiative. The primary goal of the e-initiative was to build base registries of data – such as census, land, property ownership, and company registration data – while the secondary goal was to strengthen the overall technical and administrative capabilities of Turkish government agencies by requiring them to manage these databases. At the same time, several government ministries initiated large scale IT projects aimed at bringing them up to speed with the digital age. This included efforts to automate many of their back-office processes. It also included the creation of a centralized system to connect and manage the data of all government agencies. The National Judicial Network (UYAP), Land Registry and Cadaster Information System (TAKBIS), Central Census Management System (MERNIS), Agricultural Information System (TARBIL), and several others were developed through this initiative. The E-Government initiative has not only served to increase the efficiency of government services, but it incentivizes Turkish citizens and residents to further develop digital literacy in order to access services.

2.2 Digital Commerce

Digital commerce refers to the buying and selling of goods and services through digital platforms.[27] All sectors of the economy, from education and health to transportation and construction, are changing as a result of digitization.[28] This is because digital technologies offer numerous advantages for businesses, including:

* Elimination of store-front costs, such as rent and building maintenance;

* Meaningful customer participation in the evolution of the service through easy-to-use feedback mechanisms and other forms of data collection; and:

* Increased labor productivity resulting from more flexible, remote work options.

[27] Kim, M. (2019) Digital product presentation, information processing, need for cognition and behavioral intent in digital commerce. Journal of Retailing and Consumer Services, 50: 362-370.

[28] Alina, N. (2016) Trends and Dimensions of Digital Economy. Analele Universităţii Constantin Brâncuşi din Târgu Jiu: Seria Economie. 1(4): 103-107.

The introduction of digital mediators into transactions has also revolutionized the economy by obviating the need for consumers to leave the house or contact a representative to make purchases. Now, product searches, purchases, and communication with retailers can take place remotely, and consumers can compare similar products online with ease.

The trend of online shopping and remote purchase has expanded at an astonishing rate in the past decade. For example, between 2017 and 2020, total online sales rose from 2 trillion USD to more than 4.2 trillion USD.[29] The number of digital shoppers also rose substantially, from 1.32 billion in 2014 to 2.05 billion in 2020.[30] The sharp increase in online activity in 2020 specifically is partially a reflection of the COVID-19 global pandemic, which saw nation-wide, mandatory quarantines as well as lengthy shelter-in-place orders. The pandemic demonstrated the heavy reliance of the modern economy on digital technologies – as individuals were subjected to shelter-in-place orders, businesses with sophisticated digital platforms profited while those without adequate digital infrastructures struggled to stay afloat. Additionally, consumers with access to digital applications were better positioned to purchase essential items while minimizing their risk of contracting COVID-19. Altogether, the trends of online consumption in the past decade, due in part to COVID-19, indicate that the digitization of consumption will only increase in the future.

Pre-COVID-19, Turkey was already seeing a 57 percent growth in annual revenue from digital commerce. However, in the first five weeks of the pandemic, digital commerce grew by an impressive 171 percent from the previous year. Further, research shows that around 41 percent of Turkish consumers have continued to purchase groceries and cleaning products through digital platforms even after the pandemic slowed, and 49 percent expressed their intention to continue practices of online shopping permanently.[31] These findings indicate that consumption practices in Turkey, which were already exhibiting favour for digital services, may have permanently adopted reliance on digital services into the norm as a result of the pandemic.

As digital commerce expands so has online banking and money sharing. The most common online payment methods in Turkey are card payments like Mastercard, Visa, and pre-paid card payments facilitated through a mobile phone or laptop.[32] BKM (Bankalararası Kart Merkezi) Express is a popular online payment system in Turkey that subscribers use to link their credit and debit cards to a virtual wallet.

[29] Neufeld, D. and Roghanizad, M. (2018) 'How Customers Decide Whether to Buy from your Website'. Harvard Business Review.

[30] Kristensen, E. (2020) "15 Eye-Opening Online Shopping Statistics for 2020". Sleeknote. Available at: <https://sleeknote.com/blog/online-shopping-statistics>.

[31] Nielsen (2019) "Nielsen, Türkiye'de Hizli Tüketim Ve E-Ticaretteki Son Trendleri Açikladi". The Nielsen Company (US). Available at: <https://www.nielsen.com/tr/tr/press-releases/2019/nielsen-announced-trends-in-fast-moving-consumer-and-e-commerce/>.

[32] Nielsen (2019) "Nielsen, Türkiye'de Hizli Tüketim Ve E-Ticaretteki Son Trendleri Açikladi". The Nielsen Company (US). Available at: <https://www.nielsen.com/tr/tr/press-releases/2019/nielsen-announced-trends-in-fast-moving-consumer-and-e-commerce/>.

As digital commerce permanently integrates into the modern economy it is important that individuals know how to shop, work, and conduct business safely online. Regardless of the method of online payment, making purchases and managing money online are associated with some risks of personal data collection, such as financial information or passwords, which may lead to identity theft by a cyber-criminal. Though online payment services offer extra layers of safety by eliminating the sharing of bank account information and insuring products in instances of theft or non-delivery, online transactions are still vulnerable. However, there are best practices in digital commerce which can empower individuals to protect their financial and personal information when online shopping. Generally, best practices before purchase include:[33][34]

1. Identify security indicators on websites, such as padlocks of key symbols;
2. Think critically about prices and deals, verify shipping and handling costs;
3. Read purchase agreements, return policies, and other information offered on a product;
4. Monitor online spending, as these purchases can be easy to lose track of;
5. Never offer personal or other sensitive information on unsecured websites;
6. Avoid using public Wi-Fi connections to make purchases; and:
7. Enable alerts or two factor authentications on credit cards for large purchases

The adoption of these practices, which essentially represent increased education on digital security related to e-commerce as well as increased standardization and regulation of e-commerce, can make overall experiences of e-commerce more productive and less risky for all actors involved. Digital citizenship training can provide the important educational basis necessary for individuals to efficiently navigate e-commerce networks.

Case study on digital commerce

While digital commerce provides many benefits for users, businesses, and workers, it is also associated with risks of identity theft as well as unauthorized or excessive purchasing. Children in particular can be vulnerable to financial scams or poor online spending habits. For example, during the COVID-19 pandemic, many parents in South Korea discovered that their children had run up hundreds to thousands of dollars' worth of online purchases on video games, social media, or through other online services, some of which were non-refundable or uninsured.[35] This was probably due to the ease of online purchases, which occur at the click of a button, and are therefore easy to disassociate with real money. However, the formation of poor online spending habits can be prevented

[33] *Commerce - digital citizenship* (2011). Heartland Area Education Agency. Available at: https://sites.google.com/a/aea11.k12.ia.us/heartland-digital-citizenship/commerce (Accessed: 6 November 2020).

[34] Federal Trade Commission (2014) "Tips for Using Public Wi-Fi Networks". Available at: <https://www.consumer.ftc.gov/articles/0014-tips-using-public-wi-fi-networks>.

[35] *South Korean dad loses US$115,000 from child's in-app purchases* (2020) *South China Morning Post*. South China Morning Post.

through education. Some of the examples listed on the Bankaroo website (an online, interactive platform designed to introduce children to concepts of online banking and spending) include:[36]

1. "Do some shopping with your child. This shows your child a few sites that are safe and gets the idea across that online shopping is fine when you take the right precautions. It also walks him through the process of searching for and finding items, reviewing an online cart, entering personal information, confirming order information and saving purchase confirmation pages or emails
2. Show your child how to log out of any retailer website that requires an account for purchase
3. Teach your child seven words: "What is this?" and "What do I do?" Encourage your child to ask both questions if he sees anything he isn't familiar with. Your answers will give him more information about how the sites and retailers are operating, thereby directing his next course of action on the sites.
4. Get your child in the habit of double-checking item and shipping totals. Mistakes sometimes happen, and you don't want your child to go through the checkout process so automatically that he doesn't catch errors. A good thing to check is whether the number of each item ordered is correct."

These examples demonstrate ways to operationalize best practices in e-commerce through proactive, and interactive, education.

2.3. Digital Communication

Digital communication is the electronic transmission of information with the aid of digital services such as computers, cellphones, and similar devices. Online communication is facilitated via email, social media, online news, videos, and websites. The prolific rise in popularity of online communication comes with both advantages – such as increased access to information as well as social connections – and disadvantages – including heightened susceptibility to disinformation – which modern, digital citizens must be able to navigate.

Digital technologies transformed traditional media by creating a more complicated ecosystem of information sharing, in which traditional media is now presented alongside information produced by entertainment companies, businesses, and individuals on internet search engines and social media platforms. Traditional news outlets hold themselves to high standards with regards to factual accuracy and accountability, which means that readers can generally presume that the reporters have done their due diligence when researching a topic. However, on social media, information from news sources is presented alongside other forms of media with much lower due diligence standards (or none), including entertainment and individual user posts. Because these sources are

[36] 'Teaching your child the dangers of internet shopping – bankaroo :: virtual bank for kids' (no date). Available at: https://www.bankaroo.com/teaching-your-child-the-dangers-of-internet-shopping/ (Accessed: 6 November 2020).

presented side by side, the overlap may frustrate a user's ability to separate verifiable information from personal opinions, entertainment, and other forms of media that they encounter as they scroll through their feed. This change in the way that media is presented and accessed has led to a crisis in information legitimacy, the magnitude of which has led some to dub this period the 'Post-Truth Era'. As a growing number of users struggle to identify legitimate news source, public opinion may be increasingly informed by illegitimate sources – or fake news. Fake news can be categorized into five types:[37]

* **Clickbait** - content which uses misleading headlines and/or graphics to attract viewers and generate revenue through advertisements on the article;
* **Satire** - entertainment content which uses sarcasm, fake stories, and/or humour to make an argument, or embarrass an individual or entity;
* **Propaganda** - content deliberately created to bias an audience or promote an agenda;
* '**Sloppy news**' - news media with sub-standard due diligence practices, known for presenting gossip or rumors as if they were verifiably true; and:
* **Biased/slanted news** - news media which strategically presents certain information, while omitting other relevant facts, in order to create a narrative that supports the author's political or personal agenda

Disinformation – or the deliberate spread of false or misleading information disguised as a credible source – is another key digital communication issue.[38] Disinformation includes falsified information and conspiracy theories (described further in chapter three). False news is generally spread for social, political, or financial gain on the part of the originator. While false news, in the form of gossip, propaganda, and rumors, has existed throughout history, its political significance is being taken more seriously in the Post-Truth Era because, with more than 4.5 billion active internet users as of 2020, the spread of misinformation is more efficient and pervasive than ever and more difficult to control due to censorship and free speech concerns.[39] Before digital communication, print media, radio, and television were a communities' main source of information. As described above, these outlets were held to high standards for due diligence in reporting, and the costs and associated with print journalism, as well as T.V. and radio airtime, generally prevented non-legitimate news agencies or independent actors from participating in the production of information. However, the advent of the internet made news and media production virtually free and widely accessible to any person

[37] Pennycook, G. and Rand, D. G. (2019) Fighting misinformation on social media using crowdsourced judgments of news source quality. Proceedings of the National Academy of Sciences of the United States of America, 116(7): 2521-2526.

[38] Vargo, C. J., Guo, L. and Amazeen, M. A. (2018) The agenda-setting power of fake news: A big data analysis of the online media landscape from 2014 to 2016. New Media & Society, 20(5): 2028-2049.

[39] Internet World Stats 2020 (No Date) Internet World Statistics Usage and Population Statistics. https://www.internetworldstats.com/stats.htm

or entity hoping to participate in news production, regardless of whether they hold their reporting to any due diligence standard.

Illegitimate news and disinformation are particularly salient issues in Turkey, whose citizen population is purported to be one of the least trusting populations of news media in the world.[40] In a recent study, 45 percent of Turkish respondents reported a belief that they could not trust "most news, most of the time"[41] In a Reuters study, 49 percent of Turkish respondents stated that they had encountered fake news online in the past week, compared to only nine percent of Germans respondents.[42] When asked where they were receiving news, Turkish respondents overwhelmingly indicated a reliance on online media as a news source, with two thirds stating that social media was a major source for news.[43] Turkey is among the top 15 countries with the longest time of both daily internet and social media usage – research indicates Turkish residents spend, on average, one and half more time online than residents in the United States and China.[44] Given the rampant distrust in media in Turkey, as well as the widespread reliance on online and social media as a major news source, the news legitimacy and disinformation crises should be at the top of Turkey's policy agenda in the coming decade.

Some individuals attribute the distrust in media in Turkey to censorship and violations of the right to free speech online by authorities. In 2018, more than 110,000 Turkish accounts were examined by the police and more than 7,000 people were detained over their social media posts.[45] Turkey has previously banned some of the most-used information communication websites in the world, including Wikipedia, Twitter, and YouTube.[46] These practices indicate that Turkish citizens and residents may benefit from training in online communication which include information about their rights to free speech online and how to effectively use privacy settings on social media accounts.

[40] Fletcher, R. (2018) "Misinformation and Disinformation Unpacked". University of Oxford Reuters Institute for the Study of Journalism. Available at: <http://media.digitalnewsreport.org/wp-content/uploads/2018/06/digital-news-report-2018.pdf>.

[41] Fletcher, R. (2018) "Misinformation and Disinformation Unpacked". University of Oxford Reuters Institute for the Study of Journalism. Available at: <http://media.digitalnewsreport.org/wp-content/uploads/2018/06/digital-news-report-2018.pdf>.

[42] Nic, N., Fletcher, R., Kalogeropoulos, A., Levy, D.A., and Nielsen, R.K., (2018) Reuters institute digital news report 2018. Reuters Institute for the Study of Journalism.

[43] Nic, N., Fletcher, R., Kalogeropoulos, A., Levy, D.A., and Nielsen, R.K. (2018) Reuters institute digital news report 2018. Reuters Institute for the Study of Journalism.

[44] Nic, N., Fletcher, R., Kalogeropoulos, A., Levy, D.A., and Nielsen, R.K. (2018) Reuters institute digital news report 2018. Reuters Institute for the Study of Journalism.

[45] Human Rights Watch (2018) "Turkey: Crackdown on Social Media Posts". Available at: <https://www.hrw.org/news/2018/03/27/turkey-crackdown-social-media-posts>.index-2017.pdf.

[46] BBC (2017) "Turkish authorities block Wikipedia without giving reason". Available at: <https://www.bbc.com/news/world-europe-39754909>.

Widespread consumption of illegitimate news and disinformation may erode public trust in legitimate reporting and journalism, which is an important feature of a healthy democracy. It may also lead to increased partisanship among citizens and lead to civil distrust and unrest.

The ability to evaluate media sources is an important 21st century skill. Digital citizens must be able to identify the characteristics of fake news and disinformation, understand the difference between legitimate news sources, opinion, and entertainment, and be able to critically evaluate information and media encountered online. They must also understand their rights to free speech online, understand the lifespan and reach of statements made online, and be able to protect their personal information from unwanted viewers. When reading content online, digital citizens should ask themselves the five 'w' questions - who, what, when, where, and why – when evaluating news.[47] Below are features to look for and consider when critically evaluating news sources based on the five 'w' questions.

1. **Who** – author's credentials such as their name, organization, affiliations, and expert status;
2. **What** – balanced and complete information, external sources, neutral tone ;
3. **When** – date of publication (to determine relevance);
4. **Where** – website appearance and maintenance, excessive advertisements, content on social media should be evaluated with extra care; and:
5. **Why** – purpose of source (whether to sell, inform, entertain, or persuade), endorsements, recommendations

While illegitimate information and disinformation are a prevalent issue globally, the development of critical evaluation skills can help digital citizens to more successfully identify invalid news and raise awareness about the reach and impact of online speech.

Case Studies on Digital Communication

Online communication skills resources and training are helpful ways for individuals to learn about disinformation. In Turkey, where distrust in media is rampant, resources have been created to help internet-users fact check information or verify news. One such resource is Teyit, an independent fact-checking website that draws on open-source material and journalism techniques to verify online content (news, social media posts, stories, conspiracy theories, and other materials).[48] The site has gained national prominence and is generally seen as a neutral source. Teyit offers tips and articles on how to be more media literate in the new digital age.[49] They also share videos demonstrat-

[47] Lotero-Echeverri, G., Romero-Rodríguez, L., and Pérez-Rodríguez, M. (2018) Fact-checking vs. Fake news: Confirmation journalism as a tool of media literacy against misinformation. Index.comunicacion, 8(2): 295-316.

[48] Teyit.org (2020) "Teyit.org." Şüpheli Bilgileri Inceleyen Doğrulama Platformu. Accessed September 28, 2020. https://teyit.org/nedir.

[49] Teyit.org. (2017) "Medya Okuryazarlığınızı Geliştirmek Için Takip Etmeniz Gereken 5 Adım: Teyit." Şüpheli Bilgileri Inceleyen Doğrulama Platformu. Accessed September 28, 2020. https://teyit.org/medya-okuryazarligini-gelistirmek-icin-takip-edilmesi-gereken-5-adim.

ing how to perform the techniques they use to analyze the accuracy and authenticity of a post. For example, the website offers a tutorial on how to use Reverse Image Searches to determine when an image first appeared online, where it was taken, in what contexts it has been used, and how often it has been used.[50] This is a helpful resource for the public in Turkey to verify viral photos and videos which purport to have been taken there.

Another useful fact-checking website in Turkey is Doğrulukpayı**,** which focuses on statements made by Turkish politicians.[51] The site tracks information demonstrating whether politicians have fulfilled promises they made during their campaigns on a 'government-meter' (*hükümetre)*, in hopes of helping Turkish voters to make more informed decisions in elections. Given Turkey's high level of distrust in media and belief in the rampant spread of fake news, which Turkish politicians across the political spectrum are accused of participating in, Dogrulukpayi is a resource which is supporting the Turkish public in making informed choices while also, and importantly, reducing political polarization caused by fake political news.

2.4. Digital Literacy

Digital literacy refers to the competencies necessary to use communication technologies to search, create, and share information online. Like digital access, digital literacy is also a requisite to equal and advantageous internet-use.

In developing countries, individual internet connectivity is rapidly increasing. The number of unique subscribers to mobile internet technologies skyrocketed from 728 million in 2010 to 1.8 billion in 2014.[52] However, despite the expansion of internet access and the falling costs of digital devices, many novice digital technology users exhibit low digital literacy. Without the basic competencies associated with internet services, such as an understanding of how to operate a search engine and evaluate results, an individual will be unable to use digital resources with purpose. Digital literacy is therefore essential to closing the digital divide – for digital access to be meaningful, digital competencies must spread in tandem with connectivity.[53] Below is a list of five critical functional skills to internet access and usage:

* Ability to install and configure internet access on a local device;

[50] Teyit.org. (2020) "Bellingcat Tersine Görsel Arama Rehberini Türkçeleştirdik: Teyit." Şüpheli Bilgileri Inceleyen Doğrulama Platformu. Accessed September 28, 2020. https://teyit.org/bellingcat-tersine-gorsel-arama-rehberini-turkcelestirdik.

[51] Weise, Zia. (2019) "Fact-checkers Seek out Grain of Truth in Turkey's Fake-news Onslaught." POLITICO. Accessed September 28, 2020. https://www.politico.eu/article/turkey-fact-checkers/.

[52] GSMA (2015) Accelerating Digital Literacy : Empowering women to use the mobile internet, https://www.gsma.-com/mobilefordevelopment/wpcontent/uploads/2015/06/DigitalLiteracy_v6_WEB_Singles.pdf

[53] GSMA (2015) Accelerating Digital Literacy : Empowering women to use the mobile internet, https://www.gsma.-com/mobilefordevelopment/wpcontent/uploads/2015/06/DigitalLiteracy_v6_WEB_Singles.pdf

* Capacity to use both familiar and novel applications, software, and online services;

* Capacity to consume, evaluate, discover, and access content;

* Ability to create and share original content, including content developed on social media;

* Capacity to install and configure settings on familiar and novel applications.

These five functional skills represent basic, yet foundational components of digital literacy. Further digital skills should be cultivated over time, allowing the user to transition from minimally to highly literate. Additional digital skills include mobile technical literacy (including the ability to use calendar, calculator, camera, and text apps), mobile internet literacy (including the ability to browse for unfamiliar and novel content online) and advanced mobile internet literacy (including the ability to generate, browse, and download online content across all relevant local devices). Figure 3 depicts the complete set of skills and capabilities symbolizing digital literacy.[54]

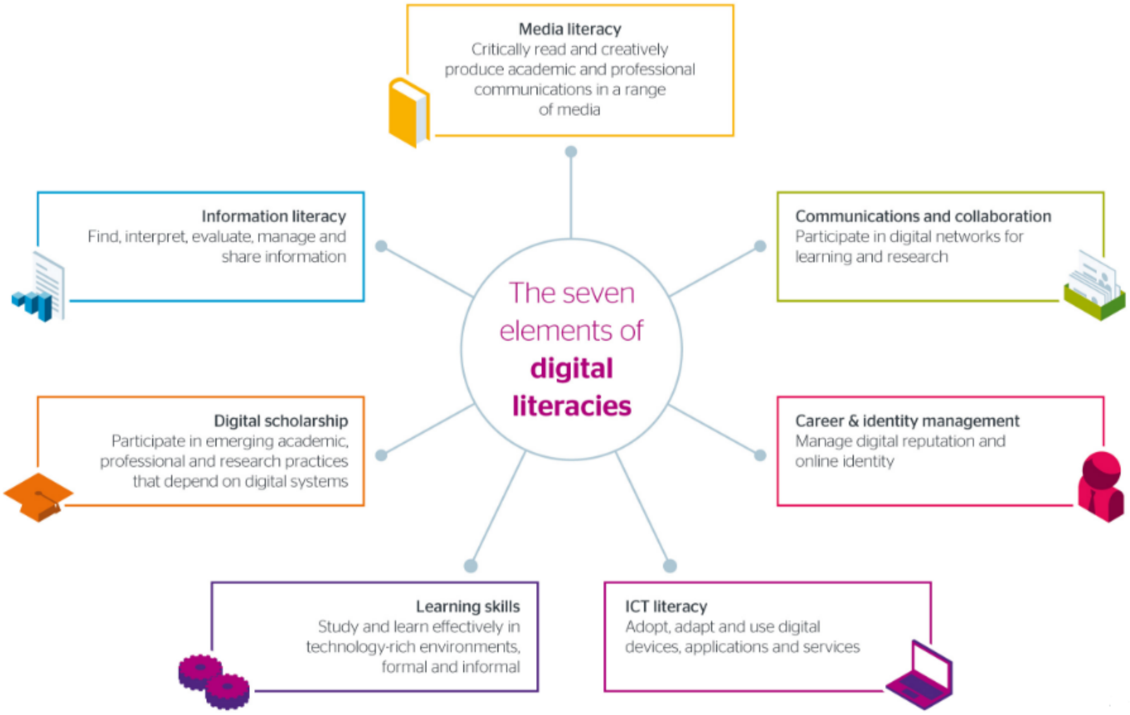

Media literacy
Critically read and creatively produce academic and professional communications in a range of media
Information literacy
Find, interpret, evaluate, manage and share information
Communications and collaboration
Participate in digital networks for learning and research
The seven elements of digital literacies
Digital scholarship
Participate in emerging academic, professional and research practices that depend on digital systems
Career & identity management
Manage digital reputation and online identity
Learning skills
Study and learn effectively in technology-rich environments, formal and informal
ICT literacy
Adopt, adapt and use digital devices, applications and services

Figure 3.: Digital literacies in a Seven Elements Model. **Source:** Jisc (2014)

Despite efforts from both the private and public sectors to promote digital literacy on a global scale, the realization of universal digital literacy has been impeded by several barriers. Critical among these is the phenomenon of ‘application islands’ in which individuals develop basic digital literacy skills with one or a few applications and, rather than developing new competencies over time, they return exclusively to the familiar applications.[55] Facebook and WhatsApp are commonly cited as

[54] Jisc (2014) Developing Digital Literacies, Available at: https://www.jisc.ac.uk/guides/developing-digital-literacies.

[55] UNESCO (2019) UNESCO Guidelines for Digital Inclusion for Low-Skilled and Low-Literate People, Available at: https://en.unesco.org/sites/default/files/unescopearson_draft_guidelines_for_digital_inclusion.pdf

popular application islands. Though many users associated with application islands possess laterally transferrable digital skills, they fail to recognize this transferability. Factors which contribute to the persistence of application islands include the following:

1. 'Application islands' are reinforced by limited social circles, which tend to include many users who exhibit digital literacy on only one, or a few, applications[56];
2. Outside of purchase, installation, or configuration, many users limit their troubleshooting efforts to their social circles, without seeking out assistance from internet service providers, or mobile network operators, themselves; and:
3. 'Application islands' are associated with a constrained mental model of the internet, meaning that users are unfamiliar with basic internet features such as web browsers, URLs, and search engines

This example demonstrates the highly social, and therefore personal, nature of digital literacy. It also may indicate that digital knowledge is shared in social groups in much the same way that social or cultural norms and knowledge are shared. Discussions of digital literacy highlight the potential of digital skills education to facilitate more purposeful internet use among individuals with new-found access.

Case Study on Digital Literacy

The development of digital literacy skills empowers individuals to take full advantage of the opportunities of the digital age to further personal, educational, and professional interests. Like traditional literacy, digital literacy is most likely to be achieved through systemic support – through policies and ample opportunity - especially for marginalized groups.

In Turkey, digital literacy became a major issue during the COVID-19 global pandemic. The effects of the global pandemic took a disproportionate toll on women in Turkey, many of which participate in the economy as textile vendors in local markets. Shelter-in-place orders in Turkey meant that many female textile vendors were unable to sell their products during the pandemic months unless they had the skills necessary to run their business online. For those without access to digital sale platforms, inability to work during the pandemic led to income loss as well as food and housing insecurity. However, this was not the case for all female textile vendors in Turkey. Beginning in 2019, UN Women partnered with the Southeastern Anatolia Project Regional Development (GAP) Administration to run digital skills workshops for local women at 44 different Multi-Purpose Community Centers.[57] The workshop imparted participants with skills in coding, computer literacy, and

[56] GSMA (2015) Accelerating Digital Literacy : Empowering women to use the mobile internet, Available at: https://www.gsma.com/mobilefordevelopment/wpcontent/uploads/2015/06/DigitalLiteracy_v6_WEB_Singles.pdf

[57] UN Women (2020) *Digital Skills help Turkish women maintain an income amid COVID-19*. UN Women | Europe and Central Asia. Available at: https://eca.unwomen.org/en/news/stories/2020/5/digital-skills-help-turkish-women-maintain-an-income-amid-covid-19 (Accessed: 7 November 2020).

digital product sales and marketing. Many of the workshop participants were able to use skills gleaned through the workshops to develop online stores and marketing strategies which allowed them to sell textiles remotely. These developments not only increased their overall business success, but also secured their incomes during COVID-19. One participant noted that while she had used social media for years, she was unable to identify and seize the marketing potential in these tools until she took the UN Women course. The success of this initiative demonstrates the impact that digital literacy can have for furthering equality and meaningful participation in society.

2.5 - Digital Etiquette

The internet has enabled the formation of new relationships between users who may engage in meaningful online communities via social media platforms, internet forums, or direct messaging. Just as with offline relationships, the formation of new connections and the maintenance of existing relationships online is contingent upon the appropriateness and quality of interactions. However, these characteristics can be difficult to decipher in online interactions because the context and social cues which humans generally rely on in face-to-face interactions, including facial expression, tone of voice, intonation, and body language are concealed by the digital interface on which they engage. As a result, actions and comments made online are inherently more ambiguous than their offline parallels. Due to the ambiguous nature of online communication, the norms and standards of politeness and acceptability online - or digital etiquette - are important features of a safe and equitable internet.[58]

Online norms are formed through a mix of organic social processes and authoritative intervention. Internet platforms provide the basic social architecture of a website by providing options and parameters for user actions and interactions.[59] For example, Instagram provides users the options to participate in photo and video sharing but places a limit on the number of media one can upload in a single post, thus establishing a parameter for user action. Other parameters include user-guidelines or community rules, which, if violated may result in the removal of content by site moderators, the banning of a particular user from the site, or if the violation is sufficiently serious the involvement of authorities. The way that users choose to interact with each other within given parameters of various digital spaces forms the basis of internet communication norms, which change with site usership over time.[60] However, online norms formed organically through user interactions may not be

[58] Chai, C., Cen F., and Sun, L. (2013) International conference on intelligent human-machine systems and cybernetics. Los Alamitos, CA: IEEE Computer Society.

[59] Brooks, B. (2015) 'Effects of Organization-Level Internet Governance: A mixed-methods case study approach to social media governance'. ProQuest LLC. PhD Thesis, Department of Media and Information Studies, Michigan State University.

[60] Brooks, B. (2015) 'Effects of Organization-Level Internet Governance: A mixed-methods case study approach to social media governance'. ProQuest LLC. PhD Thesis, Department of Media and Information Studies, Michigan State University.

optimal for the formation of a safe and equitable internet due to the challenges associated with this approach.

One challenge associated with online interaction is the propensity of individual text-based interpretation to lead to misunderstandings and conflict. Because communication technologies and platforms are relatively new, user-norms are not concrete, and a wide range of behaviors are employed by users with different levels of digital literacy and technology familiarity. Such a range of behaviors requires constant interpretation on the part of the message recipient. However, incorrect text-based interpretations may result in professional and/or personal misunderstandings which can have serious repercussions for an individual, organization, or company. For example, in 2001 a CEO at Cerner sent a message to hundreds of his employees to boost office management of under-performing employees, however the aggressive wording of the email resulted in backlash from the employees. The message read:

> “We are getting less than 40 hours of work from a large number of our 'employees'. The parking lot is sparsely used at 8:00 a.m.; likewise at 5:00 p.m. As managers, you either do not know what your EMPLOYEES are doing; or you do not CARE. You have created expectations on the work effort, which allowed this to happen inside Cerner, creating an unhealthy environment. In either case, you have a problem and you will fix it or I will replace you...You have two weeks. Tick-tock”.[61]

The contents of this email were leaked to the press and within days, the company’s stock plummeted. The email remains one of the most infamous examples of the consequences associated with inappropriate email etiquette.

Though emails of the above nature are relatively rare today, many misunderstandings still occur in digital exchanges. These misunderstandings stem from the highly interpretive nature of online communications. An NYU study on internet social behavior had email recipients attempt to gauge the tone of an email and to state their level of certainty that their interpretation of the email was correct. Interestingly, the study found that recipients correctly interpreted the tone of the email only 50 percent of the time, despite reporting 90 percent confidence on average in their interpretations.[62] The study highlighted that online interaction is ego-centric, meaning that users are likely to feel certain that their interpretation of online events is accurate without needing to clarify with the user on the other end of the exchange. This phenomenon may underpin many of the professional and personal conflicts which occur as a result of misunderstandings of communications online.

The other key challenge associated with organically formed online norms is the formation of undesirable or anti-social norms. A 2015 study found that children and youth are likely to engage in online behaviors if their peers approve of those behaviors, such as cyberbullying or the sharing of se-

[61] Burton, T. and Silverman, R. (2001) ‘Cerner ceo isn’t happy with workers, which is sad news for company’s stock’, Wall Street Journal, 30 March. Available at: https://www.wsj.com/articles/SB985910853715635424 (Accessed: 25 September 2020).

[62] Kruger, J. et al. (2005) ‘Egocentrism over e-mail: can we communicate as well as we think?’, Journal of personality and social psychology. doi: 10.1037/0022-3514.89.6.925.

xually explicit photos, regardless of parental guidelines or intervention by authorities.[63] The findings indicated that user guidelines and authoritative intervention has only limited influence on adolescent user-behavior. The prevalence of anti-social or inappropriate behaviour online is not limited to children and youth; a Pew research study found that 41 percent of American adults had directly experienced harassment online and 66 percent of respondents reported witnessing harassment online.[64] These findings demonstrate that despite authoritative attempts to foster safe and positive community interaction through user-guidelines and content moderation by social media companies, anti-social and inappropriate behaviours persist online. The findings emphasize a need for shared standards of online politeness and conduct guided by pro-social and conscientious behavioral principles.

In light of the challenges described above, digital etiquette is a concept being introduced in schools, universities, and professional offices globally in order to better facilitate a safe and universally beneficial internet.[65] At present, digital etiquette remains conceptually underdeveloped in the literature. In practice, digital etiquette refers to a set of basic communication instructions meant to promote positive user interactions in a variety of online communications. Generally, practice guides issued by schools and professional offices describe the following digital etiquette principles:[66]

1) Craft clear messages with appropriate punctuation
2) Use formal address and language with superiors, colleagues, and strangers
3) Know the appropriate times and places to use technology
4) Respect the data and privacy of other users
5) Do not participate in cyberbullying, harassment, stalking or inflammatory posting
6) Consider the effects that your actions or messages may have on other users
7) Represent yourself accurately online

Digital etiquette is seen as increasingly necessary as more social interactions move online for all age groups.[67] As a result of the COVID-19 pandemic, millions of professionals adapted to Zoom, Microsoft Teams, and other video chatting technologies while working remotely. This resulted in a slew of articles on the etiquette of video-chatting technologies which included recommendations such as introducing everyone in the group, sharing video as a default, putting audio on mute when it

[63] Gámez-Guadix, M., Borrajo, E. and Almendros, C. (2016) 'Risky online behaviors among adolescents: Longitudinal relations among problematic Internet use, cyberbullying perpetration, and meeting strangers online', Journal of Behavioral Addictions, 5(1), pp. 100–107. doi: 10.1556/2006.5.2016.013.

[64] Duggan, M. (2017) Online Harassment. Pew Internet Project 2017.

[65] Ribble, M. (2015) Digital citizenship in schools: nine elements all students should know. Available at: http://site.ebrary.com/id/11155264 (Accessed: 17 September 2020).

[66] Ribble, M. (2015) Digital citizenship in schools: nine elements all students should know. Available at: http://site.ebrary.com/id/11155264 (Accessed: 17 September 2020).

[67] Preece, J. (2004) Etiquette Online: From nice to necessary. Communications of the ACM (accepted, in press).

is not your turn to speak, and using a hand emoji when you wished to share a comment or respond to a question. These and other standards of polite behavior online can foster more productive business communications, especially given the predictions that work in the future will be increasingly remote and reliant on technology communications.[68]

The dissemination of these shared rules of etiquette can also foster more positive personal interactions between users. For children and youth in particular, digital etiquette is important for healthy psycho-social development.[69] Because many children and youth today have grown up with internet access and exposure to social media, formative experiences may occur online or may overlap with internet use and communication.[70] Given the limited impact of authoritative intervention in child internet use and the propensity of children to engage in risky and potentially damaging behaviour if unsupervised, digital etiquette training from a young age can have a profound impact on their health and safety.

Case Study on Digital Etiquette

As a result of the COVID-19 pandemic schools worldwide have been forced to turn to online learning and remote education in order to stop the spread of the disease and protect the health of children and educators alike. However, remote learning has led to students spending an unprecedented amount of time online, including communicating with teachers and classmates through groups chats and emails. In light of the challenges created by this shift to remote learning, the UK Scouts Programme partnered with the internet tech company, Nominet, to introduce a 'Digital Citizen' badge for their students.

Participating scouts received interactive training on how to evaluate the validity of news sources online, how to protect their data when subscribing to new services or downloading apps, how to improve their curriculum vitae, and how to behave online in an ethical way.[71] Since its introduction, the digital citizen badge information has been downloaded by more than 26,000 scouts.[72] Programmes like these have the potential to impart students with skills to help them critically engage with the information available to them online and to thoughtfully engage with their peers on digital plat-

[68] Trapp, R. (2020) Remote working has its problems, but it points to the future, Forbes. Available at: https://www.-forbes.com/sites/rogertrapp/2020/07/21/remote-working-has-its-problems-but-it-points-to-the-future/ (Accessed: 25 September 2020).

[69] González-Cabrera, J. et al. (2018) 'Relationship between cyberbullying and health-related quality of life in a sample of children and adolescents', Quality of Life Research, 27(10), pp. 2609–2618. doi: 10.1007/s11136-018-1901-9.

[70] McGillivray, D. (2016) 'Young people, digital media making and critical digital citizenship', Leisure Studies, 35(6), pp. 724–738. doi: 10.1080/02614367.2015.1062041.

[71] Sharma, R. (2020) Scouts to learn how to spot fake news for the new 'Digital Citizen' badge (2020) inews.co.uk. Available at: https://inews.co.uk/news/scouts-fake-news-badge-digitial-citizen-misinformation-643106 (Accessed: 24 September 2020).

[72] Sharma, R. (2020) Scouts to learn how to spot fake news for the new 'Digital Citizen' badge (2020) inews.co.uk. Available at: https://inews.co.uk/news/scouts-fake-news-badge-digitial-citizen-misinformation-643106 (Accessed: 24 September 2020).

forms. Such skills will support the success of their learning during remote learning periods and are likely to stay with them as they transition into adulthood and the professional world.

In an increasingly online world, interactions between users can have profound personal and professional impacts. Inappropriate interactions online can have a range of serious outcomes, including soured professional relationships, job loss, and the devaluing of company reputation. For students, inappropriate internet use can result in school expulsions and cyberbullying, among other things. Digital etiquette can foster safer online communities and result in more positive user experiences for all. If taught in schools, digital etiquette may be more effective and long lasting as young users grow up with a common language of politeness and respect for each other.

2.6. Digital Law

Digital law refers to the legislation and legal principles associated with internet use in all its forms. As a legal concept, digital law can be elusive, as it covers the complete range of possible actions and actors associated with the internet and its corresponding objects. Unlike more classical legal fields, digital law draws on a variety of disciplines, including contract, privacy, and commerce law, among others.[73] It covers issues such as trademark and copyright infringement, ensuring the validity of E-commerce transactions, unauthorized data sharing, and lawful content moderation by social media companies. Basic knowledge of digital law and data privacy principles is useful to digital citizenship because knowledge of legal and illegal internet use can empower users to engage in the digital sphere with the knowledge that they have access to legal recourse if their rights are violated. It can also equip them with the information they need to respect the rights and property of others online.

Digital law corresponds to national and/or regional jurisdictions and can differ significantly by region. In the European Union, digital law is constituted through legal directives and regulations. The General Data Protection Regulation (GDPR) was introduced in the European Union in 2018 in response to rising public concern over data privacy and protection violations related to social media use and E-commerce which were not sufficiently covered in existing directives on internet law.[74] As a regulation, the GDPR immediately entered into force for all EU member states, though individual member states retain some autonomy in the implementation and enforcement of regulations. Principles in the GDPR include consent to the processing of data, the provision of basic information about how data is used, the right to erasure of personal data and objection to data processing, the right to data portability, and the right to not be subject to automatic data processing which may result in

[73] Brigham, J., Schreiner (2004) A.T.M. Introduction: The Semiotics of Digital Law. Int J Semiot Law 17, 259–266.

[74] Sobolewski, M., Mazur, J. and Paliński, M. (2017) ‘Gdpr: a step towards a user-centric internet?’, Intereconomics, 52(4), pp. 207–213. doi: 10.1007/s10272-017-0676-5.

profiling.[75]. Digital citizenship training can help deter illegal actions online by imparting individuals with knowledge about the permissibility of actions online and their corresponding consequences.

As a legal field of practice, digital law is constantly innovating as ethical and legal issues arise with the creation of new internet services. A particularly innovative area of digital law is in personal data collection and processing. According to the UK Information Commissioner's Office, personal data is any information which corresponds to an identified or identifiable individual.[76] Personal data points scattered across the internet form the digital analog of an individual, or their 'data double'.[77] Data doubles are made legible through data processing, or the connecting of data points related to a specific person by a company or political entity for the purposes of marketing or surveillance.[78] Data doubles are a new concept which raise a host of ethical concerns which have not yet been thoroughly addressed by academics or rights defenders.

Globally, there is a growing sense of concern about the way data are collected and used. In a 2019 research study conducted by Ipsos, 75 percent of respondents reported feeling that social media companies were the biggest source of blame for the misuse of personal data, second only to cyber criminals.[79] The rising concern worldwide over diminishing user-control and ability to protect their personal data reflects the general shift in the purpose of the internet away from user-centricity and towards E-commerce in the past decades.[80] Though the internet was originally conceptualized as a "decentralized network of networks" formed on the principle of user-centricity, the widespread proliferation and success of business models based on data mining in recent years has undermined the user-centric principle by isolating users from their personal data, monetizing their engagement, and in some cases manipulating the user's experience of the internet.[81] As public concern over this shift becomes more evident, digital law is following suit - in the EU, the Digital Services Act (DSA) is being introduced as regulatory measure to give users greater control of their personal data. The

[75] Sobolewski, M., Mazur, J. and Paliński, M. (2017) 'Gdpr: a step towards a user-centric internet?', Intereconomics, 52(4), pp. 207–213. doi: 10.1007/s10272-017-0676-5.

[76] What is personal data? (2020) Information Commissioner's Office of the United Kingdom. International Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/ (Accessed: 23 September 2020).

[77] Cooke, T. (2018) 'Data-doubles', in Arrigo, B (ed.), The sage encyclopedia of surveillance, security, and privacy, SAGE Publications, Inc., Thousand Oaks, CA, pp. 283-284, viewed 22 September 2020, doi: 10.4135/9781483359922.n123.

[78] Cooke, T. (2018) 'Data-doubles', in Arrigo, B (ed.), The sage encyclopedia of surveillance, security, and privacy, SAGE Publications, Inc., Thousand Oaks, CA, pp. 283-284, viewed 22 September 2020, doi: 10.4135/9781483359922.n123.

[79] Cigi-Ipsos global survey on internet security and trust (2019) Centre for International Governance Innovation. Available at: https://www.cigionline.org/internet-survey-2019 (Accessed: 23 September 2020).

[80] Sobolewski, M., Mazur, J. and Paliński, M. (2017) 'Gdpr: a step towards a user-centric internet?', Intereconomics, 52(4), pp. 207–213. doi: 10.1007/s10272-017-0676-5.

[81] Sobolewski, M., Mazur, J. and Paliński, M. (2017) 'Gdpr: a step towards a user-centric internet?', Intereconomics, 52(4), pp. 207–213. doi: 10.1007/s10272-017-0676-5.

DSA would provide regulatory guidelines for social media and other large internet platforms on how they may collect and use data. It also attempts to give users more control over how they interact with content online, greater ability to contest content moderation decisions conducted by social media companies, and allows them to use the internet anonymously.[82] Some scholars suggest that the legislation may represent a significant advancement in efforts to articulate and secure digital rights.[83]

The COVID-19 pandemic has also raised important legal and ethical questions about the rights of governments and political authorities to collect, store, and use data. During the outbreak of the virus, many governments used new technologies, including mobile apps, censored wristband trackers, and digital check-in systems to track the movements of individuals living in their territories in order to curb its spread.[84] While some countries have introduced data-sensitive measures such as making location tracing applications voluntary, other countries have used more invasive data collection methods. In China, drones, artificial intelligence, street camera footage, and location-tracing apps were used to track the movements of citizens and fine violators of the quarantine.[85] Rights groups have since called for more transparency and government accountability for the collection of personal data used to govern the COVID-19 pandemic.[86] As the COVID-19 pandemic winds down, the ways which data were used by authorities to govern the crisis are likely to be questioned by digital and privacy rights defenders, debates which may influence the evolution of digital rights and law in the future.

Case Studies on Digital Law

Digital law influences internet governance by creating and enforcing penalties for violators of digital rights. An apt example of a digital law case which had significant impact for internet governance is the allegations brought by the state of New York and the American Federal Trade Commission (FTC) against Google and its subsidiary, YouTube, for illegally processing the personal data of mi-

[82] Schmon, C. (2020) Eff responds to eu commission on the digital services act: put users back in control, Electronic Frontier Foundation. Available at: https://www.eff.org/deeplinks/2020/09/eff-responds-eu-commission-digital-services-act-put-users-back-control (Accessed: 24 September 2020).

[83] Schmon, C. (2020) Eff responds to eu commission on the digital services act: put users back in control, Electronic Frontier Foundation. Available at: https://www.eff.org/deeplinks/2020/09/eff-responds-eu-commission-digital-services-act-put-users-back-control (Accessed: 24 September 2020).

[84] Anwar, N. (2020) Governments have collected large amounts of data to fight the coronavirus. That's raising privacy concerns, CNBC. Available at: https://www.cnbc.com/2020/08/17/governments-collected-data-to-fight-coronavirus-raising-privacy-concerns.html (Accessed: 24 September 2020).

[85] Anwar, N. (2020) Governments have collected large amounts of data to fight the coronavirus. That's raising privacy concerns, CNBC. Available at: https://www.cnbc.com/2020/08/17/governments-collected-data-to-fight-coronavirus-raising-privacy-concerns.html (Accessed: 24 September 2020).

[86] Mobile location data and covid-19: q&a (2020) Human Rights Watch. Available at: https://www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa (Accessed: 25 September 2020).

nors for the purpose of sending the minor users targeted advertisements.[87] The allegations claimed that Google and YouTube had violated the Children's Online Privacy Protection Act (COPPA) which requires sites to obtain parental consent before collecting and processing the personal data of internet users on child-directed channels, as the viewers are assumed to be under the age of 13.[88] YouTube not only collected personal data but used it to ascribe identifiers to the viewers in order to send them targeted advertisements, a strategy which earned the company millions of dollars in revenue.[89] According to the suit, YouTube's own internal content sorting system labeled some media as being directed towards children, which was a clear violation of COPPA. In 2019, Google, the parent company of YouTube, settled with the FTC and the state of New York for a total of $170 million. The settlement also included an obligation that the company would have to create and implement a system in which child-directed YouTube channels would have to identify their content as child-directed. It also required the company to obtain "verifiable parental consent" on all child-directed content in the future.[90] The case represents the effectiveness of digital law in enforcing protective measures.

Another famous example of digital law is the case of A&M Records versus Napster Inc. - 239 F.3d 1004 (9th Cir. 2001).[91] In 2001 the famous record company A&M sued Napster Inc., a first of its kind peer-to-peer MP3 file sharing service, for allowing users to share audio files without obtaining copyright permissions from the artists. The central issue of the case was whether a file once paid for by one party could be legally shared with another party. The case was significant because, before Napster audio files were obtained through the purchase of physical objects including C.D.s, records, and tapes. The objects associated with audio made copyright straightforward; it was almost impossible to enjoy audio without paying the musician for their work. However, the advent of digital media revolutionized the way that users interacted with audio by making file access efficient and easily transferable online. The court found Napster's services to be unlawful because the copyright infringement undermined the artists' ability to gather revenue from their work. Napster subsequently dissolved within three months of the final judgement. The ruling in A&M Records v. Napster Inc. set a precedent for copyright law related to peer-to-peer file sharing which dictates how similar services operate today.

[87] Google and YouTube will pay record $170 million for alleged violations of children's privacy law (2019) Federal Trade Commission. Available at: https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations (Accessed: 25 September 2020).

[88] Google and YouTube will pay record $170 million for alleged violations of children's privacy law (2019) Federal Trade Commission. Available at: https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations (Accessed: 25 September 2020).

[89] Google and YouTube will pay record $170 million for alleged violations of children's privacy law (2019) Federal Trade Commission. Available at: https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations (Accessed: 25 September 2020).

[90] Google and YouTube will pay record $170 million for alleged violations of children's privacy law (2019) Federal Trade Commission. Available at: https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations (Accessed: 25 September 2020).

[91] A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001)

Over time, developments in digital law and regulation influence companies to incorporate respect for digital rights into the design of new technologies and digital services. A shift in digital services towards more user-centric principles based on digital rights will enable more positive outcomes for all internet users, and a basic understanding of digital law and data privacy principles can empower individual users to maintain control of their digital identity and to protect themselves both online and offline.

2.7- Digital Rights and Responsibilities

As the world we live in becomes increasingly integrated with the internet and digital technologies, it is important that internet users have a strong conceptual grasp of their rights and responsibilities online. Digital rights refer to the rights and freedoms necessary to enjoy the benefits of the internet and its associated objects. Digital responsibilities refer to positive and negative duties internet users have which can promote a safer and more beneficial internet for all. Taken together, digital rights and responsibilities are the building blocks of digital citizenship as they connect individuals into a greater community based on shared values and mutual respect.

At present, there is no universally accepted bill of digital rights despite strong international interest in its creation. In 2011, the United Nations declared internet access to be a universal human right, making it the premier digital right.[92] Beyond this measure, a number of attempts to articulate internet rights and freedoms through ‘declarations of principles’ and similar documents have been made by various actors, including the UN bodies, governments, international organizations, think tanks, and academics though none have gained widespread traction.[93] Most documents proposing internet rights address both traditional human rights and more innovative rights related specifically to internet use. Key digital rights generally cited in these documents and in digital citizenship training events are as follows:[94]

1. Right to access the internet and to use digital technologies;
2. Right to create and share content online;
3. Right to personal data privacy and secure communications;
4. Right to self-expression online through the sharing of information and opinions;
5. Right to engage in secure transactions online; and:
6. Right to report illegal activity online

[92] Kravets, D. (2011) ‘U. N. Report declares internet access a human right’, Wired, 3 June. Available at: https://www.wired.com/2011/06/internet-a-human-right/ (Accessed: 25 September 2020).

[93] Pettrachin, A. (2018) ‘Towards a universal declaration on internet rights and freedoms?’:, International Communication Gazette. doi: 10.1177/1748048518757139.

[94] ‘A digital rights agenda for 2021 and beyond’ (2020) *Access Now*, 18 August. Available at: https://www.accessnow.org/a-digital-rights-agenda-for-2021-and-beyond/ (Accessed: 24 September 2020).

Digital rights commonly referenced in the media are the right to privacy and the right to freedom of expression. Recently, trends in content moderation regulation by social media companies have raised concern about the right to free speech and expression online. The social media era has ushered in unprecedented amounts of illegal and harmful content online including hate speech, sexually explicit content regarding minors, videos depicting violence and abuse, cyberbullying, and disinformation.[95] In attempts to control and deter this activity, many countries are pushing legislation which will increase penalties for social media companies for failing to address the content swiftly. Germany and France recently introduced legislation which would impose heavy fines for companies who do not deter "obviously illegal" content almost immediately.[96] However, the regulations have received criticism because while the measures require social media companies to censor and remove content, they do not require them to provide users with a mechanism to challenge and appeal the decision.[97]

In tandem with digital rights come the responsibilities that individuals hold to promote a safe and equitable internet. Digital responsibilities are the behaviors necessary to ensure the protection of the digital rights of all internet users. Digital responsibilities generally included in digital citizenship training are as follows:

1. Refrain from cyberbullying and use appropriate language / speech online;
2. Obey intellectual property laws;
3. Respect others by asking for their permission to share their content and by citing sources;
4. Report illegal activity and dangerous behavior online;
5. Represent yourself accurately online; and:
6. Adhere to the guidelines and rules of conduct on each site on which you participate

The internet encourages people to engage in communities by providing opportunities for users to communicate, collaborate, and share information. However, just as the internet can be used to connect individuals for positive purposes, it can also be used to achieve morally undesirable goals. Some individuals use the internet to obtain illegal content or to facilitate illegal activity, or to spread hate speech and encourage violence.

[95] Vincent, J. (2020) Former YouTube content moderator sues the company after developing symptoms of PTSD, The Verge. Available at: https://www.theverge.com/2020/9/22/21450477/youtube-content-moderator-sues-lawsuit-ptsd-graphic-content-exposure (Accessed: 25 September 2020).

[96] Martins Dos Santos, B. and Morrar, D. (2020) 'The push for content moderation legislation around the world', *Brookings*, 21 September. Available at:https://www.brookings.edu/blog/techtank/2020/09/21/the-push-for-content-moderation-legislation-around-the-world/ (Accessed: 25 September 2020).

[97] Martins Dos Santos, B. and Morrar, D. (2020) 'The push for content moderation legislation around the world', *Brookings*, 21 September. Available at:https://www.brookings.edu/blog/techtank/2020/09/21/the-push-for-content-moderation-legislation-around-the-world/ (Accessed: 25 September 2020).

Individual internet users have both negative and positive responsibilities to promote a safe, shared internet.[98] Negative responsibilities, or responsibilities which do not require action from the user, include the responsibility not to engage in hate speech, bullying, or illegal activity. Positive responsibilities, or responsibilities which require action on behalf of the user, and include flagging illegal content and reporting violence or abuse to appropriate authorities. They also include the responsibility to approach users who have violated the rights of others, for example by alerting a friend that the illegal downloading of content online is not an appropriate use of the internet and is harmful to the artist or creator of the content. These interventions may offset the negative effects of dubious internet use by influencing more conscious engagement online.

Case studies of digital rights and responsibilities

Digital responsibilities extend to all actors who benefit from internet engagement, including individuals, organizations, and companies. Companies are legally obligated to respect the digital rights of their users, but they also have an ethical responsibility to promote the safety and wellbeing of their users by dealing with illegal or abusive activity online, such as cyberbullying. In 2017, the popular social media platform, Instagram, introduced new features to help mitigate the effects of cyberbullying. A poll conducted in the UK asked 1,479 youth aged 14 - 24 to rate social media apps and platforms based on prevalent problems such as cyberbullying, anxiety, depression, and self-esteem. The results of the poll ranked Instagram as having the worst impact on the mental health of its users.[99] In response, Instagram implemented new features designed to give users more control over their interaction on the platform by enabling settings which could block certain users from commenting on posts. It also developed an artificial intelligence algorithm designed to detect and remove comments that feature words commonly linked to bullying, and it introduced a mechanism for users to report suspected cyber-bullying of themselves or others.[100] This intervention is an ambitious effort by Instagram to curb abuse online and demonstrates that the company takes seriously its responsibilities to promote a safe digital experience for its users.

In the modern era digital technologies have become common symbols of work, school, and personal life. Given the prevalence of internet access and use, the need for education on the rights and responsibilities associated with digital technologies has become salient. Digital rights belong to all internet users, and empower individuals to take full advantage of the benefits associated with the internet. Knowledge of and respect for digital rights and responsibilities may help prevent abuses online and may enable more users to harness the potentials of the internet to their benefit.

[98] Cohen-Almagor, R. (2015). Readers' Responsibility. In Confronting the Internet's Dark Side: Moral and Social Responsibility on the Free Highway (pp. 115-146). Cambridge: Cambridge University Press. doi:10.1017/CBO9781316226391.006

[99] *BBC News* (2017) 'Instagram "worst for young mental health"', 19 May. Available at: https://www.bbc.com/news/health-39955295 (Accessed: 25 September 2020).

[100] Pelletiere, N. (2017) *Instagram unveils tools to help fight cyberbullying*, *ABC News*. Available at: https://abcnews.go.com/Lifestyle/instagram-unveils-tools-fight-cyberbullying/story?id=50127367 (Accessed: 25 September 2020).

2.8. Digital Health and Wellbeing

Digital health and wellbeing relate to using the internet and mobile devices in a way that does not deteriorate one′s mental and physical health.[101] Excessive internet gambling, gaming, pornography, mobile phone use or information surfing may meet the criteria for a diagnosis of internet addiction and is associated with depression, anxiety, ADHD, and other mental health issues. The frequency of high risk for addiction is higher among college students and adolescents. Excessive internet use may decrease ability to read deeply, think with focus, concentrate on tasks, and control impulses. Moreover, excessive internet use takes individuals away from activities that promote mental health and may increase the risk of depression, anxiety, and suicidal thoughts.[102] Digital citizens must have awareness of health and wellbeing issues related to internet use in order to develop habits and boundaries which will help mitigate the more negative side effects and consequences of the digital age.

In addition to excessive internet use, digital health and wellbeing include knowing how to deal with cyberbullying. Cyberbullying is a form of bullying that takes place on social media, messaging services, gaming platforms, and mobile phones.[103] Its characteristics include abusive, targeted, deliberate, and repeated behavior intended to damage and harm another person. Examples of cyberbullying include spreading lies or posting embarrassing photos of someone on social media; sending hurtful messages or threats via messaging platforms; impersonating someone and sending messages to others on their behalf.[104] Individuals who experience cyberbullying are encouraged to deal with the event by taking the following actions:

* Do not respond to unwanted or disturbing messages;

* Delete and/or block the bully;

* Keep evidence of the harassment in case it continues and needs to be taken to authorities;

* If the harassment is a public post or photo, report it to the social media platform;

* Tell a trusted friend or family member about the experience; and:

* Take care of your mental and physical health, seek professional help if necessary;

[101] Devlin, A. M. et al. (2016) Delivering digital health and well-being at scale: lessons learned during the implementation of the Dallas program in the United Kingdom. Journal of the American Medical Informatics Association: JAMIA, 23(1): 48-59.

[102] Devlin, A. M. et al. (2016) Delivering digital health and well-being at scale: lessons learned during the implementation of the Dallas program in the United Kingdom. Journal of the American Medical Informatics Association: JAMIA, 23(1): 48-59.

[103] Aricak, T., Siyahhan, S., Uzunhasanoglu, A., Saribeyoglu, S., Ciplak, S., Yilmaz, N., and Memmedov, C. (2018) 'Cyberbullying among Turkish Adolescents.' Cyberpsychology & Behavior 11 (3), 253-261. DOI: 10.1089/cpb.2007.0016

[104] Baroncelli, A. et al. (2020) Triarchic Model Traits as Predictors of Bullying and Cyberbullying in Adolescence. Journal of interpersonal violence: 1-27.

Psychosocial outcomes related to cyberbullying are potentially more harmful and last longer than outcomes related to bullying which occurs in person. An explanation for this difference is that cyberbullying leaves a digital trace which can be revisited by the victim many times, allowing them to relive the event and making it difficult to overcome feelings of shame and humiliation. Instances of cyberbullying also have the potential to be virally spread among the victim's peer group or elsewhere online, which increases feelings of embarrassment for the victim. The persistence and reach of cyberbullying and online harassment is associated with long lasting mental, emotional, and physical effects.[105][106] The individual being bullied can feel upset, embarrassed, angry, ashamed, and tired due to loss of sleep. In extreme cases, cyberbullying can lead to suicide.[107] Individuals affected by cyberbullying and harassment can benefit from psychological support services by allowing them to regain confidence and restore health.

Cyberbullying may be more prevalent because the mediating role of technology disinhibits the bully, and technology features may embolden them to increase their impact while concealing their identity. Unlike traditional bullying, cyberbullying does not require that the bully be close to the victim.[108] Rather, the power of the bully comes from being technologically competent and/or their ability to hide their identity on the internet. In the same vein, the mediation of technology may disincentivize witnesses to report instances of bullying, because screens can cause viewers to feel removed from the incident. However, there is evidence that bystanders of cyberbullying do often feel distress and feel some pressure to respond to incidents, yet relatively few actively defend cyber victims.[109] This may be due to a lack of understanding of ways to appropriately respond to these incidents.

Active digital citizens should be well informed of the psycho-social dangers associated with internet use and communication. This includes understanding the signs of internet addiction, cyberbullying, and harassment and how to deal with them. Knowledge of these phenomena will allow digital citizens to engage with the internet in a safe, moderate way and to help respect peer users.

Case Studies on Digital Health and Well Being

Given the growing prevalence of internet use in Turkey, understandings of digital health and safety principles are important for Turkish internet users to internalize. As Turkey is one of the most active

[105] Aricak et al. (2018) Cyberbullying among Turkish Adolescents. Cyberpsychology & Behavior, 11(3): 253-259.

[106] Kubiszewski, V. et al. (2015) Does cyberbullying overlap with school bullying when taking modality of involvement into account? Computers in Human Behavior, 43: 49–57.

[107] Baroncelli, A. et al. (2020) Triarchic Model Traits as Predictors of Bullying and Cyberbullying in Adolescence. Journal of interpersonal violence: 1-27.

[108] Aricak et al. (2018) Cyberbullying among Turkish Adolescents. Cyberpsychology & Behavior, 11(3): 253-259.

[109] Sarmiento, A., Herrera-López, M., and Zuch, I. (2019) Is cyberbullying a group process? Online and offline bystanders of cyberbullying act as defenders, reinforcers and outsiders. Computers in Human Behavior, 99: 328–334.

countries in social media use, issues of cyberbullying and internet addiction are likely to increase in proportion to overall internet use unless addressed through education and policy.

A 2006 study on cyberbullying surveyed 269 students in grades 6-10 (ages 12-19) in Istanbul, Turkey.[110] The questionnaire measured the students' psychological and behavioral constructs such as engagement and exposure to cyberbullying. The study revealed that 35.7 percent of the students displayed cyberbullying behaviors. Of the students who displayed cyberbullying behaviors, 19 percent were boys and 16.7 percent were girls.[111] When asked about their engagement in cyberbullying, 59.5 percent of the students reported saying things online that they would not have said in person.[112] More than a quarter (26.8 percent) of the students reported telling lies online, 13 percent reported sending infected e-mails, and 6.7 percent reported displaying pictures of other people without their consent. In the same study, 5.9 percent of respondents gave answers that indicated they had been cyber-victims. More than one-third (36.1 percent) of the students reported encountering or being exposed to unwanted and disturbing behaviors on the Internet. Almost a quarter (23.7 percent) of the students reported experiencing harassment through phone messages and calls.

2.9 - Digital Security

Digital security refers to the protection of one's digital identity. The concept of digital identity includes one's digital personality, which is constituted through the personal data associated with an individual's likes, behaviors, and interests shared across various social media websites.[113] Digital identity is also constituted by the personal data associated with one's engagement with and use of internet services, such as purchased subscriptions, online medical and health accounts, or online banking.[114] When personal accounts or data are compromised in hacking events or other cybersecurity breaches, the results can be devastating for one's personal, professional, or financial well-being. Cybercrime can range from the hijacking of social media accounts for the purposes of damaging an individual's reputation to collecting personal data for the purpose of influencing politics through disinformation campaigns. As cybercrime becomes increasingly complex and malicious, govern-

[110] Aricak, T., Siyahhan, S., Uzunhasanoglu, A., Saribeyoglu, S., Ciplak, S., Yilmaz, N., and Memmedov, C. (2008) 'Cyberbullying among Turkish Adolescents.' Cyberpsychology & Behavior 11 (3), 253-261. DOI: 10.1089/cpb.2007.0016

[111] Aricak, T., Siyahhan, S., Uzunhasanoglu, A., Saribeyoglu, S., Ciplak, S., Yilmaz, N., and Memmedov, C. (2008) 'Cyberbullying among Turkish Adolescents.' Cyberpsychology & Behavior 11 (3), 253-261. DOI: 10.1089/cpb.2007.0016

[112] Aricak, T., Siyahhan, S., Uzunhasanoglu, A., Saribeyoglu, S., Ciplak, S., Yilmaz, N., and Memmedov, C. (2008) 'Cyberbullying among Turkish Adolescents.' Cyberpsychology & Behavior 11 (3), 253-261. DOI: 10.1089/cpb.2007.0016

[113] *What's your digital identity?* (no date). Norton Life Lock. Available at: /content/lifelock-msm/us/en-us/learn/identity-theft-resources/whats-your-digital-identity (Accessed: 1 October 2020).

[114] *What's your digital identity?* (no date). Norton Life Lock. Available at: /content/lifelock-msm/us/en-us/learn/identity-theft-resources/whats-your-digital-identity (Accessed: 1 October 2020).

ments are passing legislation to help protect personal data and to increase penalties for cybercriminals. Digital security is an important skill because its implementation can have lasting and profound effects on an individual's ability to take full advantage of the internet without fear of being compromised.

Social media data is sensitive and in need of protection. Data linked to social media accounts include biographical information, personal photos and videos, blog posts and other personal statements, likes and interests, and associations. Examples of accounts associated with one's digital identity on social media include Facebook, Instagram, TikTok, Tumblr, Twitter, LinkedIn, QQ, Snapchat, WeChat, Reddit, and Pinterest, among many others. When the digital security of social media accounts is compromised, users' personal and professional reputations can suffer as a result of the breach. Individual impacts may include the loss of personal reputation if private photos are published on a personal account or used to blackmail an individual. Hacking aimed at high profile individuals can have both individual impacts for the public figure as well as financial and/or political impacts on communities who follow that individual. For example, a 2019 hacking event resulted in the compromising of 130 Twitter accounts of high-profile individuals, including Bill Gates, Kim Kardashian West, Kanye West, Jeff Bezos, and Elon Musk.[115] The accounts were hijacked for the purpose of sending tweets which appeared to be from the celebrities and authority figures asking readers to send money to a bitcoin account under the premise that the celebrities and authority figures would double the amount sent to the account in a spirit of charity. It is believed that the hackers may have made up to 10 million dollars from the scam.[116] While this hacking event was driven by financial gain, other breaches may have malicious political or personal intentions. For example, if the social media account of a politician is hacked and used to publish incorrect or divisive information, such as hate speech against a minority group, the results can be damaging to the entire community. These examples highlight the importance of digital security for both personal and community safety and stability.

Personal data used to access internet services is also a component of digital identity. For example, login names, challenge questions, and passwords related to professional software, subscriptions, mobile banking, or other services are sensitive information which, if compromised, can give hackers control of financial accounts such as loan information or bank accounts, allowing them to withdraw money, take out lines of credit, or commit other illegal acts of identity theft. The COVID-19 pandemic saw a rise in identity theft facilitated through fake government stimulus check scams. Internet service data can also be used for political purposes, such as to undermine political campaigns. A notorious example from 2016 was when hackers associated with WikiLeaks released private emails from the presidential campaign staff of United States politician, Hilary Clinton. The hackers

[115] Winder, D. (2019) 'Get yourself cybersecure for 2020', *The Observer*, 31 December. Available at: https://www.theguardian.com/technology/2019/dec/31/get-cybersecure-for-2020-cybersecurity-passwords-smartphone (Accessed: 1 October 2020).

[116] Hern, A. (2020) *130 high-profile Twitter accounts targeted in hacking attack. the Guardian*. Available at: http://www.theguardian.com/technology/2020/jul/17/130-high-profile-twitter-accounts-targeted-in-hacking-attack (Accessed: 1 October 2020).

leaked information which revealed sensitive information about Mrs. Clinton's campaign and consequently caused internal division in the democratic party leading up to the election.[117] Hacking incidents and data breaches used to manipulate or control politics are urgent issues in cybersecurity, as they are believed to be potentially highly influential in the outcomes of political processes.

Scammers and hackers commonly masquerade as authority figures or professional colleagues in order to solicit highly sensitive information related to an individual's identity. Scammers also use emails and links which, if opened, infect a device with malware that enables the hacker to lock the device until the user procures a payment. While there are many kinds of scams, the most common ones can be categorized into seven groups:[118]

- **Reconnaissance -** Technique in which the hacker collects open-source information on an individual and uses it to compromise their account;
- **SQL injection** - Technique which manipulates database queries on websites or platforms to retrieve sensitive information on users of that service;
- **Phishing** – Technique which uses spam emails containing links to fraudulent websites meant to imitate a trusted website, such as a bank. The message will ask the reader to enter sensitive information, such as bank details, onto the website to recover an account or verify information;
- **Spear phishing** - Phishing attack directed at a particular person or organization. Messages strategically uses information which will convince the recipient that they know the messenger to gain trust and entice the recipient to disclose sensitive information;
- **Malware attack** - Malicious software installed on a computer, usually without the computer owner's knowledge, through phishing scams. Once installed, malware can be used to control the computer, capture keystrokes, or look for documents on the computer; and:
- **Weak authentication** - Techniques which exploit poor security systems such as weak passwords, insecure password reset methods, or allowing an indefinite number of invalid login attempts

The tactics used by scammers and hackers to steal personal information can be difficult to spot, however, basic knowledge of the indicators of suspicious online activity can help individuals fortify their security. For example, the National Cybersecurity Alliance advises individuals to protect themselves from phishing scams by looking out for spelling errors in the messages, checking web addresses and URLs, not opening suspicious attachments, not responding to messages designed to create panic, and to not respond to a message which asks for confirmation of personal

[117] BBC News (2016) '18 revelations from Wikileaks emails', 27 October. Available at: https://www.bbc.com/news/world-us-canada-37639370 (Accessed: 1 October 2020).

[118] Çalışkan, B. (2019) Digital security awareness and practices of journalists in Turkey: A descriptive study. Conflict & communication online, 18(1): 1-16.

information.[119] These basic but critical cyber security skills can help individuals to protect their information and overall financial and personal well-being.

Though digital security can be difficult to achieve given the evolving nature of technology and the complexity of cyberattacks, there are best practices in digital security which can minimize the risks of data privacy breaches. Commonly referenced best practices for individuals are as follows:[120]

* Keep software and firewalls as up to date as possible;

* Know the common signs of phishing scams;

* Create unique and random passwords, do not reuse passwords;

* Enable the self-destruct feature on smart technologies where possible;

* Choose secure two-factor authentication features, avoid SMS based authentication;

* Protect yourself by using secure wifi channels at home and outside of the home;

* Turn off devices when they are not being actively used; and:

* Think critically about challenge questions, do not use information that is traceable

Governments are responding to digital security and privacy issues by increasing the penalties associated with cybercrime - for example, in 2013 the European Union (EU) significantly increased the prison sentences of individuals found guilty of cybercrime, and in 2020, the EU imposed its first-ever sanctions on entities from China, Russia, and North Korea for their alleged involvement in cyberattacks and hacking of European organizations and citizens.[121][122] These actions represent government understanding of the gravity of cybersecurity breaches in the modern age and may indicate what we can expect from legislation related to cybersecurity from other governments in the future.

A 2014 study analyzed 400 Facebook profiles of experts and academics in Turkey.[123] More than 95 percent of the sample reported that they do not share personal information such as address, phones, political views, birthdays, or religious views on their accounts. Female respondents were less likely than male respondents to share basic personal and location information. Respondents demonstrated least concern for the privacy of their photos. Half of female users (50.2 percent) and 38.3 percent of male had a high level of privacy. Of the 400 Facebook profiles analyzed, 54 percent hide their

[119] National cybersecurity awareness month (no date) Federal Bureau of Investigation. Available at: https://www.fbi.-gov/investigate/cyber/national-cybersecurity-awareness-month (Accessed: 1 October 2020).

[120] Staff, W. (2017) ‘The wired guide to digital security’, Wired, 9 December. Available at: https://www.wired.com/2017/12/digital-security-guide/ (Accessed: 1 October 2020).

[121] Kerr, D. (no date) EU increases penalties for cybercriminals and hackers, CNET. Available at: https://www.cnet.-com/news/eu-increases-penalties-for-cybercriminals-and-hackers/ (Accessed: 1 October 2020).

[122] Ashoka (2020) “Misinformation Spreads Faster Than Coronavirus: How A Social Organization in Turkey is Fighting Fake News”. Forbes. Available at: <https://www.forbes.com/sites/ashoka/2020/04/17/misinformation-spreads-faster-than-coronavirus-how-a-social-organization-in-turkey-is-fighting-fake-news/#1183e69c417d>.

[123] Külcü, O. and Henkoglu, T (2014) Privacy in social networks: An analysis of Facebook. International Journal of Information Management, 34: 761-769.

friends list and 29.8 percent hide their photos. Overall, Facebook users who signed up between 2010 and 2013 show an average of privacy over 60 percent.[124] Journalists are another group to which privacy and security online are a concern. According to a 2014 study, journalists in Turkey frequently face security issues, including digital attacks.[125] The study found that many journalists in Turkey lack awareness of digital security risks, and only a small percentage have undertaken safety training to protect themselves and their devices in the digital world. The interest of Turkish social media users and journalists in data privacy and security, show that they would benefit from digital account security training.

Case Study on Digital Security

Cyber security can be particularly difficult for children to understand and implement due to their limited ability to identify threats and assess risk. In order to address this, Google developed a computer game, called Interland, to teach children about digital security and other topics related to digital citizenship. The game, launched as part of Google's "Be Internet Awesome" initiative for children, teaches elementary school age students about basic safety and security principles online through gamification techniques. Gamers can visit four islands "Tower of Treasure: Secure your Secrets"; "Mindful Mountain: Share with Care"; "Reality River: Don't Fall for Fake"; and: Kind Kingdom: Its Cool to be Kind." Each island comes with simple but engaging activities, designed to help gamers subliminally internalize important information about digital safety. For example, one game features a race in which the driver must pick up phone messages, photos, and videos on the racetrack and store them into a nearby tower for safety: if the driver crashes, they risk having the items they collected stolen by a hacker and consequently, they lose points. Each time the player completes a level, they receive a new badge, such as the "Data Defender Badge" which is announced along with a short but concise message about the sensitivity of personal data and the importance of securing it. Programs like these are growing in popularity given the prevalence of child internet and technology use. Pew Research which indicated that 92 percent [126] Google created the 'Be Awesome Online' initiative to foster critical digital security and citizenship for children approaching their teenage years in hopes that the children would be able to avoid issues with privacy and safety online that older teenagers have struggled to deal with in the past due to a lack of education on the subject. Google's goal is to reach five million school aged children with the game per year.

Digital security and privacy are growing in importance as work and social life increasingly merge with technology use. Though digital services can help individuals efficiently manage their finances, medical information, businesses, and personal lives online, the very inter-connectivity that facili-

[124] Külcü, O. and Henkoglu, T. (2014) Privacy in social networks: An analysis of Facebook. International Journal of Information Management, 34: 761-769.

[125] Çalışkan, B.)2019. Digital security awareness and practices of journalists in Turkey: A descriptive study. Conflict & communication online, 18(1): 1-16.

[126] Lenhart, M. (2015) 'Teens, social media & technology overview 2015', Pew Research Center: Internet, Science & Tech, 9 April. Available at: https://www.pewresearch.org/internet/2015/04/09/teens-social-media-technology-2015/ (Accessed: 1 October 2020).

tates the benefits of the internet also exposes users to security risks. While security risks associated with internet use cannot be completely eradicated, knowledge of digital security and privacy best practices can help individuals to minimize risk and maximize benefits.

Chapter 3 – Challenges to Digital Citizenship in Turkey

3.1. Context

What are the major challenges to digital citizenship in Turkey? How could we address them? Major political and social barriers to the implementation of digital citizenship in Turkey persist. At present, the government of Turkey is attempting to manage the complex problems stemming from the global technological revolution and foster digital citizenship. It is developing new techno-political concepts such as 'cyber-nation' (*siber vatan*) as well as making legislative efforts to tackle persistent issues on social media.[127] Specifically, the government recently amended Law No. 5651 (Regulation of Publications on the Internet and Combating Crimes Committed by Means of Such Publications) in order to create new obligations for large social network providers (SNPs). SNPs based outside of Turkey whose platforms see daily traffic from one million or more users in Turkey are obligated to follow the new rules set forth in the amendment. Two noteworthy changes in the law are: (a) they require SNPs to employ at least one local representative in Turkey to deal with requests and demands from their users as well as the judicial and administrative authorities; and (b) SNPs are obliged to respond to users' filed complaints of alleged violations of their personal rights on the platform, including violations of privacy, within 48 hours.[128] Failure to fulfil the new requirements will be met with heavy legal sanctions. An SNP could face fines up to 40 million euros if it does not employ any local representative in Turkey, who deals with requests from the users and authorities.

While the legal changes in the Law No. 5651 could help to create a more effective working relationship between the companies and the state, there are concerns that the measures will restrict freedom of expression online. The Republican People's Party (CHP) has appealed to the new regulation to the Constitutional Court of Turkey.[129] Even before the recent amendment, Law No. 5651 had been challenged by free speech advocates for tending towards censorship. Indeed, from 2008 to 2016 the law was used to block access to 109,805 websites in Turkey.[130] The European Court of

[127] Güven, B. (2020) 'AK Parti'li Ünal&#39;dan "Sosyal Medya Düzenlemesi" Açıklaması.' Available at: https://www.aa.com.tr/tr/politika/ak-partili-unaldan-sosyal-medya-duzenlemesi-aciklamasi/1902512

[128] iii Resmi Gazete (2020) 'BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURULU KARARI' *Resmi Gazete* 31262 (02/10/2020) Available at: https://www.resmigazete.gov.tr/eskiler/2020/10/20201002.pdf

[129] Hurriyet Daily News (2020) 'Turkish Parliament Passes Law to Regulate Social Media Content.' Available at: https://www.hurriyetdailynews.com/turkish-parliament-passes-law-to-regulate-social-media-content-156957

[130] Canata, F. (2016) '5651 Sayılı Kanun Kapsamında İnternet Düzenlemeleri ve Düşünce-İfade Özgürlüğü Üzerine Bir Değerlendirme.' *Türk Kütüphaneciliği* 30 (2): 185-205.

Human Rights (ECHR) recently overturned a Turkish interim court's judgment on a case related to Law No. 5651, as they found that the law's application showed a serious violation of the applicant's freedom of expression.[131] This, as well as the other concerns related to free speech and Law No. 5651 in Turkey, demonstrates the difficulties inherent to navigating the new digital era.

While freedom of speech is a fundamental right in need of protection, as described in chapter two, abuses of free speech online may have serious consequences for the health and safety of users, as well as greater political consequences for governments and societies. In Turkey, major challenges to the realization of digital citizenship include: conspiracy theories, fake news, hate speech and cyber-bullying.

3.2 Challenges

Conspiracy theories

Conspiracy theories are explanations of 'events in terms of the significant causal agency of a relatively small group of persons-the conspirators-acting in secret'.[132] They can have substantial impacts with potentially global reach: conspiracy theories which refute the existence of climate change may lower individual's desire or willingness to take or support actions which would reduce their carbon footprint;[133] conspiracy theories which place doubt on who can contract the AIDS disease may decrease some individual's likelihood to engage in safe sexual practices despite their equal vulnerability to the disease.[134] In the modern era, characterized by skepticism and disagreement about the effects of COVID-19, and growing challenges to the legitimacy of news and information, conspiracy theories are likely to grow and may have profound consequences.

Scholarship on the subject is divided between recommendations to avert conspiracy theories because of their potentially harmful impacts and to view them as natural consequences of the human will to learn.[135] The academic literature indicates that conspiracy theories are caused by a combination of social, political, and psychological factors. Political contexts and factors, such as partisans-

[131] ECHR. (2013) 'Case of Ahmet Yıldırım v. Turkey (Application no. 3111/10).' Available at: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-115705%22]}

[132] Keeley, B. (1999) 'Of Conspiracy Theories.' *The Journal of Philosophy* 96(3): 109-126.

[133] Jolley, D. and Douglas, K. (2014) 'The Social Consequences of Conspiracism: Exposure to Conspiracy Theories Decreases Intentions to Engage in Politics and to Reduce One's Carbon Footprint.' *British Journal of Psychology* 105 (1): 35–56.

[134] Bogart, L. M. and Thorburn, S. (2005) 'Are HIV/AIDS Conspiracy Beliefs a Barrier to HIV Prevention among African Americans?' *Journal of Acquired Immune Deficiency Syndromes* 38(2): 213–218.

[135] Nefes, T. S. (2013) 'Political Parties' Perceptions and Uses of Anti-Semitic Conspiracy Theories in Turkey.' *The Sociological Review* 61(2): 247-264.

hip,[136] may make some individuals more prone to believe in conspiracy theories.[137] For example, a study posits that the prevalence of conspiracy theories in the United States may be due to Americans' distrust of the state and authorities.[138] Additionally, the research identified psychological characteristics which indicate a predisposition towards conspiratorial thinking, such as delusional ideation,[139] boredom[140] and stress.[141] Though scholars disagree on the specific impacts of conspiracy theories themselves, they agree that conspiracy theories could have negative influences on believers, such as depolitization,[142] justification for intergroup hatred,[143] decreased pro-social behaviour,[144] and reduced trust in science and government.[145]

Conspiracy theories are a frequent topic of discussion in Turkish politics and society. A variety of actors, representing the complete spectrum of political beliefs, engage conspiracy theories to explain recent social and political developments.[146] An examination of the political communication in the Turkish parliament shows that the deep-state conspiracy theory has been used in different periods by various actors, ranging from the political Islamist Welfare Party (*Refah Partisi*) to left-wing

[136] Uscinski, J. E., & Parent, J. M. (2014) *American Conspiracy Theories*. New York, NY: Oxford University Press; Uscinski, J. E., Klofstad, C., & Atkinson, M. D. (2016) 'What drives conspiratorial beliefs? The role of informational cues and predispositions.' *Political Research Quarterly* 69(1): 57–71.

[137] Goldberg, R. A. (2001) *Enemies Within: The Culture of Conspiracy in Modern America*. New Haven and London: Yale University Press; Nefes, T. S. (2014) 'Rationale of conspiracy theorizing: who shot the president Chen Shui-bian?' *Rationality and Society* 26(3): 373-394; Nefes, T. S. (2015a) 'Scrutinizing impacts of conspiracy theories on readers' political views: a rational choice perspective on anti-Semitic rhetoric in Turkey', *British Journal of Sociology* 66(3): 557-575; Rohr, I. (2003) 'The use of antisemitism in the Spanish Civil War.' *Patterns of Prejudice* 37(2): 195-211.

[138] Olmsted, K. (2009) *Real Enemies: Conspiracy Theories and American Democracy, World War I to 9/11*. New York: Oxford University Press.

[139] Dagnall et al. (2015) 'Conspiracy Theory and Cognitive Style: A Worldview.' *Frontiers in Psychology* 6: 206.

[140] Brotherton, R. and Eser, S. (2015) 'Bored to Fears: Boredom Proneness, Paranoia, and Conspiracy Theories.' *Personality and Individual Differences* 80: 1–5.

[141] Swami, V. et al (2016) 'Putting the Stress on Conspiracy Theories: Examining Associations between Psychological Stress, Anxiety, and Belief in Conspiracy Theories.' *Personality and Individual Differences* 99: 72–76.

[142] Fenster, M. (1999) *Conspiracy Theories: Secrecy and Power in American Culture*. Minneapolis, MN: University of Minnesota Press.

[143] Cohn, N. (2005) *Warrant for Genocide: The Myth of the Jewish World Conspiracy and the Protocols of Elders of Zion*. London: Serif.

[144] Van der Linden, S. (2015) 'The Conspiracy-effect: Exposure to Conspiracy Theories (about Global Warming) Decreases Pro-Social Behavior and Science Acceptance.' *Personality and Individual Differences* 87: 171–173.

[145] Bogart, L. M. and Thorburn, S. (2005) 'Are HIV/AIDS Conspiracy Beliefs a Barrier to HIV Prevention among African Americans?' *Journal of Acquired Immune Deficiency Syndromes* 38(2): 213–218.

[146] Gürpınar, D. and Nefes, T. S. (2020) 'A Survey of the Scholarship on Conspiracy theories in Turkey', in M. Butter and P. Knight (eds.) *Routledge Handbook of Conspiracy Theories*, Abingdon: Routledge: 610-623.

Kurdish political actors from the Peoples' Democratic Party (*Halklarin Demokratik Partisi*).[147] Despite the prevalence of conspiracy theories in Turkey, there are only a handful of recent studies that address their socio-political significance[148] and only one on the online communication associated with these accounts.[149] Studies find both historical factors and contemporary political interests to be the root causes of conspiracy theories.[150] One such historical factor is the "Sevres Syndrome“[151] refers that persistent anxieties about the potential threats against Turkish national borders posed by the alleged collaboration of external enemies and the minorities in the country.[152] In addition, political motivations have been documented as central causes.[153] Conspiracy theories increased political polarization.[154] and have the potential to feed into ethno-religious hostilities in Turkey.[155] For example, conspiracy theories about the crypto-Judaic Dönme community influenced the rise of anti-Semitic sentiment.[156] Furthermore, the scholarship starts to analyze the conspiracy

[147] Nefes, T. S. (2018) 'The Conspiratorial Style in Turkish Politics: Discussing the Deep state in the Parliament', in J. Uscinski (ed.) *Conspiracy Theories and the People Who Believe Them*, New York: Oxford University Press: 385-395.

[148] De Medeiros, J. (2018) *Conspiracy Theory in Turkey: Politics and Protest in the Age of "Post-Truth"*, London: I.B. Tauris; Gürpınar, D. (2013) 'Historical Revisionism vs. Conspiracy Theories: Transformations of Turkish Historical Scholarship and Conspiracy Theories as a Constitutive Element in Transforming Turkish Nationalism.' *Journal of Balkan and Near Eastern Studies* 15(4): 412-433; Gürpınar, D. (2019) *Conspiracy Theories in Turkey: Conspiracy Nation*. London and New York: Routledge.

[149] Nefes, T. S. (2017) 'The Impacts of the Turkish Government's Conspiratorial Framing about the Gezi Park Protests.' *Social Movement Studies* 16(5): 610-622.

[150] Guida, M. (2008). 'The Sèvres syndrome and "Komplo" theories in the Islamist and Secular Press.' *Turkish Studies, 9*(1), 37-52; Nefes, T. S. (2015b) 'Understanding the Anti-Semitic Rhetoric in Turkey through the Sevres Syndrome', *Turkish Studies* 16(4): 572-587.

[151] De Medeiros, J. (2018) *Conspiracy Theory in Turkey: Politics and Protest in the Age of "Post-Truth"*, London: I.B. Tauris; Nefes, T. S. (2017) 'The impacts of the Turkish government's conspiratorial framing about the Gezi Park Protests', *Social Movement Studies* 16(5): 610-622.

[152] The name comes from the Treaty of Sevres, an agreement signed by the Ottoman Empire and allied countries in 1920 at the end of the First World War, which reassigned portions of the Ottoman territory to the allied powers and Ottoman minorities. Turkish opponents of the treaty, led by Mustafa Kemal Atatürk, initiated rebellion against the responsible authorities, which ultimately led to the Turkish Independence War in 1919. The resolution of the war in 1923 led to the formation of Turkey's contemporary borders. Though this war ended nearly a century ago, modern conspiracy theories echo some of the anxieties prevalent at that time, such as fear of dismemberment by foreign powers and minorities.

[153] De Medeiros, J. (2018) *Conspiracy Theory in Turkey: Politics and Protest in the Age of "Post-Truth"*, London: I.B. Tauris.

[154] Nefes, T. S. (2017) 'The Impacts of the Turkish Government's Conspiratorial Framing about the Gezi Park Protests.' *Social Movement Studies* 16(5): 610-622.

[155] De Medeiros, J. (2018) *Conspiracy Theory in Turkey: Politics and Protest in the Age of "Post-Truth"*, London: I.B. Tauris.

[156] Nefes, T. S. (2012) 'The History of the Social Constructions of Dönmes (converts)', *Journal of Historical Sociology* 25(3): 413-439; Nefes, T. S. (2015c) *Online Anti-Semitism in Turkey*, New York: Palgrave Macmillan.

theories about the COVID-19 in Turkey and presents that that higher levels of intuitional trust and religiosity are robust predictors of believing in these accounts.[157]

Fake News

While the term 'fake news' is not actually new, in recent years its significance has been revitalized in global political debates. The resurgence of this term is the result of the alleged influence of fake news and disinformation on the outcome of the 2016 U.S. presidential election.[158] In the wake of the election, fake news and how to address it, has become an important policy concern for both governments and media platforms alike. Policy makers must first understand what it is, who it affects, and the outcomes associated with its spread. At present, the influence of fake news on individual and public opinions is an understudied area with scarce data. Though a recent paper found that their audience is a relatively small group of frequent internet users, the characteristics and composition of these groups remains unclear.[159] Lack of sufficient data on their audience and scope more generally makes it difficult for policy makers to develop strategies to stymie the spread of potentially harmful disinformation, and as such, is an important area for future research.

A growing body of research examines the spread of fake news on social media.[160] Scholars employed computational social science methods to trace the rate and reach of these spreads.[161] Findings indicate that partisanship and poorly developed reasoning abilities are the characteristics most heavily associated with a likelihood to believe fake news.[162] The latter characteristic has been determined to be more predictive of susceptibility to fake news, as some studies have shown that, giv-

[157] Alper, S., Bayrak, F., & Yilmaz, O. (2020) 'Psychological Correlates of COVID-19 Conspiracy Beliefs and Preventive Measures: Evidence from Turkey.' Available at: https://doi.org/10.1007/s12144-020-00903-0

[158] Grinberg N., Joseph, K., Friedland L., Swire-Thompson, B., Lazer D. (2019) 'Fake News on Twitter during the 2016 U.S. Presidential Election.' *Science* 363(6425): 374-378. DOI: 10.1126/science.aau2706; Nielsen, R. K. and Graves, L. (2017) '"News You Don't Believe": Audience Perspectives on Fake News.' Available at: https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2017-10/Nielsen%26Graves_factsheet_1710v3_FINAL_download.pdf

[159] Nelson J.L. and Taneja, H. (2018) 'The Small, Disloyal fake news audience: The role of audience availability in fake news consumption.' *New Media & Society* 20(10): 3720-3737. doi:10.1177/1461444818758715

[160] Lazer, D., Baum, M., Benkler, J., Berinsky, A., Greenhill, K., Metzger, M.,…Zittrain, J. (2018) 'The Science of Fake News." *Science* 359(6380), 1094–1096.

[161] Bovet, A. & Makse, H. A. (2019) 'Influence of Fake News in Twitter during the 2016 US Presidential Election.' *Nature Communications* 10 (7). https://doi.org/10.1038/s41467-018-07761-2

[162] Badawy, A., Lerman, K., Ferrara, E. (2018) 'Who Falls for Online Political Manipulation? The case of the Russian Interference Campaign in the 2016 US Presidential Election.' Available at: https://arxiv.org/pdf/1808.03281.pdf AND Pennycook, G. and Rand, D. (2019) 'Lazy, not Biased: Susceptibility to Partisan Fake News is Better Explained by Lack of Reasoning than by Motivated Reasoning.' *Cognition* 199: 39-60.

en the opportunity to critically reexamine the information, individuals representing all sides of the political spectrum were able to accept that news they had previously believed in was fake.[163]

Partisanship is a persistent societal issue in Turkey, now compounded by the spread of conspiracy theories and fake news online. According to the 2018 Reuters Institute Digital News Report, among 37 countries, Turkey had the highest proportion of respondents who had encountered 'stories that are completely made up for political or commercial reasons.'[164] In parallel, Ünver argued that fake news is very prevalent in Turkey compared to Western democracies.[165] Teyit, the Turkish fact-checking organization, noted that most of the online fake news in the country pertains to politics.[166] For example, many fake Twitter accounts have been linked to spread of political propaganda.[167] Creators of fake political accounts, or individuals who spread propaganda meant to discredit a political party online or who make comments to entice political dispute, are referred to as political 'trolls'. Studies indicate a strong trolling presence in Turkey.[168]

We conducted a nationwide survey[169] on digital citizenship with 3350 people and inquired about people's awareness about trolling and disinformation in the following manner: 'Could you please indicate whether you have a good idea of what each of these terms mean? Yes/No: Trolling, Disinformation'. As Figure 1 below presents, 47% of the respondents confirmed to have a good idea about trolling. The proportion of awareness is higher among the ones who have higher socio-economic status and higher levels of education. Moreover, younger respondents are more likely to have awareness about the term. A similar pattern is valid for awareness about disinformation. As shown in Figure 2 below, people from higher socio-economic status, a younger age group and with a hig-

[163] Bago, B., Rand, D. G., & Pennycook, G. (2020) 'Fake News, Fast and Slow: Deliberation Reduces Belief in False (but not True) News Headlines.' *Journal of Experimental Psychology: General* 149(8), 1608–1613. https://doi.org/10.1037/xge0000729

[164] Yanatma, S. (2018) 'Reuters Institute Digital News Report 2018 Turkey Supplementary Report.' Available at: https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2018-11/Digital%20News%20Report%20-%20Turkey%20Supplement%202018%20FINAL.pdf

[165] Ünver, A. (2019) 'Russian Digital Media and Information Ecosystem in Turkey.' Available at: https://edam.org.tr/en/russian-digital-media-and-information-ecosystem-in-turkey/

[166] Ünal, R. and Çiçeklioğlu, A. Ş. (2019) 'The Function and Importance of Fact-Checking Organizations in the Era of Fake News: Teyit.Org, an Example from Turkey.' *Media Studies* 10 (19): 140-160.

[167]; Bulut, E. and Yoruk, E. (2017) "Digital Populism: Trolls and Political Polarization of Twitter in Turkey", *International Journal of Communication* 11: 4093–4117

[168] Saka, E. (2018) 'Social Media in Turkey as a Space for Political Battles: AKTrolls and other Politically motivated trolling,' *Middle East Critique*, 27 (2): 161-177.

[169] The research was conducted by INGEV (Huma Devlopment Foundation) in September and October 2020. It adheres to the standard quantification methodology established by the Turkish Researchers' Association (TUAD) for measurement of Socio-Economic Status. In cooperation with the Advertisers' Association, TUAD carried out a socioeconomic status (SES) study in 2012 with the objective of setting up a reference methodology based on consumer behaviour in Turkey, taking both income and education levels into consideration. We use this particular SES measurement scale. Each participant is categorized into a SES group through an assessment matrix based on their education level and occupation. For more information please see: https://tuad.org.tr/en/projects/socio-economic-statu-2012

her level of education are more likely to know the meaning of disinformation. Moreover, 26% percent of the respondents acknowledged an awareness of disinformation. Overall, these data indicate lower levels of general public awareness about fake news in Turkey.

Figure 1

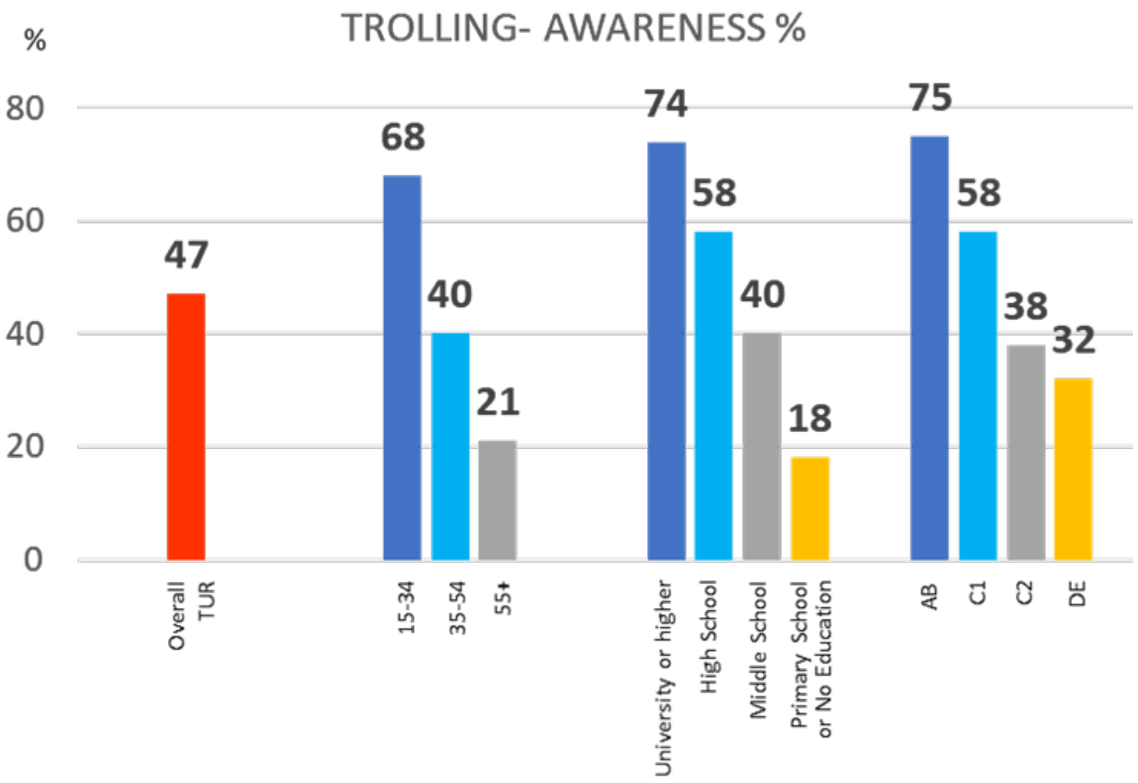
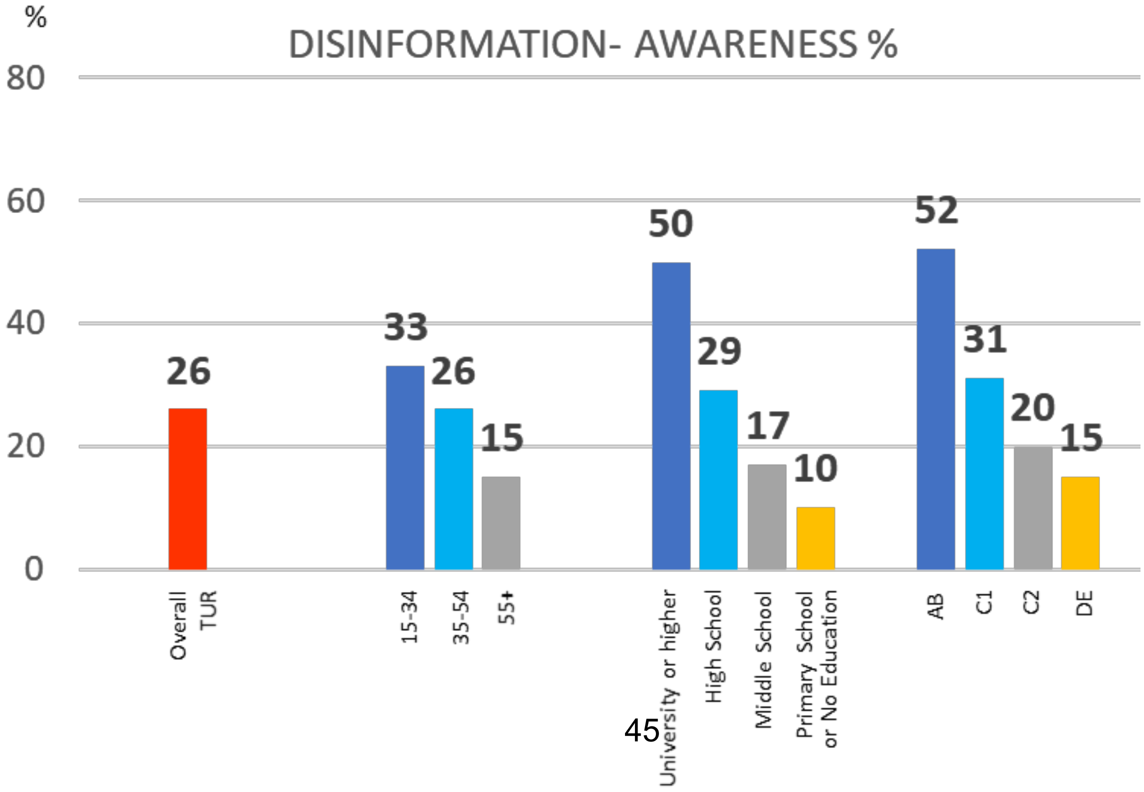


Figure 2



Hate Speech

The United Nations defines hate speech as ‘any kind of communication in speech, writing or behaviour, that attacks or uses pejorative or discriminatory language with reference to a person or a group on the based on an immutable characteristic they possess, such as religion, ethnicity, political nationality, political opinion, gender or other central identity characteristics.’[170] Hate speech could have disastrous effects on the severity of intergroup conflict. An infamous example comes from the Rwandan Genocide: radio broadcasts significantly increased civilian participation in the military-led violence.[171] This case demonstrates the dire consequences that unchecked hate speech can have on its targets.

Many of the desirable features of the internet which enable free expression[172] – such as anonymity, interactivity, immediacy, and global reach – also make it an extremely useful and effective way to spread hate speech and stimulate conflict. Partisanship is an important factor.[173] A study on the official Facebook pages of extreme-right political parties in Spain found that derogatory language was frequently used in posts and comments directed towards the groups’ political opponents.[174] Another study found links between anti-refugee comments on Facebook and crimes against refugees in Germany.[175] Similarly, the wide reach of social media has been linked to ethnic hate crimes – committed by groups or mobs - in Russia, especially in cities which had a higher baseline level of nati-

[170] United Nations (2019) ‘United Nations Strategy and Plan of Action on Hate Speech.’ Available at: https://www.un.org/en/genocideprevention/documents/UN%20Strategy%20and%20Plan%20of%20Action%20on%20Hate%20Speech%2018%20June%20SYNOPSIS.pdf

[171] Yanagizawa-Drott, D. (2014) ‘Propaganda and Conflict: Evidence from the Rwandan Genocide.’ *The Quarterly Journal of Economics* 129 (4): 1947–1994. https://doi.org/10.1093/qje/qju020

[172] Parker, D. and Song, M. (2006) ‘New Ethnicities Online: Reflexive Racialisation and the Internet.’ *Sociological Review* 54(3): 575–594.

[173] Adams, J. and Roscigno, J. V. (2005) ‘White Supremacists, Oppositional Culture and the World Wide Web.’ *Social Forces* 84(2): 759–778; Banks, J. (2010) ‘Regulating Hate Speech Online.’ *International Review of Law, Computers & Technology* 24(3): 233–239; Douglas, K.M., Mcgarty, C., Bliuc A, et al. (2005) ‘Understanding cyberhate: Social competition and social creativity in online white supremacist groups.’ *Social Science Computer Review* 23(1): 68–76; Ekman, M. (2018) ‘Anti-Refugee Mobilization in Social Media: The Case of Soldiers of Odin.’ *Social Media+ Society* 4(1): 1–11; McNamee, LG, Peterson, B. L. and Peña, J. (2010) ‘A Call to Educate, Participate, Invoke and Indict: Understanding the Communication of Online Hate Groups.’ *Communication Monographs* 77(2): 257–280; Perry, B. and Olsson, P. (2009) ‘Cyberhate: The Globalization of Hate.’ *Information & Communications Technology Law* 18(2): 185–199; Wahlström., and Törnberg, A. (2019) ‘Social Media Mechanisms for Right-Wing Political Violence in the 21st Century: Discursive Opportunities, Group Dynamics, and Co-Ordination.’ *Terrorism and Political Violence*, DOI: 10.1080/09546553.2019.1586676

[174] Ben-David, A. and Matamoros-Fernandez, A. (2016) ‘Hate Speech and Covert Discrimination on Social Media: Monitoring the Facebook Pages of Extreme-Right Political Parties in Spain.’ *International Journal of Communication* 10: 1167–1193

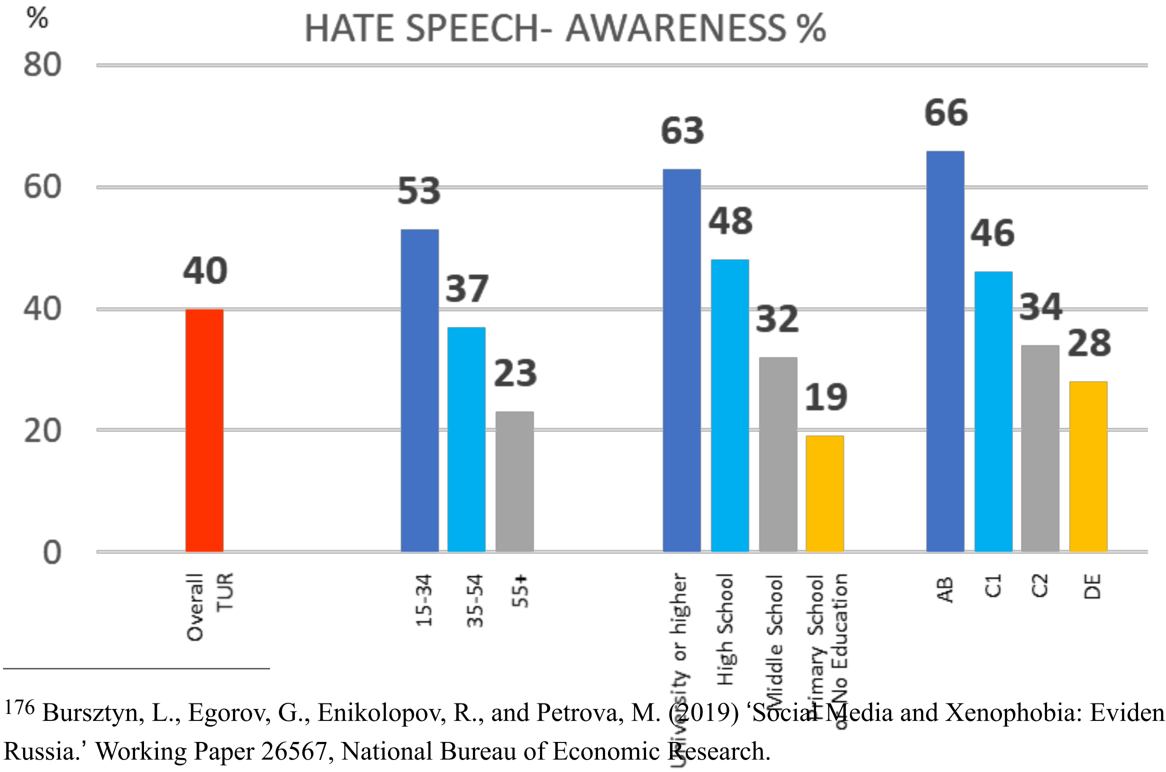
[175] Müller, K. and Schwarz, C. (2020) ‘Fanning the Flames of Hate: Social Media and Hate Crime.’ Available at SSRN: https://ssrn.com/abstract=3082972 or http://dx.doi.org/10.2139/ssrn.3082972

onalist sentiment before the introduction of online social media.[176] As these examples highlight, the role of the internet and hate speech in reports of hate crimes is gaining significance. In response, various technology companies actively tackle the problem by removing any content that can be classified as hate speech.

Turkey's markedly high rates of both social media use and partisanship mean that hate speech could potentially be a serious issue undermining democracy, peace, and security in the country. At present, online hate speech in Turkey is understudied. Twitter has been noted as a platform used to voice anti-refugee and racist sentiment in towards Syrians in Turkey. Armenians, Syrians and Greeks are the ethnic groups most often targeted by hate speech, both on and offline, where they are described as outsiders and threats.[177] Importantly, the Turkish legal system generally does not punish hate speech targeting minority groups.[178]

Our nationwide survey conducted with 3350 respondents inquired about people's awareness about hate speech: 'Could you please indicate whether you have a good idea of what each of these terms mean? Yes/No: Hate speech'. As Figure 3 below presents, 40% of the respondents state that they are familiar with the term hate speech. The proportion of awareness increases among people, who have higher levels of education, higher socio-economic status and are younger.

Figure 3



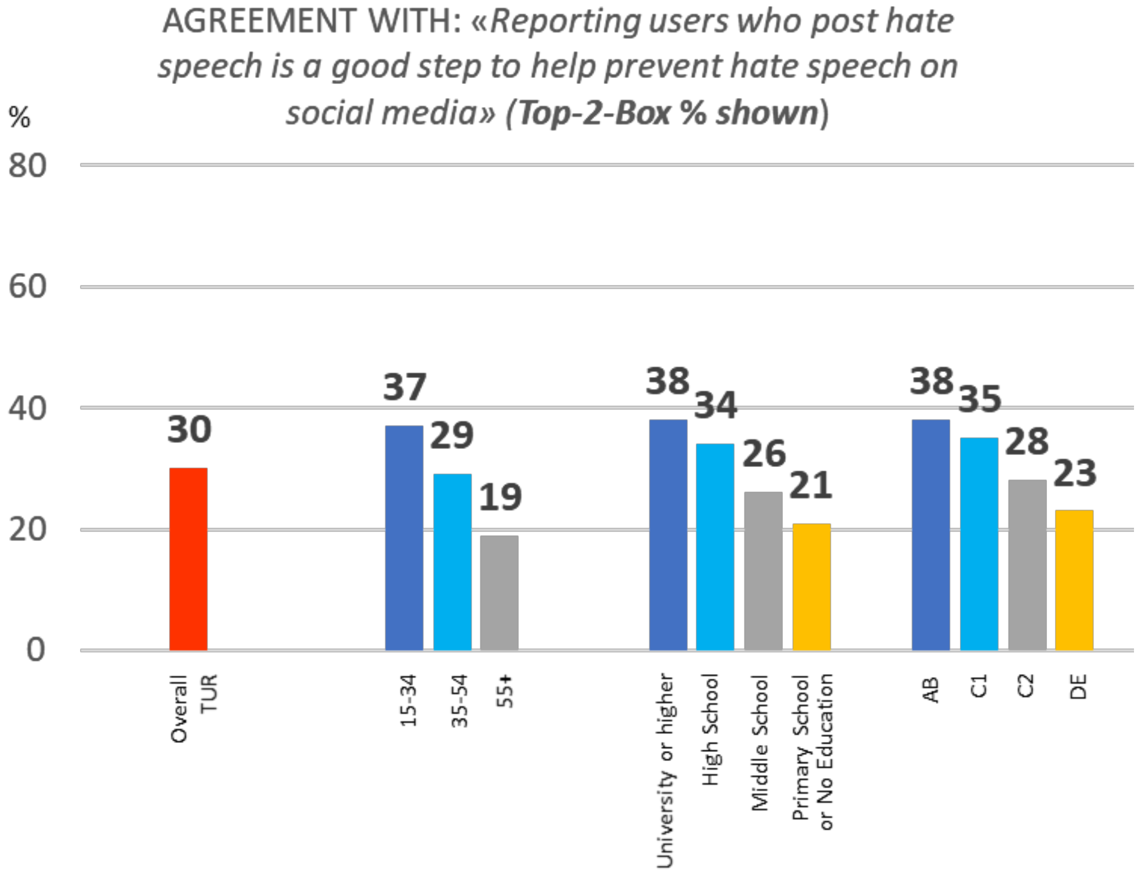
[176] Bursztyn, L., Egorov, G., Enikolopov, R., and Petrova, M. (2019) 'Social Media and Xenophobia: Evidence from Russia.' Working Paper 26567, National Bureau of Economic Research.

[177] Ozduzen, O., Korkut, U. and Ozduzen, C. (2020) "Refugees are not welcome': Digital racism, online placemaking and the evolving categorization of Syrians in Turkey.' *New Media and Society*, 1-21. DOI: 10.1177/1461444820956341 AND Dink Foundation. (2020) 'Media Watch on Hate Speech 2019.' Available at: https://hrantdink.org/attachments/article/2664/Nefret-soylemi-ve-Ayr%C4%B1mc%C4%B1-Soylem-2019-Raporu.pdf

[178] Deveci, C. and Binbuğa Kınık, B. (2019) 'Nationalist Bias in Turkish Official Discourse on Hate Speech: a Rawlsian criticism.' *Turkish Studies* 20(1): 26-48, DOI: 10.1080/14683849.2018.1479961

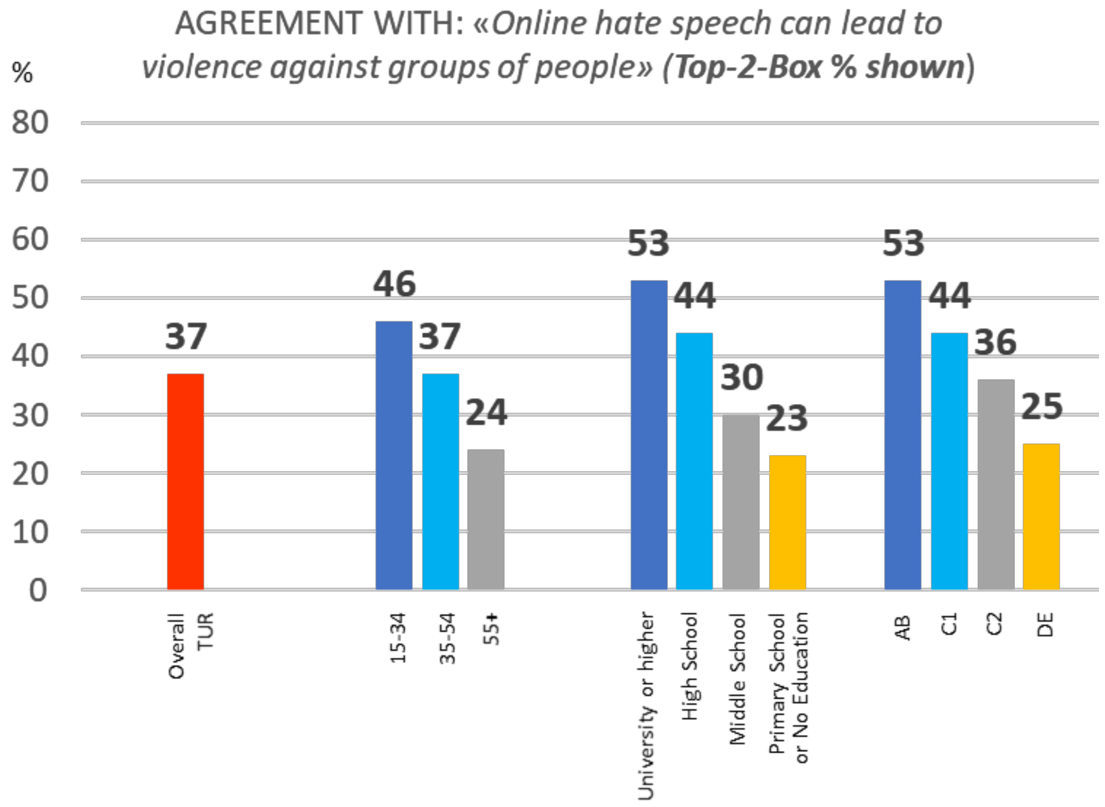
In addition, we asked whether they would agree with the following statement: ‘Reporting users who post hate speech is a good step to help prevent hate speech on social media.’ Figure 4 below shows that 30% of the respondents agree. Parallel to the findings on the awareness, the agreement increases among people with higher levels of education, higher socio-economic status and from a younger age group.

Figure 4



We also asked whether the respondents would agree with the following statement: ‘Online hate speech can lead to violence against groups of people.’ As Figure 5 below demonstrates, 37% of the respondents agree. The proportion of agreement among the respondents is higher among the ones who have higher socio-economic status, higher levels of education and are younger.

Figure 5



In short, the data illustrate lower levels of public awareness about hate speech in Turkey. Among the people with awareness, the majority agree with the two statements which underline the significance of hate speech for society. 30% of the overall population agreed with the idea of reporting hate speech, 37% of the overall population agreed with the potential relationship between hate speech and violence. Given that only 40% knew the meaning of the term, these data would mean that 30/40 (75%) and 37/40 (92%) of the people with awareness agreed with the statements. This might suggest that if the awareness is widespread among the population, the rate of agreement about the significance and dangers of hate speech would dramatically increase.

Cyberbullying

Although the term cyberbullying has been around only for two decades, it has been widely regarded as a serious health problem effecting children and adolescents today.[179] Cyberbullying is associated

[179] Aboujaoude E, Savage MW, Starcevic V, Salame WO. (2015) 'Cyberbullying: Review of an Old Problem Gone Viral.' *Journal of Adolescent Health*, 57(1): 10-18.

with increased rates of depression[180], fear[181], trouble sleeping[182] and a heightened risk of suicide.[183] Two comparative studies highlight the importance of cyberbullying in Turkey. A research on the cyberbullying perception among educators in Canada and Turkey finds that cyberbullying is seen as a problem in both countries and educators supported the idea of using an anti-cyberbully infused curriculum.[184] Another research on adolescents in Estonia, Italy, Germany and Turkey demonstrates that Turkish students perceived cyberbullying to be more serious than students from the other country, potentially indicating the larger impacts that cyberbullying could have on Turkish children.[185] The gradually expanding academic literature on cyberbullying in Turkey explores the factors that are associated with being cyberbullied through quantitative studies based on survey data. They find the following factors as significant predictors of cyberbullying victimhood:

- being male[186]
- loneliness[187]
- being single[188]

[180] Selkie, E. M., Kota, R., Chan, Y., and Moreno, M. (2015) 'Cyberbullying, Depression, and Problem Alcohol Use in Female College Students: A Multisite Study' *Cyberpsychology, Behavior, and Social Networking* 18(2): 79-86. http://doi.org/10.1089/cyber.2014.0371

[181] Randa, R. (2013) 'The Influence of the Cyber-social Environment on Fear of Victimization: Cyberbullying and School.' *Security Journal* 26: 331–348. https://doi.org/10.1057/sj.2013.22

[182] Sourander A, Brunstein Klomek A, Ikonen M, et al. (2010) 'Psychosocial Risk Factors Associated with Cyberbullying Among Adolescents: A Population-Based Study.' *Archives of General Psychiatry* 67(7): 720–728 doi:10.1001/archgenpsychiatry.2010.79

[183] Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). 'Bullying in the Digital Age: A Critical Review and Meta-analysis of Cyberbullying Research among Youth.' *Psychological Bulletin* 140(4): 1073–1137. https://doi.org/10.1037/a0035618

[184] Ryan, T., Kariuki, M., and Yilmaz, H. (2011) 'A Comparative Analysis of Cyberbullying Perceptions of Preservice Educators: Canada and Turkey.' *Turkish Online Journal of Educational Technology – TOJET* 10 (3): 1-12.

[185] Palladino, B. E., Menesini E., Nocentini A., Luik, P., Naruskov, K., Ucanok, Z., Dogan, A., Schultze-Krumbholz, A., Hess, M., and Scheithauer, H. (2017) 'Perceived Severity of Cyberbullying: Differences and Similarities across Four Countries.' *Frontiers in Psychology* 8: 15-24.

[186] Akbulut, Y., and Eristi, B. (2010) 'Cyberbullying and Victimisation among Turkish University Students.' *Australasian Journal of Educational Technology*, 27(7): 1155-1170; Aricak, T., Siyahhan, S., Uzunhasanoglu, A., Saribeyoglu, S., Ciplak, S., Yilmaz, N., and Memmedov, C. (2008) 'Cyberbullying among Turkish Adolescents.' *Cyberpsychology & Behavior* 11 (3), 253-261. DOI: 10.1089/cpb.2007.0016; Erdur-Baker, O. (2010) 'Cyberbullying and its Correlation to Traditional Bullying, Gender and Frequent and Risky Usage of Internet Mediated Communication Tools.' *New Media & Society* 12 (1): 109–125. DOI: 10.1177/1461444809341260.

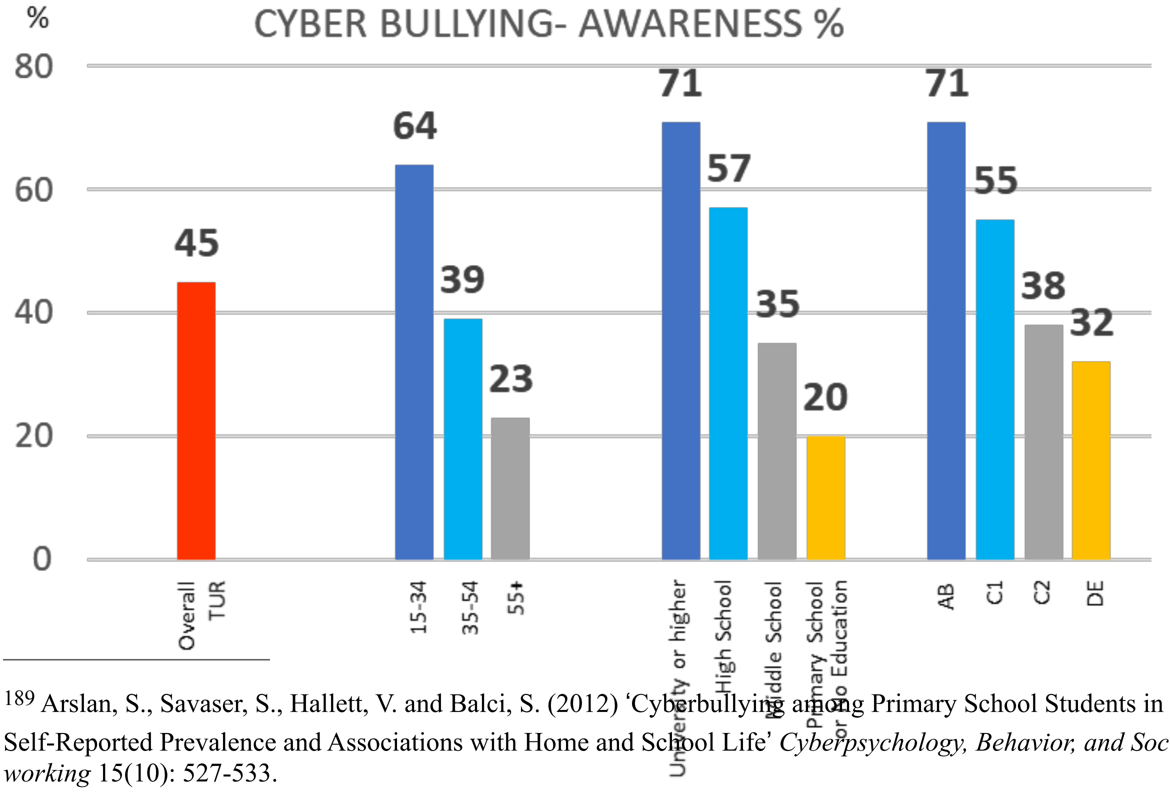
[187] Sahin, M. (2012) 'The Relationship between the Cyberbullying/Cybervictmization and Loneliness among Adolescents.' *Children and Youth Services Review* 34 (4): 834-837.

[188] Akbulut, Y., Sahin Y. L. and Eristi, B. (2010) 'One-to-One Learning in the Mobile and Ubiquitous Computing Age.' *Journal of Educational Technology & Society* 13(4): 192-201.

- lower levels of school satisfaction and achievement[189]
- duration of internet use[190]
- emotional instability[191]
- lack of emotional awareness[192]
- psychotism[193]

Our nationwide survey with 3350 respondents investigated people's awareness about cyberbullying with the following question: 'Could you please indicate whether you have a good idea of what each of these terms mean? Yes/No: Cyberbullying'. As Figure 6 below illustrates, 45% of the respondents confirmed to have a good idea about cyberbullying. Younger people, those with higher levels of education and/or from higher socio-economic status have higher proportions of awareness with respect to cyber-bullying compared to the rest of the population.

Figure 6



[189] Arslan, S., Savaser, S., Hallett, V. and Balci, S. (2012) 'Cyberbullying among Primary School Students in Turkey: Self-Reported Prevalence and Associations with Home and School Life' *Cyberpsychology, Behavior, and Social Networking* 15(10): 527-533.

[190] Topçu, Ç., Erdur-Baker, Ö., and Çapa-Aydin, Y. (2008) 'Examination of Cyberbullying Experiences among Turkish Students from Different School Types' *Cyberpsychology & Behavior* 11 (6): 643-648. DOI: 10.1089/cpb.2007.0161

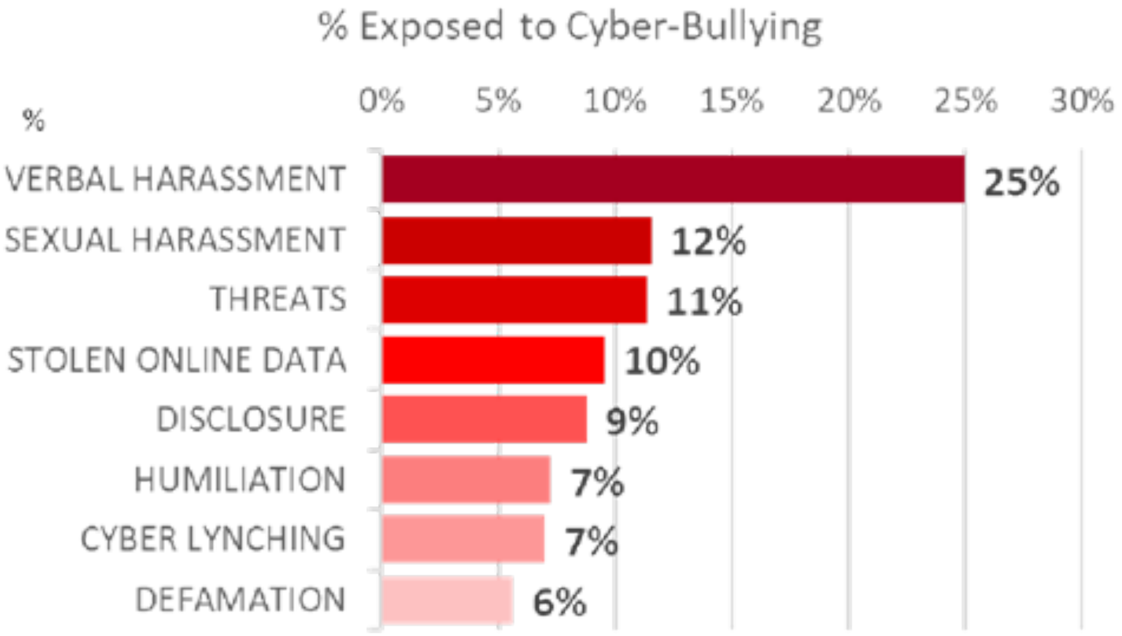
[191] Celik, S., Atak, H. and Erguzen, A. (2012) 'The Effect of Personality on Cyberbullying among University Students in Turkey.' *Egitim Arastirmalari - Eurasian Journal of Educational Research* 49: 129-150.

[192] Gül, H., Fırat, S., Sertçelik, M., Gül, A., Gürel, Y., and Kılıç, B. G. (2019) 'Cyberbullying among a Clinical Adolescent Sample in Turkey: Effects of Problematic Smartphone Use, Psychiatric Symptoms, and Emotion Regulation Difficulties.' *Psychiatry and Clinical Psychopharmacology*, 29(4): 547-557, DOI: 10.1080/24750573.2018.1472923

[193] Ozden, M. S. and Icellioglu, S. (2014) 'The Perception of Cyberbullying and Cybervictimization by University Students in terms of their Personality Factors.' *Procedia - Social and Behavioral Sciences* 116: 4379–4383.

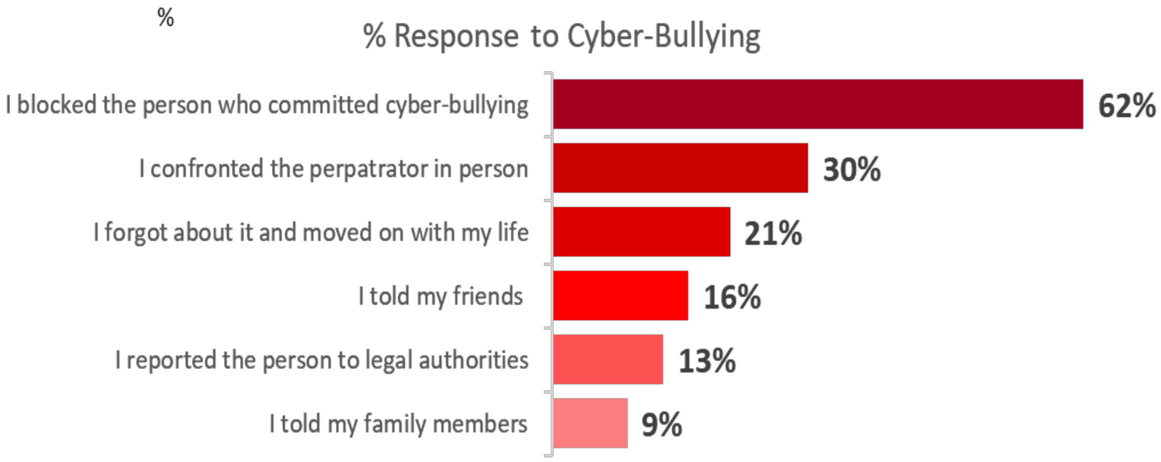
Our study also investigated the exposure to cyberbullying by inquiring to what extent the respondents experienced behaviors associated with cyberbullying in the following manner: 'I will read you some expressions. Considering your personal life please indicate whether you are exposed to any of these situations'. Figure 7 below illustrates definitions of these behaviors and to what extent the respondents were victimized. Verbal harassment is the most prevalent form of cyber-bullying. Around 1 in 10 people also report that they experienced sexual harassment or threats online as well as having their data stolen or their photos/videos shared without permission. Overall rate of those who have experienced at least one of these types of online behaviors is 33%. In other words, 1 in 3 respondents were the victim of at least one type of cyber-bullying.

Figure 7



The research also inquired about people's responses to being cyber-bullied in the following manner: 'You stated that you were exposed to some undesirable situations (cyberbullying) in the Internet environment. Please indicate which of the following best describes your behavior in that situation.' As summarized in Figure 8 below, blocking the person/account who committed cyber-bullying is the most frequent response. This is followed by confronting the perpetrator in person, forgetting about it, telling the friends, legal authorities and family members. Besides, another survey question asked the following: 'Which of the training programs regarding Digital Citizenship would you be interested in participating? Coping with cyberbullying.' 66% of the respondents acknowledged that they would be interested to attend a course on coping with cyberbullying.

Figure 8



All in all, the data underlines that while the majority of the respondents (55%) are unaware of the term cyberbullying, 33% of the respondents experienced one form of it. Moreover, there is a general interest in learning to cope with the cyberbullying among the respondents. This might suggest that if the public awareness increases, then there would be an increased interest in learning about the ways to cope with cyberbullying. Expanding on the findings from our study and academic discussions, the next section will discuss the ways the challenges to the digital citizenship in Turkey could be addressed.

3.3 The Path Forward: Recommendations

One should keep in mind that these challenges are not endemic to digital activities but widespread around the world with no definitive solutions. For example, although conspiracy theories are as old as human history, effective policies against them are yet to be discovered. Nevertheless, the findings of our research and the academic literature review form the basis of the following policy and practice recommendations:

Tackling conspiracy theories

1) Workshops on conspiracy theories – including characteristics and consequences – should be held jointly with Turkish political parties, given the prevalence of conspiracy theories along party lines. This may help to reduce their spread and impact.

2) Education curriculum at all levels should include information about the meaning and negative consequences of conspiracy theories.

Tackling fake news

1) Workshops on fake news – including characteristics and consequences – should be held jointly with Turkish political parties, which may help to reduce the spread and impact of fake news.

2) In line with the criticism to the scholarship for lacking bottom-up analyses on audience, the academic research on Turkey could include qualitative analyses on the effects and meaning of fake news to provide an in-depth picture on its significance. The scholarship is limited to quantitative research.

3) Education curriculum at all levels should include information about the meaning and negative consequences of fake news and how to spot them. Our nationwide survey demonstrated that only a minority of people know the meaning of trolling (47%) and disinformation (26%). Hence, the general public would be well served by any courses on the topic.

Tackling hate speech

1) Workshops on hate speech – including the characteristics and consequences associated with it – should be held jointly with political parties, given the prevalence of hate speech along political party lines. This may help to reduce the spread of hate speech.

2) Education curriculum at all levels should include information about the meaning and negative consequences of hate speech. Our nationwide survey indicated a lower level of general public awareness about hate speech in Turkey with 40% of the respondents knowing the term. It also noted that among the people who knew about the term, there was awareness about its consequences and how to respond to it. In other words, there is an urgent need to increase public awareness about hate speech, which would help to tackle the problem, as people seem to develop sensitivity against it once they know the meaning.

Tackling cyberbullying

1) In line with the importance of understanding the meaning of cyberbullying for young people and developing bottom-up approaches,[194] qualitative research should be conducted at schools to understand the meaning and consequences of cyberbullying in Turkey. At present, no such study exists.

2) Education curriculum at all levels should include information about the meaning and negative consequences of cyberbullying. Our nationwide research found that while the majority of the respondents (55%) did not know the meaning of cyberbullying, 66% of the respondents would be interested to attend a course about how to cope with cyberbullying. In other words, there is both a need and demand to increase public awareness about cyberbullying.

[194] Kofoed, J. and Staksrud, E. (2019) '"We Always Torment Different People, so by Definition, We are no Bullies": The Problem of Definitions in Cyberbullying Research.' *New Media & Society*, 21(4): 1006–1020.