Strengthening of Digital Literacy to Support Student Community Service to Prevent Hoax and Cybercrime

Chusnu Syarifa Diah Kusuma(✉), Riana Isti Muslikhah, and Suhartanto

Universitas Negeri Yogyakarta, Yogyakarta, Indonesia
chusnu@uny.ac.id

Abstract. In 2021, the number of internet users in Indonesia increased to around 202.6 million people. Social media have 170 million users with an average of three hours a day accessing social media. This increasing number raises new problems in the digital world, such as hoaxes and cybercrime cases. Most students are generation Z which considers active users of the internet and social media. For them, the Internet and Social Media are a thing that is Taken for Granted. Students are an agent of change through community service. Student Community Service is a free and sincere activity of students to help the community to achieve a better life. Then, this generation is important for the development of Indonesia. The article aimed to discuss the efforts to prevent digital crime as an act of anticipation through the strengthening of digital literacy. Also, this article discusses younger generation students as technology-literate to prevent hoaxes and cybercrimes. The student is a motor to create an advanced civilization of the digital world. To achieve that purpose, the student's community service is needed. Students are very close to community service as they are the youth and the future of the nation. The explanation method was used in this article. The conclusion was the need to strengthen students on insights into Digital Skills, Digital Culture, Digital Ethics, and Digital Safety to support the student community service and contribute to creating a smart digital user community.

Keywords: Digital Literacy · Hoax · Cybercrime

1 Introduction

In Indonesia, internet user is very active. According to datareportal.com, data per January 2021, 345.3 million of 274.9 million Indonesian people are active on a mobile phone connection. Among them, 202.6 million is internet user. And, 170 million people are active users of social media. Seen from internet using, they use 8 h and 52 min to access the internet through various devices. Users use 2 h and 50 min to watch TV, 3 h and 14 min to access social media, and 1 h and 38 min to read the news (both online and printed media). Moreover, the top five social media used in Indonesia are Youtube, Whatsapp, Instagram, Facebook, and Twitter. Internet access has become the primary need as it brings an easy way to people, such as getting fast and instant information. Especially,

J. Priyana and N. K. Sari (Eds.): ICERI 2021, ASSEHR 705, pp. 477–487, 2022.
https://doi.org/10.2991/978-2-494069-67-1_54

the internet becomes the media for online learning during the pandemic. Social Media, such as Instagram, not only be a diary but also play as media of self-promotion that bring huge benefits.

The culture of using digital media is an ability and skill of an individual in reading, understanding, analyzing, checking, and building insights to various daily problems. But, the main problem is that the high of internet penetration is not followed by the ability and skill of the user to receive a piece of information on the internet. That means, many Indonesian people are on the internet and obtain pieces of information without being equipped with adequate digital literacy. Per March 2021, The Ministry of Communication and Informatic has been recorded and labeled to 2.360 hoaxes on Covid-19, 1.857 contents on Facebook, 435 contents on Twitter, 45 contents on YouTube, 20 contents on Instagram, and 177 content on Vaccine of covid-19. Data on Polri (Indonesian National Police), accept 937 cybercrime cases from April to Juli 2021. From that number, the top three of the cases are provocative cases, hate content, and hate speech with a total of 473 cases. Then, it follows by online scamming of 259 cases and porn content of 82 cases.

Indonesia is currently in Demographic Bonus period where, according to the population census in 2020, most the population is from Generation Z/Gen Z, born between 1997 and 2012, (27.94%). The proportion of Millennial Generation is slightly below that of Gen Z, at 25.87%. This means that Gen Z plays a significant role in influencing the development of Indonesia at present and in the future. Gen Z characters are more diverse, global in nature, and influence the culture and attitudes of most people. One stands out point, Gen Z can take advantage of technological changes in various aspects of their lives. The technology that they use, is as natural as they breathe.

The Indonesian Internet Service Providers Association (APJII) on a survey conducted in 2019–2020 shows that internet users in Indonesia are dominated by the age group of 15–19 years (91%) and followed by the age group of 20–24 years (88.5%). The average user accesses the internet to open social media (51.5%) and communication (32.9%). This means that most internet users, especially social media, are Generation Z and Y (millennials). Gen Z was born and raised in overprotective parenting amid an uncertain world, such as economic recession, digital transformation, invasions in several countries, natural disasters, and disease outbreaks. These factors made generation Z becomes less tolerant of environmental ambiguity as they were raised in a too much-protected environment. The research of the American Psychological Association, cited in Media Literacy for Digital Natives: The Perspective of Generation Z in Jakarta (2018) confirms the findings. The ability to manage stress and achieve a healthy lifestyle decreases from generation to generation. If this phenomenon continues, Generation Z will be the most stressed generation in history. This condition is also related to the character of Gen Z who has no restrictions with other individuals. Then, they could be easier to be in unstable conditions due to receiving information and conditions that are rapidly changing and completely random.

The factors could be the reason for the frequent spread of hoaxes, so there is a need for digital literacy as an effort to filter the information received, especially on social media platforms. In order not to be provoked, a person needs to be a wise internet user by equipping themselves with digital literacy, such as always cross-checking the source of information and filtering the followed accounts. Also, it is important to equip the user

with digital safety skills, such as changing passwords regularly and not giving any data and information to others.

According to a report by the Check Point Institute, Software Technologies Inc., Indonesia is the third most targeted country in digital security threats after the United States and India. The financial industry and personal data are the sectors most vulnerable to digital security threats (Liputan6.com, 14 June 2021). The problem is that the technology can only mitigate the symptoms that arise in the information chaos but does not address the basic problem. The tendency to immediately believe what is read on the internet and the failure to verify must be addressed.

2 Discussion

Students who are mostly Generation Z are agents of change because students are the people who should bring positive changes and constructive impact on people's lives, as well as create positive values in society. Through community service, students may become the agent of change, especially in fighting hoaxes and cybercrime. However, students need to have adequate digital literacy before being involved in community service activities. Community service activities may be in education, such as training of digital literacy trainers.

2.1 Hoax

Around 1808, the term "Hoax" first appeared in English, in a book entitled Sins Against Science, wrote by Linda Walsh. The hoax also derive from the words of ancient witches "Hocus Pocus" in Latin "Hoc est corpus". It is used by the witches as a weapon to deceive others by turn out the words to be deceptive. The term hoax is also used by Thomas Ady in 1965, in a book entitled Candle in the dark. The term of Hoax became popular around 2006 that used in a film, with title of Hoax. The film is directed by Lasse Halstorm and starred by Richard Gere. The definition of hoax information is information that is not true, false, and invalid of information. In the Cambridge dictionary, the word hoax means a deceptive act, dishonest word, or false with the aim of misleading or a mere joke. In other words, outsmarting activities, trick cases are also called hoaxes. Furthermore, the site of hoaxes.org in a cultural context leads the definition of hoaxes are one of the deceptive activities. If the newspaper intentionally prints and contains fake stories and news, it is also the same with Facebook when the content is fake, we can call it a hoax.

The image of publicity maneuvers as fake bomb threats, false political claims, business fraud, scientific fraud, and poisoning is a hoax. Ahead of the election campaign of the governor of Jakarta in 2017, the production of hoax news is increasingly rampant.

Kumar and Shah [1] categorize false information based on its intention and knowledge content. False information based on the author's intentions is classified as misinformation and disinformation [2–4]. Misinformation refers to the unintentional spread of false information. Meanwhile, disinformation refers to the intentional dissemination and creation of an information [4]. Based on intentions, false information is defined as misinformation, which is created without the aiming to mislead. The common factor of misinformation includes misrepresentation or distortion of original information

by actors, due to lack of understanding, attention, or cognitive bias [2, 5]. In contrast, disinformation is created with the intention of misleading and deceiving readers [2, 3].

In a survey MASTEL in 2017, released by Kominfo, social media is the highest contributor media and disseminate of hoax issues. Social media is at the highest level by 92.4%, as a media used to disseminate and spread hoaxes. And, it followed by instant messaging applications by 62.8%. The pages/websites are the third places by 34.9%. In the place of fourth to seventh are television, printed media, email, and radio, but a percentage is less than ten percent. The data proves that social media is like a knife when it is not used properly.

Marino in Arwendria [6] distinguishes fake news or hoax into six types: (1) fantasy fake, is intentionally designed to entertain, such as other world stories about the emergence of Bat Boy and Elvis from Weekly World News, Enquirer, etc.; (2) funny fake, is designed to entertain; (3) fony fake, is designed to prank someone; (4) fallacious fake or elite propaganda, is misleading and only seeking for sensationalism; (5) flat fake or full power propaganda, is pretending to be satire and gets people to click on the link; and (6) falshivka fake or propaganda de ruski, fake news originating from Moscow.

Based on the type of content, the Parliamentary Office of Science and Technology [7] distinguishes hoax into six: (1) fabricated content, is completely false content, (2) manipulated content, is distorted information or original images, for example, more sensational titles and often popularized, (3) seductive content and imitation of original sources, for example using branding from established news agencies, (4) misleading content, use to misleading information, for example, presenting comments as facts, (5) connection error content, content factually accurate information but shared with contextual misinformation, for example; the title of the article does not reflect the content, (6) Satire and parody, presenting funny news but fake news look like if it were true. Social media can be used as a means of disseminating any kind of information. However, a critical attitude is needed to respond to any information. Belshaw [8] explains eight important elements of digital literacy, namely creative (doing new things), cognitive (expanding the mind), cultural (understanding the context), constructive (creating positive things), communicative (capable of communicating and networking), civic (supporting the realization of civil society), confident (confident and responsible), and critical (critically addressing content). Two important elements to ward off and anticipate coronavirus hoaxes are cognitive and critical. Cognitive can also be defined as an attitude to broaden the horizons of thinking. While the critical element requires social media users to activate critical power when they receive information. Here, users should filter the information on social media, and not just accept the information they receive. One of the critical action of responding to hoaxes on social media is by understanding the patterns of spreading hoaxes that often appear on social media. Some patterns used to spread hoax news include, (1) Start with words that are suggestive and exciting, (2) Often use the name of a well-known person or organization, (3) Unreasonable, and often accompanied by incorrect research results, (4) Does not exist in mainstream media, and is usually only come via SMS or websites with unknown attribution, (5) Usually accompanied by capital letters or exclamation points.

The following are the tips to identify whether the news is a fact or a hoax. (1) the urgent or normal of news because it has been widely reported in various media, and

group members also get it from many other places, (2) Is the source of news from a reliable expert or unknown source? (3) Pay attention to the source of the news. If it is from the media, is the media valid and reliable? If it is not from the mainstream media, should not share it with other people, (4) Is the information important, useful, and urgent, or ordinary, or maybe it is not suitable for the group? (5) Am I sending this news with a motive to be seen as cool, always up to date, or the fear of missing out (FOMO), then eager to share? 6. Think again before sharing, such as does it harm us if we do not share? If it is not harmful, it should stop sharing. Because the same or similar information may have been read by other people through other sources.

2.2 Cybercrime

Cybercrime is a crime that uses the computers and internet as a media for committing the acts of criminal. Cybercrime includes copyright infringement, and hacking, child pornography and exploitation. It also includes a lost or stolen confidential information that breaches the privacy.

Also, Cybercrime refers to activity of criminal using a network or computer as a place, target, and tool of crime, such as check forgery, online auction fraud, confidence fraud, credit card fraud/carding, child pornography, identity fraud, etc. According to Brenda Nawawi [9], cybercrime is a new phenomenon in crime due to a direct impact of the development of information technology. Some terms of this new cybercrime label added, such as (virtual-space/Cyberspace offense), a new dimension of "transnational crime", a new dimension of "white-collar crime", and a new dimension of "hi-tech crime."

According to Sutanto [10] in his book on cybercrime-the motives and prosecution of cybercrime consist of two types. First, crimes use information technology (IT) as a facility. For example, piracy (copyright or intellectual property rights, etc.); pornography; credit card fraud and theft (carding); e-mail fraud; fraud and bank account break-ins; online gambling; terrorism; perverted site; internet materials related to Sara (such as the spread of ethnic and racial or religious hatred); transaction and distribution of illegal drugs; sex transactions; and others. Second, Crimes target information technology systems and facilities. This type of cybercrime does not use computers and the internet as a medium or means of criminal acts but makes it a target, such as illegal access of a system (hacking), destroying internet sites and data servers (cracking), and defecting.

The cybercrime qualifications as quoted by Barda Nawawi Arief in Ronal [11], are qualifications for cybercrime referring the Convention on Cybercrime in Budapest, Hungary in 2001. They are: (1) Illegal access: intentionally accessing a computer system without rights; (2) Data interference: have no rights and intentionally deleting, changing, destroying or deleting computer data; (3) Illegal interception: have no rights and intentionally to secretly capture or hear the transmission and dissemination of private computer data, from or within a computer system using technical aids; (4) System interference: intentionally doing serious barriers or interference without rights to the computer system function; (5) Devices Misuse: computer tools misuse including computer passwords, access codes, and computer programs; (6) Computer related Forgery: Forgery (have no rights and intentionally changing, entering, deleting authentic data to

become inauthentic data with the purpose of being used as authentic data); (7) Computer related Fraud: Fraud (have no rights and intentionally make the loss of other people's property/goods by changing, entering, deleting computer data or by interfering the functioning of a computer system, with the motive of economic benefits). To prevent cybercrime, the government and Police need to immediately take countermeasures and law enforcement, namely by disseminating, realizing, and implementing various existing laws and regulations, such as the Criminal Code and the ITE Law to ensnare the actor of cybercrime.

The action of Cybercrime countermeasures in Indonesia is: (1) A technological approach in Cybercrime Prevention Efforts to Secure Computer Network Software. The Preventive actions of the approach are (a) Regulating access (access control) through an authentication mechanism using a password, (b) Firewall, a program which is a device that is placed between the internet and the internal network to block access in and out of unauthorized persons, and (c) Intruder Detection System (IDS), including Autobase that detects probing by monitoring log files, and (d) Routine backup, for backup when the system is successfully entered by other (intruders), etc. (2) Hardware Security in Cybercrime Prevention Efforts. The steps are Computer locking, Using of dial back is the use of double telephones to make and accept a phone call, by taking turns in using telephone lines. (3) Efforts to disseminate information on computers and the internet amid society, including (a) Introduction to computers and the internet through education; (b) Information Technology Seminars to introduce computer technology to the public. The seminars are very helpful for the public. The seminars can be in the form of interactive discussions, book reviews, seminars and training, workshops, and so on. (4) Law Enforcement against Cybercrime Transnational crime in cybercrime will relate to jurisdictional issues. In cyberspace, it is difficult to act against actors as they are outside the territory of Indonesia. This problem later will be a matter of jurisdiction of cybercrime enforcement in Indonesia. This means, which law will be applied in dealing with cybercrime. Then, several aspects related to cybercrime law enforcement efforts include aspects of officers for law enforcement, legal instruments, and implementation.

2.3 Digital Literacy

According to Graff [12], literacy is the ability of a person to write and read. The benefits of literacy are (a) Increase vocabulary, (b) Optimizing brain performance because it is often used for reading and writing activities, (c) Gaining new insights and information, (d) Better on interpersonal skills, (e) Increasing ability to understand to information, (f). Improve verbal ability, (g) Improve analytical and thinking skills, (h) Help improve the focus and concentration ability, and (i). Improve ability to compose meaningful words and write (www.dosenPendidikan.co.id). Literacy is very relevant to the era where human life is dominated by information technology, namely the digital literacy. In general, possessing digital literacy means that you understand how to use digital information, according to Putra in Sumiati [13]. Gilster [14] defines digital literacy as the ability to use and understand information in many formats from various sources when it is presented on a computer [15]. According to Brian in 2015, a journal written by Maulana [14] mentioned 10 benefits of digital literacy. They are (1) Save money, (2) Always up to date, (3) Save time, (4) more secure, (5) Learn faster, (6) Always connected, (7)

Making better decisions, (8) Provide a job, (9) Makes happier, and (10) Influence the world. According to Kominfo, Cybercretion and Deloitte (2020), in the world of digital literacy, also need to learn about digital skills, digital culture, digital ethics, and digital safety.

2.3.1 Digital Skills

The Essential of Digital Skills [16] outlines five categories of digital skills and the tasks within each category. Those categories is needed by individuals, aiming they classified as have digital skills for work or digital skills for life: (1) Communication skills; needed to collaborate, communicate, and share information, such as sending e-mail and using word processing software. (2) Handling content and information skills: needed to manage, secure, and find store digital content and information, such as the skills to assess the internet content reliability and use search engines. (3) Transactions skills: needed to sell and buy services and goods, apply and register for services, and manage online transactions. For example, the ability to purchase and book for tickets online. (4) Troubleshooting skills: needed to find solutions to problems in using online services and digital tools, such as using video tutorials to learn how to do something and live chat facilities to solve a problem. (5) Be secure and safe, and legal online: the skills needed to stay legal, safe and confident online, such as recognizing suspicious links in emails and settings the privacy on social media.

The framework also outlines a digital 'foundation' set of skills as the basic skills that underpin essential digital skills and consist the ability to perform tasks, such as connecting to trusted Wi-Fi networks and turning on devices. A person, who has digital skills essential for life, can perform all tasks at the basic level, or at least have one task from the five skill categories.

2.3.2 Digital Culture

The digitalization process started having an impact on culture that is caused by the widespread use of personal computers and other digital devices, as well as the advance of the Internet as a mass communication. For example, smartphones lead to the digital culture phenomenon. Digital technology has penetrated to human life. Then, many studies on digital culture have the potential to cover all aspects of everyday life. And, it is not limited to modern communication technologies or the Internet.

The digital culture concept is seen as a function of socio-economic systems and an ideology of management based on the sharing and penetration of digital technologies. This human society phenomenon is based on global changes in communication, interaction, and technology, system interactions with the external environment and in intrasystem processes. The concept of digital culture cover methods, rules, traditions, norms, and decision making and communication forms. The central core of digital culture is values system that characterizes how an organization (system) supports and promotes the use of digital technology in its function, with the efficiency goal. Therefore, the "digital culture" term refer to a single space of an information technology to bring about

almost complete and a clear transformation of the world, with the help of digital technology. And, those will ensure the unification the external environment elements and individual components into a single production super-system.

Digital culture reflects the development stages of the phenomenon of culture within society in the 21st century. It is based on several things, such as digital social networks and communication technology, digital visualization and images, space virtualization and the material world, digital and information systems, and creating technology-based value systems. The digital culture phenomenon is often linked to the common media transformation as the primary way of information and communication—starting from broadcasting and printing with the same content for all users, personalized networks and media using digital technologies for the information content processing and transmission.

Digital technology changes the information material characteristic (in this case, education) based on digital databases and automated. This phenomenon lead to a general change in the digital environment and information which often understand in digital culture as an algorithmic processes culture (then called "algorithmic culture")—this is personalized social media channels, content, personalized advertising and recommendation systems on the Internet, etc. Digital databases, at the same time, are much more flexible than non-digital. Also, it provide chances and opportunities—internet platforms, social networks, search engines, etc. [17].

2.3.3 Digital Ethics

Today, many people still do not understand the practice of digital ethics conducted by IT companies as there is gaps in laws. There is minimal consensus on the investigation of political philosophy and moral, with major disagreements, even on ethics of basic digital. The biggest challenge in digital ethics is to examine the unseen or never exist elements, with various consequences and effects on established traditions and morals. Uncontrollable risk is attached as the uncertainty condition created by new technology companies, followed by questions about new technologies. Outcomes in digital ethics and uncontrolled possibilities are common that caused by the inability to predict the effects of different new technologies on society due to the theoretical nature of perceived outcomes [2]. The main problem of modern technology poses to digital ethics is the privacy breach by analyzing the big data technologies, which are used to make a decision by business organizations [18]. Data aggregation technology is very important in the collection of personal data. And, important questions arise whether the business activities are ethically acceptable, as data is used in decisions making about production and marketing strategy [19]. Privacy is any personal information, including data of financial, medical, behavioral, biographical and biometric from analytics of business. In sum, data analysis violates the boundaries of personal privacy when the use of personal data without the consent of the information data owner [20]. While there are privacy concerns about how a business collects personal data, it might be an option not to accept for a business to have consent from the data owner. Generally, companies collect data of their user to increase service to customer by offering more personalized products and services [21].

2.3.4 Digital Safety

Digital safety is the ability of individuals to recognize, group, apply, analyze, and improve digital security in everyday life. Digital safety is a guide for individuals to keep themselves safe. Therefore, it needs to be equipped with basic knowledge of hardware protection features, protection of digital identity and personal data on digital platforms, digital fraud, digital track records in media (downloading and uploading), and minor safety (catfishing).

Digital safety is also one of the areas of competence in digital literacy frameworks, such as DigCom and the Digital Literacy Global Framework [22]. Based on the DigCom 2.1 digital literacy framework, digital safety in this study refers to the competence area of safety which consists of 4 competencies as indicators, namely: (1) protecting privacy and personal data; (2) protecting devices; (3) protecting the environment, and (4) protecting well-being and health [22].

An effort to keep privacy in cyberspace is to be aware of the digital footprints. Digital footprints are all forms of digital traces, created by the user on the digital media device. When entering and logging on the internet, users leave a digital footprint, both a passive or an active footprint. Passive user footprints are traces that appear automatically (such as browsing history, cookies). While the active user footprint is consciously created (joining/registering to a site/application where a user provides personal information/data, sharing location, spreading articles from one site to other users, etc.).

Digital footprints clearly have potential dangers, for example, access to personal data, identity theft, doxing, and framing. Therefore, it is a priority to leave a good digital record and footprints. Digital footprints are difficult to remove and take many forms. Besides that, digital footprints are lifelong profiles of good conduct. Digital footprints are also important for professionals (work, social education, etc.) and personal (family, friendship). The tip is, not to post randomly just because it is fun, enjoyable, and viral, but to do important posts ethically and legally.

3 Conclusion

Students are mostly of Generation Z. And Generation Z is possible to take advantage of technological changes in various aspects of their lives. Also, Gen Z is called an agent of change whose role is to help to prevent the spread of hoaxes and cybercrime through digital literacy.

Digital literacy consisted of digital skills that included the skills of (1) communication, (2) transactions, (3) handling content and information, (4) being safe and legal online, (5) problem solving, as well as digital culture, digital ethics, and digital safety. In other words, it needs to strengthen the insight among students into digital skills, digital culture, digital ethics, and digital safety. The factor is urgent because, in community service activities, students might contribute to creating an intelligent digital user community.

References

1. S. Kumar and N. Shah, "False Information on Web and Social Media: A Survey," no. May, 2018.
2. D. Fallis, "A Functional Analysis of Disinformation," 2014.
3. P. Hernon, "Disinformation and misinformation through the internet: Findings of an exploratory study," *Gov. Inf. Q.*, vol. 12, no. 2, pp. 133–139, 1995.
4. C. Wardle and H. Derakhshan, "Information disorder: Toward an interdisciplinary framework for research and policy making," *Counc. Eur. Rep.*, pp. 1–108, 2017.
5. B. Skyrms, "The flow of information in signaling games," *Philos. Stud.*, vol. 147, no. 1, pp. 155–165, 2010.
6. A. Arwendria and A. Oktavia, "Upaya Pemerintah Indonesia Mengendalikan Berita Palsu," *Baca J. Dokumentasi Dan Inf.*, vol. 40, no. 2, p. 195, 2019.
7. U. Parliament, "Developing essential digital skills," *Postnote*, no. 643, pp. 1–6, 2021.
8. D. A. Belshaw, "What is 'digital literacy'? Douglas A . J . Belshaw," *Durham E-Theses Online*, vol. 0, pp. 0–274, 2012.
9. No name, "No title," no. 1, p. 282, 2008.
10. L. Andri Wijaya, "Cybercrime Comparison under criminal law in some countries," jurnal pembaharuan hukum, vol. V, no. 2, p. 217–226, 2018.
11. Ronal, "Kata Kunci : Cyber Crime Tinjauan Yuridis 1," vol. 7, pp. 1–14, 2015.
12. H. J. Graff and J. Duffy, "Literacies and Language Education," *Literacies Lang. Educ.*, no. January 2014, 2016.
13. E. Sumiati and Wijonarko, "Manfaat Literasi Digital Bagi Masyarakat Dan Sektor Pendidikan Pada Saat Pandemi Covid-19," *Bul. Perpust. Univ. Islam Indones.*, vol. 3, no. 2, pp. 65–80, 2020.
14. M. Maulana, "Definisi_Manfaat_dan_Elemen_Penting_Lite," pp. 1–12.
15. N. Pratiwi and P. Nola, "Pengaruh Literasi Digital terhadap Psikologis Anak dan Remaja Nani," *J. iIlmiah Progr. Stud. Pendidik. Bhs. dan Sastra Indones.*, no., pp. 1–24, 2019.
16. The Tech Partnership, "Essential Digital Skills," *LLoyds Bank Consum.*, p. 9, 2018.
17. I. Levitskaya and M. Straka, "The Digital Culture of Industry in the Transition to Sustainable Development," *E3S Web Conf.*, vol. 278, p. 03019, 2021.
18. B. Schermer, S. Van Der Hof, B. Custers, F. Dechesne, and W. Pieters, "eLaw Working Paper Series," no. 2018, 2019.
19. J. Damen, L. Köhler, and S. Woodard, "The Human Right of Privacy in the Digital Age," *Staat, R. und Polit. – Forschungsund Diskuss.*, no. 3, 2017.
20. A. Rezgui, A. Bouguettaya, and M. Y. Eltoweissy, "Privacy on the web: Facts, challenges, and solutions," *IEEE Secur. Priv.*, vol. 1, no. 6, pp. 40–49, 2003.
21. A. Zwitter, "Big Data ethics," *Big Data Soc.*, vol. 1, no. 2, 2014.
22. S. Carretero, R. Vuorikari, and Y. Punie, *The Digital Competence Framework for Citizens With Eight*, no. May. 2017.