Ethics in Cybersecurity. What Are the Challenges We Need to Be Aware of and How to Handle Them?

Denitsa Kozhuharova, Atanas Kirov(✉), and Zhanin Al-Shargabi

Law and Internet Foundation, Sofia, Bulgaria
{denitsa.kozhuharova,atanas.kirov}@netlaw.bg

Abstract. In the field of research, the role of ethics grows more and more every year. One might be surprised but even in the field of technology there is a necessity for experts to understand and to implement ethical principles. Ethics itself could be understood as a code or a moral way by which a person lives and works. But within the field of information technology and cybersecurity research there is a chance that even the most technical appropriate solution does not go in line with the corresponding ethical principles. Experts need to implement fundamental ethical principles in their technical products in order not to cause harm or have any negative effect on their users. To the vast majority of challenges that will be reflected in this chapter are discussed within the EU-funded project GUARD, namely what are the proper actions which need to be taken to ensure ethical compliance. Challenges such as ensuring the privacy of the users, reporting and handling incidental findings, testing the technological product, mitigating biases etc. could have different negative effect on humans if not dealt with properly. The current chapter would explore the questions posed above alongside a description of a methodology resulting in the combined efforts of experts both in the field of cybersecurity and ethics.

Keywords: Cybersecurity · Ethics · Cyberethics · Data · Privacy · Hacking · Information · Incidental findings · Assessment · Risk · Measures · Guidance · Mitigation

1 Introduction

Ethics can be understood as the code by which one should live, work, and treat others. Humanity has always been in pursuit of guiding principles, which would lead its actions and shape its communities. There are numerous schools of thought that seek to understand what makes certain actions ethical and how people can make ethically sound choices. Consequentialists for example link the morality of actions to their effects, with utilitarianists justifying all actions if in the end they are in pursuit of the greater good. Deontologists seek fundamental rules and principles which should guide individuals throughout their life. The list of conflicting views on what is ethical is ever-growing. Different cultures and religions also differ in their understanding of ethics.

J. Kołodziej et al. (Eds.): Cybersecurity of Digital Service Chains, LNCS 13300, pp. 202–221, 2022.
https://doi.org/10.1007/978-3-031-04036-8_9

Still, there are some views that seem to be universal. For example, every individual would condemn any harm done to innocent people or every individual puts high value on their right to privacy and freedom. There are certain ethical principles that are overarching and shape our understanding of the world around us. They guide us during our private life and often they can also shape the way we carry out our work and professional arrangements. In this trail of thought, there are many ethical principles that different professional field have accepted as values linked to loyalty and honesty. There are certain moral expectations we have when thinking of professionals. This is because we are dependent on them, their professionalism and moral integrity. We have become accustomed to erase the human element to all things linked to technology. But with the evolution of technology and our almost absolute dependency on it, cybersecurity professionals are facing increasingly more moral and ethical dilemmas.

When thinking of cybersecurity professionals, we seem to undermine the humanitarian aspect of their profession. However, on the other side of our screen there is a whole team of professionals that strives to protect our personal data, fight off malicious attacks, and manage a wide range of security risks. These individuals are left in a field with little or no legal guidelines to ensure a universal standard of protection. With the evolution of newer and newer technologies, like cloud computing, artificial intelligence (AI), Internet of Things (IoT), the risks continue to grow and to test our understanding of what is ethical and what is not. Can hacking be justified if it is in response to an established breach? Is the market for zero-day exploits something that should be supported? How do we ensure the privacy of users in the era of big data and cloud computing? These and more questions continue to challenge both professionals and scholars. This chapter seeks to examine some of the key ethical discussions in cybersecurity.

Firstly, under Sect. 2 it will focus on contemporary ethical issues in cyber security. This includes some of the well-known issues, such as data privacy and security breaches. A detailed analysis will cover questions relating to hacking, the reasons behind hacking and types of hackers. Furthermore, it is also important to examine risks in new and emerging technologies in relation to that under the next subsection this chapter will focus on topics concerning Internet of Things and Cloud computing. Here the ethical dilemmas are again connected to issues similar as the above-mentioned ones. The next subsection will examine the morality of testing new technologies which could have an effect on individuals and their well-being. Lastly, Sect. 3 will focus on some possible mitigation measures in order to ensure not only ethical compliance but also compliance with the relevant legal provisions.

2 Contemporary Ethical Issues in Cybersecurity

The ethical issues that arise in the field of cybersecurity vary in terms of the activities implemented by the stakeholders and the legal requirements in regard to the level of security. The intensity of the risks that may arise to the individuals should be also considered. With the increasing advent of new technologies, cybersecurity related ethical risks could occur in any area of everyday life – the economy, healthcare, public safety, transportation, etc. and to cause different level of harm to the individuals.

The risks themselves have different effects on them – some have a direct consequence on their rights such as violation of their privacy and dignity [20], others can have a

detrimental effect on their economic activity such as hacking and other types of security breaches [7]. Before any mitigation measures are taken to address the specific risk, the concerned entities must become well acquainted with it so they are able to take the most appropriate measure to address it and to reduce any harmful effect that may be caused.

2.1 Data Privacy of Users

Processing of personal data presents some inherent risks to the rights of individuals [5]. The data may be lost, destroyed, subject of an unlawful change, disclosed to unauthorized parties or processed in an unlawful manner. The risks that could occur from the processing of personal data could vary depending on the nature and scale of processing. Large-scale processing including the processing of sensitive data, have a higher risk for individuals [16]. It is important to properly identify, address and mitigate any risks in advance, significantly limiting the negative impact on data subjects as a result of the processing.

Besides a fundamental human right, data privacy is of great importance since it tackles information inequality. Usually, individuals are in adverse position when negotiating contracts about the use of their data and do not have the means to check if their counterparties are living up to the terms of the agreement. Data protection regulations ensure fair conditions and adequate protection measures when transferring data [40]. Furthermore, data privacy protects individuals from discrimination [19]. It is well known that personal information when used in different context may lead to unfair treatment and disadvantages for the data subjects. This is especially the case with the uncontrolled use of new technologies with the motive of protecting public security. Privacy regulations are restricting the usage of sensitive information thus protecting individuals especially in marginalized communities from unfair treatment and harm [24]. Finally, privacy regulations will preserve human dignity and protect people from outside forces that could have negative effect on their decision-making process.

Special attention should be granted to some types of data that processing would require the implementation of additional protection measures. Such example is the data managed by healthcare systems and organisations or the so-called health data. This according to the General Data Protection Regulation (GDPR) is any data related to the physical or mental health of an individual including information that is related to the provision of health care services. Health data is considered as special category of personal data and could be processed only on several explicitly stated grounds in the GDPR. This chapter will not emphasize the grounds for processing this type of data, but it will present some challenges and mitigation measures that need to be considered. In any case, data controllers that are processing health data and medical institutions should do any activity related to this specific type of data in secure environments that are ensuring the security of the information.

Here we should conclude that the establishment of common ethical principles for lawful data processing is essential for risk governance and mitigation. The principles should take into consideration basic fundamental rights envisaged in international conventions and cover how to obtain, use, process, and store personal data. With their help data controllers must always demonstrate transparency and guarantee the data subjects rights under the GDPR.

2.2 Security Breaches and Risks. Contemplating the Idea of "Ethical Hacking"

When discussing cybersecurity issues, most people would equate this field to any and all efforts to combat hacking and cyber intrusions. All of us face concerns that malicious individuals will manage to gain access to our devices, our personal data, financial information, etc. and misuse it for personal gain. Still, this chapter seeks to question these ideas. Is hacking always unethical? What are the current ethical dilemmas linked to hacking and cyber intrusions?

Types of Hackers

Scholars in the field of cyberethics differentiate hackers based on their intention and practices [3, 36]. Some researchers have even set apart the hackers from the early days of the Internet [27]. These hackers were not at most driven by malicious intent but engaged in hacking activities for personal satisfaction or recognition [27]. This raises the question if these hacker's activities did not pursue material gain and cause material harm, are they still ethically reprimandable? Here, the answer should be in the affirmative. No matter the incentive, hackers still breach the privacy and security of private devices and data, this cannot be accepted, even if it was done with no serious intentions behind it.

These considerations are no longer as relevant. Hackers now by large are incentives by their personal and material gain. With the development of the Internet, the main intentions behind hacking have substantially changed [27]. As we become more and more dependent on technologies, all spheres of our life become linked to the Internet and to a wide range of devices. The cyber sphere today contains everything linked to a person: personal information, intellectual property, banking information, trade secrets, security passwords, etc. [27]. This should not only be said in the context of the individual, most services also are heavily dependent on the Internet, as more and more public and private services become digitalized. The banks, hospitals, schools, military, small business as well as transnational corporations are intangibly linked to the cyber sphere. This creates millions of opportunities for people skilled in programming and cyber intrusions to generate large profit in exchange for access to critical data [27]. A hacker can not only steal our banking information and go on a spending spree, but they can also carry out an attack against our online election systems under the guidance of a third party (which can be a foreign government or terrorist group for example) and get millions in payment. There is a multitude of lucrative opportunities that can incentivize modern hackers to carry out their cyberattacks. Thus, it seems that the early days where online savvy youngsters broke into systems for fun and recognition, but had no ill intent, have become out-of-date and a different classification, more aware of the intentions behind hacks, must be used.

Such a classification for hackers, which is based on the reasons behind their actions, is: white hat hackers, black hat hackers and grey hat hackers.

White Hat Hackers

White hat hackers are those that pursue legitimate goals and have gained authorization for their activities [36, 51]. Often these individuals are hired by different companies to test their security systems and find security vulnerabilities. For example, regarding a potential security issue, a group of white hat hackers would utilize similar methods used

by malicious hackers in order to find the potential exploits. But instead of causing harm or stealing data, this would be done in order to pinpoint vulnerabilities and create guidelines how to cure them [30]. An important contribution of white hackers in business, would be their impact of securing company networks and in this way protecting trade secrets and business practices. Furthermore, authors have recognized how white hat hackers help guarantee a seller's product security [30].

It is important to note that the white hat hackers can be employed solely by one company or work as a freelancer and help numerous companies. Interestingly, there are situations where white hat hackers offer their services for free for certain institutions or other bodies in need. For example, during the COVID-19 pandemic there was a rise of cyberattacks against hospitals, which led to a group of professionals to create the Cyber Alliance to Defend Our Healthcare, which aims to help hospitals strengthen they cybersecurity systems and avoid risks and counter attacks [54].

Black Hat Hackers

Black hat hackers on the other hand act in an illegal manner [3, 27, 36]. Often when we think of hackers, we think of this subgroup which in the pursuit of monetary gain, for example cause harm to us and our communities. Some of the methods used most often by these hackers include [26]:

- Phishing
- Ransomware
- Worms
- Viruses
- DoS/DDoS Attacks
- Cookie theft

Grey Hat Hackers

These hackers sit on the intersection between white and black hats, thus their activities raise the most ethical debates. They could be in pursuit of higher ideological goals, or they could be influenced again by purely personal incentives such as looking for entertainment [3, 27, 36]. They may break certain legal restraints, but ultimately, they would not seek out causing harm. Most grey hats abide by their personal understanding of ethical questions and their own established ethical principles.

Another concept that causes ethical questions is 'hacktivism' [52]. This phenomenon is linked to instances where hacking was carried out with a particular social or political goal which would seemingly justify the use of illegal methods of intrusion, or any harms caused by the actions. Such instances could include attacks carried out by abusive governments, leaking information of pedophiles, attacks against businesses that are known for environmental abuses. Evidently, there is much diversity in ethical reasoning and hacking methods that fall under the umbrella of 'hacktivism', thus this chapter will elaborate in detail whether there could be an ethical framework that would justify illegal hacking based on the goals it pursues.

Are White Hat Hackers Always Ethical?

At first glance it seems easy to address ethical questions connected to hacking. When

discussing black hat hackers, they would always be deemed unethical. In essence they harm innocent individuals for personal gain, they cause financial and emotional strain, and they may even threaten the fundamental structures of our societies. On the other hand, white hat hackers could always be justified, they are seeking to help the individuals whose securities they check and abide by all legal requirements.

This would be a very narrow-minded view on such questions. Jaquet-Chiffelle and Loi discuss an interesting hypothetical case where a white hat hacker, who was hired to check the security systems of a company, finds information connected to unethical practices of the company [27]. The question is whether this hacker should share these findings with the authorities or other relevant third parties. One argument against sharing is that this would ruin the trust between companies and hackers, which in the long run will make them less likely to commission security checks and would lower their level of overall protection [27]. Another argument is that in some jurisdiction sharing such findings may even be a breach of the legal regulations that protects company secrets [27]. Still, this does not answer the ethical dilemma of a hacker keeping information that exposes grave violations of the company.

Furthermore, another ethical issue is the mere existence of such a category of hackers. It is important to note that these classifications are neither static, nor are they linked to the individual, but to their actions [3, 27, 36]. That is to say that a hacker can carry out business as a white hat hacker, but also at some point carry out illegal intrusions for personal gain. The danger then lies in all the information and skills they have acquired working for corporations and learning their security methods and secrets. Another consideration is linked to white hat hackers that work for many companies based on freelancing. There may be a risk that one of these individuals who worked for one company also gets into contact with a competing company and shares critical information for monetary gain.

Such and similar concerns cause some scholars to question the mere practice of teaching technology students how to hack, since in essence this gives them the ability to later on cause a wide range of issues and harms [21]. In our view, the current developments in the field of cybersecurity have reached a point of no return. Amateur hackers are spending their time engrossed in a multitude of online resources that teach them newer and newer ways to find exploits and carry out intrusions. Botnet systems are automizing different processes of online abuse and leading to unimaginable levels of harm. For example, a ransomware attack against Colonial Pipeline led to widespread gasoline shortages in a number of states in the USA, and in the end the company was forced to pay $4.4 million dollars in bitcoin to the hacker group to stop further damages [48]. While the US government managed to return some of the money, this is one instance from a large pool of similar crimes that becoming widespread in today's digital age. Another similar example is the attack against Keseya, a company that manages IT infrastructure for several firms and enterprises. This attack influences a number of their clients, businesses such as the Swedish supermarket Coop had to temporarily close 800 of their shops due to the attack, which would have led to large financial loses [38]. Even governments are finding zero-day exploits and are not notifying system holders in order to be able to exploit them later on if needed as part of investigations [32].

In such circumstances, no matter the moral considerations, our only option is to invest even more in cultivating experts that can carry out intrusions against malicious systems

and that can check our own systems for any weakness. We need to put our resources into educating professionals and promoting a strong moral code and work ethic in order to ensure they do not decide to engage in illegal and unethical activities. In the end, we must also accept that there will also be questionable instances when discussing hacking and cyber intrusions. Sometimes a hacker may stumble upon information they were not supposed to find or in order to ensure there are no weaknesses in a system they may have to resort to some technical methods that breach to some extent the privacy of certain users. Then we must accept that the course of action is left to that individual and their discretion. As the judge who may be put in a position to balance two conflicting interests or to find an answer to an ethical conflict, the white hat hacker must decide their course of action and carry the professional consequences if that decision proves to be unsound. Still, their actions should not be discussed through the lenses of right and wrong. The people that hired the hacker have already consented to the actions and decisions carried out by that individual.

Can Hacktivism Be Justified?

Another important ethical issue concerns the existence of so-called 'hacktivists'. These individuals carry out illegal cyber intrusions in the alleged pursuit of an ideological goal and/or the protection of ethical values such as free speech, equality, etc. A proposed definition of the types of attacks they carry out would regards instances where '*the hack is used in relation to some political or social agenda carried out by private individuals for their own political ends, often with this political element acting as a central justification for the hack*'[4]. This raises several ethical dilemmas.

Firstly, some argue that instances of hacktivist are of a non-violent nature. Delmas discusses them precisely as a means of civil disobedience [13]. Some prominent online hacktivists even link their actions to the core values of the Internet [28]. Such descriptions would place such activities within the grounds of civil protests and would make them justified [13].

However, it must be noted that often hacktivism can be linked to harms and damages [4]. These damages can be of a diverse character: financial, physical, reputational, etc. Bellaby raises the concern that hackers lack the moral authority to engage in political violence [4]. It has been argued that only the state has the authority to engage in political violence, based on political theories such as the 'Social Contract Theory' [4]. Individuals have renounced authority to the state to protect their rights and interests and have given up their rights to seek out justice on their own. Under this framework, the actions carried out by hacktivists are not ethically sound.

Still, it must be noted, that in certain cases where the state has not carried out its obligations accordingly, individuals can then resort to actions on their own. Bellaby however narrows them to cases of state negligence, which would concern potential harms to individuals due to the state's continuous inaction or misconduct [4]. For example, a singular misstep taken by the state, would not justify counteractions by vigilantes. However, cases of largescale state abuse can lead to a justified response by a hacktivist group.

For example, this precisely concerns operations of the hacktivist group Anonymous, such as Operation Tunisia and Operation Egypt, where hackers broke into the security systems of governmental organizations in order to help protesters and to aid dissidents

from online censorship [46]. In this case not only the state did not protect its citizens, but it also actively infringed their rights and interests. Thus, seemingly the actions of the hacktivists while illegal, were morally justifiable.

During the coronavirus pandemic, Anonymous also shared information about COVID-19 cases in Nicaragua, which the government was hiding. This again would fall under measures taken due to the government's inaction or ill-intent [50]. Another similar example raised by Bellaby are the attacks carried out by Anonymous with the intent of protecting minority rights [4]. The organization executed a number of intrusions against the Ugandan government in order to stop a bill that would have harmed the rights of members of the LGBT+ community [49].

Such cases are on one hand controversial, since they in fact seek to impose a certain political view through coercive measures. In this instance, the actions of the group were in clash with the cultural understandings of the state in question, still they can be justified since they were in the pursuit of the basic human rights of the minority in question. We would argue that such examples of hacktivism always seek to strike a balance between conflicting principles and political ideologies. Some authors have recognized that sometimes these clashes can be so extreme, that a hacktivist's actions can also be justified as measures of self-defense [4]. It could be argued that Anonymous not only sought to achieve a political change in the societies they influenced, they sought to protect the basic integrity and life of the individuals that were threatened by the state.

These considerations are more difficult to justify in the case of attacks against businesses. It is generally recognized that the state is authorised to regulate and overlook business activities as well as sanction those that carry out illegal activities or otherwise harm consumers or their own employees. When the state does not in fact take action against a malicious company, some would claim that hacktivists are justified in intervening in order to protect human rights or other similar values. For example, there have been a number of attacks carried out by hackers with the aim of sabotaging corporations that harm the environment, like the taking down of the French company Areva's website, which is in the nuclear power business [4]. Attacks on businesses are more problematic. Often political activists will have their own personal or political biases [4]. While state actions will include thorough investigations and numerous levels of checks and balances before retributive actions are carried out against companies and enterprises, hackers can carry out attacks based on their own personal opinions about a certain company and its perceived misconduct. Furthermore, the attacks carried out by hackers may lead to much collateral damage, the financial and material damages to corporations will not only harm the corporate itself, but may also influence its employees, many of whom might not even be aware, let alone complicit, in the actions of the company that lead to the attacks.

Thus, when discussing political hacktivism, it should be noted that any conclusions on the moral character of such actions will be very case specific and will call for a very detailed analysis of the proportionality of such actions and their intent.

2.3 New Risks in Developing Fields – IoT and Cloud Computing

A key characteristic of cybersecurity is that it is ever-developing. With the emergence of new technologies, new ethical questions arise as well. This chapter will focus on two

emerging technologies that may pose cybersecurity risks and some interesting ethical questions.

Internet of Things

Internet of Things (IoT) would refer to the rise of devices that are linked to the Internet and are able to communicate, send and receive data and help individuals in their everyday life [1]. The IoT is said to lead to a revolution in our physical relationship with our devices [1, 23]. But as revolutionary as these devices are, there are a wide range of ethical issues that these technologies create.

Privacy and Consent

The issue with IoT devices is that often users might not know what kind of information their devices collect. For example Allof discusses how a sex toy collected a wide range of information about its user: vibration settings, dates and times the device was used, email addresses of users [1, 42]. This anecdote while humorous, should cause great concern. Currently, we have become accustomed to the idea that the Internet has created an enormous market for our data and personal information. Still, it is frightening how this breach of our private life can reach such intimate spheres of our life as those discussed above.

The rise of IoT devices is driving these processes forward. As more and more everyday devices are being linked to the cybersphere and are starting to collect data, carry out different services, etc., we will have to be as aware as possible about what we give our consent to prior to using a device. From smart watches, smart kitchen appliance, even smart water bottles to digitalized personal assistants, the risks are never ending. For example, smart watches that track our fitness routines could give away precise information of our daily routine or whereabouts [1]. The use of smart kitchen appliance could give away information when we are in our home and when we are absent, which in turn may create a security risk [1]. In such circumstances it is extremely important for individuals to be able to decide what information to give to devices and what not to share.

This raises the question of informed consent. If an individual is given full information about what the device collects and how it will use the information, and if individual gives their informed consent, then many of the ethical issues can be dealt with. It is important to highlight that the informed consent should cover the requirements under Article 4 of the GDPR, namely that consent should be freely given, specific, informed and unambiguous. Moreover, the data controller must be able to demonstrate that consent is given at any time during the processing and to give the possibility for the data subject to withdraw it. Consent is an integral part of the data subjects' right to be informed and its violation leads to non-compliance with data protection law, but it is also an ethical issue. Apart from that there are also some other considerations that needs to be taken care of:

- Firstly, an ethical dilemma is whether we can expect users who lack technological knowledge to be able to make sound decisions when facing complex issues such as data processing, collection, storage and potential risks [1].
- Secondly, it has been pointed out by many experts that often the Terms and Conditions of companies and devices are very technical in character or prolonged in order to

disincentivize users who are traying to familiarize themselves with them [1]. This is an infringement of the right of the data subject to be informed under which any information provided to the data subject must be easily accessible, understandable and provided in clear and plain language [43]. In the end many users just look over these documents and give their consent just to access the service or use the device to its full capacity.

- Third, some device/service providers may even link the use to accepting all of the applicable Terms and Conditions [1]. Maybe some of us have faced this when trying to access a certain website. It could have even been a reason we decided to switch to another website where we could gain similar content but with less privacy breaches. Thus, we could be tempted to overlook all of these considerations. If someone does not want their smart bracelet to collect private information on their location, they can go running with a normal chronometer. But one must analyze these issues with a look towards the future.

In the near future, where IoT would have become an omnipresent part of our daily lives, we might not have the luxury to refuse their use. Furthermore, the use of such devices may no longer be just an individualistic decision, they may become integrated in the systems we use, in our healthcare, education, government [10]. Thus, now in the beginning of their implementation we must make sure that all privacy concerns are thoroughly dealt with. Such devices must not become a "Pandora's box", filled with sensitive information we do not even know we shared.

Security

Another issue is linked to the safety of users [1, 44, 53]. IoT is beginning to reach all spheres of our lives. At the same time, the risks of malfunction or malicious cyber intrusions are rising. The fact that smart devices are linked to networks and are programmable raises many concerns that they can easily be compromised.

There are already many well-known cases of security failures of smart devices. There have been numerous cases of baby monitors being hacked by criminals who use it to spy on infant children [41] or of IoT children's dolls also serving as surveillance devices [22], there is a plethora of other household devices that also were discovered to pose surveillance weaknesses [39]. All of these cases pose a large threat to individuals, they can cause emotional damage or even expose sensitive data to malicious individuals that can then use it for their own benefit. Imagine a criminal knowing when your child is left alone at home based on the surveillance data they have access to. Or imagine your family was one of the victims of the hacked Cayla doll[1]. Trough the doll, criminals would be able to communicate with your child, manipulate it into sharing data or even make it open a door or window they can later use to infiltrate your house when you least expect it.

[1] This toy was able to connect to Bluetooth networks, communicate with families, ask questions, collect data, share that data with a voice recognition company in the USA. More on this can be found in: Erickson A.: This pretty blond doll could be spying on your family, https://www.washingtonpost.com/news/worldviews/wp/2017/02/23/this-pretty-blond-doll-could-be-spying-on-your-family, Accessed 2022/02/03;

What is even more frightening is that some security threats pose direct and unmanageable threats. If a security breach in the form of data leakage can be managed by changing passwords or limiting the amount of data a device can collect and share, some threats cannot be mitigated and must completely be eliminated. For example, some IoT health devices such as implantable cardiac devices can be hacked and stopped or used to administrate irregular pacing or shocks [31].

Such cases are extremely troubling as they pose even life-threatening risks to consumer. They also would have detrimental effects on public trust and may have dire financial and reputational consequences for businesses and developers. A survey by Internet Society shows that 75% of consumers do not trust the way their data is shared and 28% of users that do not own a smart device would not buy one due to security risks [25].

It is an ethical question who should bear the responsibility of ensuring there are enough countermeasures to guarantee user security. The survey of Internet Society also discovered that 88% of consumers believe security standards should be assured by regulators, 81% trust manufacturers and 80% retailers [25]. These positions cause several points of conflict. On one hand, governments and state regulators often are left behind when it comes to emerging technologies and cannot keep up with the newest risks and tendencies in cybersecurity. On the other hand, retailers do not in fact have a direct say on the designs of devices and the safety precautions that can be installed in them. This would call for a level of self-regulation by manufacturers. Some may argue that expecting manufacturers to ensure security standards on their own discretion would not be effective as this would be in conflict with their business interests.

As discussed by many, businesses have as a main priority profit and growth. If a new product is set to launch and has already promised large gains for the company, there may be pressure to overlook any potential security threats that have emerged last minute. However, it must be noted that businesses recognize how important security is to users and cannot afford to compromise their reputation. Thus, we would argue that businesses themselves in fact have taken the burden of ensuring consumer safety, even if bases on profit incentives. Regulators must then work in cooperation with them to ensure threats are avoided or mitigated.

Cloud Computing

Cloud computing systems can be defined as "*software-related activities performed by users thanks to pools of computing resources, which are accessible through a network, where they are made available by some providers*" [47]. Many of us have used such services when working with products such as Google Drive, Microsoft Share Point, Dropbox, Gmail, Facebook. Broadly cloud computing can be classified under the following types [35]:

- Infrastructure as a service (IaaS) – cloud service providers supply consumers with basic computer resources such as storage, servers, etc.
- Platform as a service (PaaS) – cloud service providers supply consumers with platforms they can use to create and deliver their own applications.
- Software as a service (SaaS) – cloud service providers build, host and supply application to consumers.

This emerging technology also poses many ethical questions and considerations.

Ownership of Data

One of the important questions is whether when using a cloud service, the users can retain ownership of their data and products. Here there is a multitude of issues. Firstly, some cloud services not only store data, they are used by users to create the data itself. This raises questions whether this data can be claimed by the cloud service provider. Secondly, the data retained by a certain cloud service may be created or uploaded from one location, but fall within a different jurisdiction based on the location of the services [45]. This conflict of jurisdictions is even more confusing, due to the fact that there is no set standard that can be established [12]. Questions of ownership are often dealt with in the terms and conditions of the cloud service providers [12]. For example, major cloud service providers, such as Office 365, Amazon Web Service and Google have similar positions on ownership and reserve all rights over the data and content stored for the users [8].

These are important considerations since they would later influence the consequences of a data breach or how information can be stored and shared. In order to ensure that users have a wide range of rights in regard to their data, as well as the ability to make decisions how it is stored and shared, they must retain ownership over it. Scholars have discussed the phenomenon of younger generation becoming less concerned over the question of data ownership [11]. De Bruin and Floridi focus on the way public perception has shifted 'from the product to the services the product represents' [11]. For example, they describe how contemporary users will focus less on who owns a certain photograph when it is uploaded and more on where they can share the photograph, whether they can edit it and other similar service based assessments [11].

Here a counterbalance would be again ensuring users are well informed of the importance of data protection and privacy as well as what consequences the decisions they make could have. De Bruin and Floridi argue against a strong regulatory role of the state and propose an approach dubbed interlucency, where consumers can make decisions after being thoroughly informed by providers [11]. This information should be effectively communicated, aimed at the particular individual and the provider must ensure the user genuinely was able to grasp the information that was shared with him.

We would also consider such an approach extremely fruitful, but one should not completely disregard the importance of government regulation as well. Through the ethical lens, the state as established was given the authority to regulate such important questions in order to protect the safety of its citizens. In this regard, the EU has taken large steps in regulating cloud services in the extent needed to protect EU citizens and their rights.[2]

Security Risks

The potential intrusions from third parties constitute the larger risk when it comes to cloud computing. This risk has some unique dimensions when it comes to cloud computing. Imagine you and your colleagues store vital information in a cloud service. One of your

[2] The European institutions and bodies have published an extensive guide: European Data Protection Supervisor, Guidelines on the use of cloud computing services, https://edps.europa.eu/sites/edp/files/publication/18-03-16_cloud_computing_guidelines_en.pdf Accessed 2022/02/08;

colleagues compromises the security of that cloud environment. All of you now will face the potential consequences of such a development. Or maybe, the centralized server of that cloud provider was hacked, and this puts you in danger along with a multitude of other users.

Still, traditional mechanisms of protection could be implemented: security checks, encryption, etc. In this sense, there may be a heightened risk of intrusions, but these can be thoroughly mitigated. At the same time, many authors have pointed out the benefits cloud services provide. Users are able to save large financial investments that would have otherwise been used for machines, storage space, maintenance, etc. For this they gain a cheaper, easily accessible product maintained and protected by a third party with more expertise in cybersecurity in the face of a cloud service provider. Thus, when balancing the ethical considerations of user security and the practical implications of a convenient service such as cloud computing, it is understandable why users would accept any potential but small harms that this new technology may bring.

2.4 Risks While Testing New Technology

Another ethical concern is how to proceed with the testing of future products. Ethical testing is nothing new, our society has faced a multitude of ethical issues when testing for example pharmaceutical products or cosmetics. A central issue in all such ethical debates is the potential risks the test subjects are exposed to [29]. Here the main argument to justify this is the consent given by the participants as well as the overarching societal interest in such testing activities. Participants often have altruistic reasons for joining test studies, but they also gain financial stimulus to award their participation or even compensate any shortcomings.

These justifications can be carried on to the field of new technology testing. However, there are also some unique considerations. Firstly, when discussing new technologies there are unforeseen risks that might not be anticipated by the experts. Unforeseen risk may be applicable to all new products, even one should expect such, but specifically in the field of technology these risks could not only be unexpected, they may be of a character that has not yet been dealt with. For example, scientists still do not know for sure how certain Bluetooth earphones and their waves can influence the brain of their users [2]. On one hand, such concerns are for what it seems unfounded with no real evidence for harm. On the other hand, if they prove to be rightfully placed, they may cause harms that we are not yet sure how to proceed with.

Secondly, another issue that can be raised is that in some instances participant consent is not always clearly given. For example, Uber is testing its self-driving cars in real life environments within urban populated areas such as San Francisco, Phoenix, Pittsburgh [34]. While the direct participants in the testing have consented to take part, all pedestrians in the testing areas have not. This is worrying, especially when one considers that such testing has already led to a casualty [33]. Defenders argue that if implemented such technologies will substantially lower casualties caused by human error. Still, this does not justify the risks bystanders are exposed to when in proximity to a product that is yet to finish all safety tests.

3 Required Measures to Ensure Ethical Compliance

In view of the above-mentioned risks and liabilities to the overall compliance with ethical principles, certain actions need to be taken in order to ensure full compliance. The measures that could be taken vary from simple organisational activities to the introduction of special technologies that ensure the protection of specific rights and freedoms of the persons concerned. In order to establish which measures should be taken, particularly with regard to new technological systems that should be integrated, appropriate conformity and impact assessments should be carried out. The best that can be done is before any new technology is developed to create a list of requirements that could be taken with regards the actual development. Such approach was taken in framework of the GUARD project funded by the European Commission's Horizon 2020 programme, under which a set of requirements (functional, design, performance, ethical, data protection and etc.) were established to be followed during the development of the platform under the project.

3.1 Implementing Organisational Measures to Ensure Ethical Compliance

Envisaging and implementing organisational measures is the base minimum for ensuring compliance with the fundamental ethical principles. What measures should be included is decided on case-by-case basis and should be pointed out that more than one measure could require to be implemented in order to reach ethical compliance. Another important thing that should be considered is that in most cases the sole implementation of organisational measures is not sufficient, and additional technical measures must be included. This depends on the variety and severity of cybersecurity risks that could occur, while the definition of the exact measures should be taken after a proper assessment of the risks, that could affect the individuals is concluded.

The measures that could be implemented are the following: 1) internal trainings for staff members and technical developers on fundamental ethics, 2) preparation of ethical codes of conduct for staff members and technical developers, 3) conducting follow-up audits to assess the level of compliance with the core ethical principles, 4) adoption of incidental findings policy that will indicate how to handle any unforeseen information, 5) introduction of ethical personnel, which goal is to advice and oversee how ethical standards should be properly implemented.

One measure that could be implemented continuously and indefinitely is the establishment of procedures for periodic monitoring of the compliance with the fundamental ethical principles. It should be noted that monitoring procedures should not be applied to every system. Before such measure is adopted an assessment of the nature of the system, its purpose and what impact it has on individuals should be conducted. For example, a system that stores and processes data that is publicly available should not be subject to a detailed monitoring procedure, unlike a similar system that processes personal data. Once this has been determined, it should be decided over what period the monitoring activities will take place [9]. As has been mentioned many times, a judgement should also be made here with regard to the nature of the system to be monitored in order the monitoring period to be determined. After all, continuous monitoring is too time and resource consuming, leading to additional difficulties.

Each of the above measures is relevant to achieving ethical compliance. Whichever, of the above measures is adopted, they should be strictly adhered to in order to avoid any loss and to prevent any damage to those implementing them. The improper implementation of the measures would impede the fulfilment of their objectives and could lead to harm to the individuals.

3.2 Carrying Out an Impact Assessment

An assessment of the impact on the rights and freedoms of citizens and the persons concerned is an appropriate measure to take in order to minimize any risks and ensure ethical compliance. Such assessment is envisaged both by the Council of Europe and EU regulations. Specifically, EU law under Article 35 of the GDPR envisages that a data protection impact assessment should be carried out when the nature of the processing is likely to result in high risk to the rights and freedoms of natural persons. This requirement is envisaged to be carried out by the data controller[3] and could also cover an assessment on the impact of fundamental rights and freedoms explicitly stated in international legislative acts such as the European Convention of Human Rights (ECHR)[4]. The main implication of the results of the impact assessment is to ensure accountability and compliance with relevant legislation and ethical principles.

GDPR does not define how the likelihood of a risk is to be assessed but it indicates what those risks might be[5]. The impact assessment should identify appropriate measures to address these risks. Where an impact assessment is required, data controllers must assess the necessity and proportionality of the processing and the possible risks of the individuals.

The Article 29 Working Party have developed guidelines under which there is criteria to determine whether or not an impact assessment is required for the specific processing activities. The criteria includes: 1) evaluation or scoring; 2) automated decision-making with legal or similar significant effect; 3) systematic monitoring, 4) sensitive data; 5) data processing on a large scale; 6) datasets that have been matched or combined; 7) data concerning vulnerable data subjects; 8) innovative use or applying technological or organisational solutions; when the processing in itself "prevents data subjects from exercising a right or using a service or a contract [18]".

Under the GDPR, there is no specific guidance on how an impact assessment should be carried out, but there are various methodologies that provide guidance on how should be proceeded with such assessment. An example of such methodology is the Standard Data Protection Model (SDM)[6], which is explicitly recommended by the Article 29 Working Party Guidelines on Data Protection Impact Assessment, and embraces the legal requirements set by the GDPR. This methodology was used in the preparation of the Data Protection Impact Assessment under the GUARD project and with its help the legal

[3] Article 35, paragraph 1, General Data Protection Regulation;

[4] Singed 4 November 1950, Effective from 3 September 1953;

[5] Recital 75, General Data Protection Regulation;

[6] This can be found at: SDM Methodology, https://www.datenschutzzentrum.de/uploads/sdm/SDMMethodology_V1.0.pdf. Accessed 2022/02/02.

requirements envisaged under the EU Data Protection Regulation were transformed into proper technical and organisational measures which will minimize any possible risks.

The methodology introduces the concept of "Data Protection Goals". It defines this term to describe certain categories of requirements derived from data protection law. It is through them that the transformation from legislative requirements into technical and organisational measures takes place. The term is also referred in the case law of the German Constitutional Court (Judgement of 27 February 2008 – 1 BvR 370/07, 1 BvR 595/07, Official Record of Decisions [BVerfGE] 120, 274). In this decision, the court pointed out that the individuals should be protected when their personal data is processed by modern technological solutions from unlimited collection, storage, usage, transfer and misuse ensuring compliance with fundamental data protection goals such as data minimization, confidentiality, integrity etc.

3.3 Adopting Privacy Enhancing Technologies

Privacy Enhancing Technologies (PETs) are technological measures that aim at protecting personal identity. These measures usually are involving different levels of encryption such as blind signatures, digital signatures, pseudonyms etc. [6]. They are effective measures to ensure privacy by design and could minimize the amount of data processed to help protect any personal information. PETs have to be distinguished from the rest of the data-security technologies. The difference is that data security is about ensuring the security of the processing activities regardless their legitimacy. On the other hand – PETs are seeking to restrict the usage of personal data or to give control of the revelation of personal data to the concerned individuals [6]. PETs are strongly related to big data, which includes the usage of a huge volume, variety and real-time data (from physical sensors, social media etc.). This leads to a very high plausibility that big data may contain personal identifiers and to an extensive variety of issues concerning data privacy such as lack of control and transparency, reusability of the data, re-identification and data inference, profiling and automated decision making [17]. Although the usage of big data is crucial for the economic and technical development, enterprises should be cautious since the risk of misuse is high making the achievement of privacy by design the best possible way to ensure compliance with the GDPR.

One of the ways in which privacy by design could be ensured is exactly with the help of PETs. Again, it should be evaluated which PETs should be implemented on a case-by-case analysis. The correct choice of technology will depend on different factors, including the type of data that it is used, volume of the data, the source, the purpose of the processing etc.

In summary there are many positive aspects to the use of PETs which could help protect data subjects from a wide range of ethical risks. The discussions related to the use of PETs will continue to evolve and be directly linked to the use of new technologies that could have negative effect to data subjects. In relation to that is important when using or designing privacy-preserving systems to follow the proper ethically informed methodologies when using or developing such systems in order to identify and mitigate any possible risks.

4 Conclusions

This article presents some of the ethical risks and issues that could occur in the field of cybersecurity, and it was based to some extend on the findings under the EU funded project GUARD. It also represents some of the measures dedicated to protecting the privacy of data subjects that were implemented during the project's lifetime regarding the technology developed within it. What can serve as a basic recommendation, especially when developing new technologies is to establish a list of requirements, including ethical ones that the system must cover before any action is taken. This will ensure compliance with the ethical principles at highest level and mitigate any negative effect on the individuals.

Regarding the ethical risks that may occur, one must be aware that they are of varying intensity and may affect different human rights and freedoms and different areas of our lives. The fields that pose many ethical issues and were thoroughly discussed include hacking and cyber intrusions, both authorized and unauthorized, risk in newer technologies such as IoT devices and cloud computing, among others. All these areas have some issues in common such privacy concerns, harms to businesses, etc., but each area proved to have its own specific issues. It is highly important to be aware of the risk that may occur in order to implement proper measures that will minimize any harmful effect to the individuals. This requires proper understanding of the issues and additional input from experts in the field.

In conclusion, we could summarize that the issues regarding ethical problems in the field of cybersecurity are complex and require a robust approach. Each emerging risk must be assessed in order to determine the negative effect it will have on the individual. Such an assessment would then make it possible to choose an appropriate response. Stakeholders taking the measures should be flexible and combine diverse measures in order to achieve better results and envisage the participation of ethical experts all together with technical developers and cybersecurity experts. Their combined work will be the best way to ensure ethical compliance and that no harm will be caused to individual.

References

1. Allhoff, F., Henschke, A.: The Internet of Things: foundational ethical issues. Internet of Things **1–2**, 55–66 (2018)
2. Are Bluetooth Headphones Dangerous? Here's What Experts Think, Healthline. https://www.healthline.com/health-news/are-wireless-headphones-dangerous. Accessed 16 Jan 2022
3. Barber, R.: Hackers pro-filed—who are they and what are their motivations? Comput. Fraud Secur. **2001**(2), 14–17 (2001)
4. Bellaby, R.W.: An ethical framework for hacking operations. Ethical Theory Moral Pract. **24**(1), 231–255 (2021). https://doi.org/10.1007/s10677-021-10166-8
5. Bishop, L.: Big data and data sharing: ethical issues. UK Data Service, UK Data Archive (2017)
6. Burker, H.: Privacy-enhancing technologies: typology, critique, vision. In: Agre, P.E., Rotenberg, M. (eds.) Technol. Privacy New Landscape, pp. 125–142. MIT Press, London (1997)
7. Cekerevac, Z., Zdenek, D., Prigoda, L., Cekerevac, P.: Hacking, protection and the consequences of hacking. Komunikacie **20**(2), 83–87 (2018)

8. Chima, R.: Cloud Security – Who Owns The Data? Blueberry Consultants. https://www.bbconsult.co.uk/blog/cloud-security-who-owns-the-data. Accessed 3 Mar 2022
9. Cybersecurity ethical obligations. https://resources.infosecinstitute.com/topic/cybersecurity-ethical-obligation/. Accessed 4 Feb 2022
10. Dahlqvist, F., Patel, M., Rajko, A., Shulman, J.: Growing opportunities in the Internet of Things, growing opportunities in the Internet of Things. https://www.mckinsey.com/industries/private-equity-and-principal-investors/our-insights/growing-opportunities-in-the-internet-of-things. Accessed 8 Feb 2022
11. De Bruin, B., Floridi, L.: The ethics of cloud computing. Sci. Eng. Ethics **23**(1), 21–39 (2016). https://doi.org/10.1007/s11948-016-9759-0
12. Delgado, R.: The ongoing question of data ownership in the cloud, socPub. https://socpub.com/articles/the-ongoing-question-of-data-ownership-in-the-cloud-13749. Accessed 3 Feb 2022
13. Delmas, C.: Is Hacktivism the new civil disobedience? Raisons Politiques **69**(1), 63–81 (2018)
14. Durant, A.: The Enemy Within. Business XL, pp. 48–51 (2007)
15. Erickson, A.: This pretty blond doll could be spying on your family. https://www.washingtonpost.com/news/worldviews/wp/2017/02/23/this-pretty-blond-doll-could-be-spying-on-your-family/. Accessed 3 Feb 2022
16. Ertem, A.: Sensitive Data and Receiving Consent according to GDPR. https://blog.scrintal.com/sensitive-data-and-receiving-consent-according-to-gdpr-a31c9ee8ea28. Accessed 8 Feb 2022
17. European Union Agency for Cybersecurity: Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics (2015)
18. European Union Agency for Fundamental Rights and Council of Europe. In: Handbook on European Data Protection Law, 2018 edn. Publications Office of the European Union, Luxembourg (2018)
19. Favaretto, M., De Clercq, E., Elger, B.S.: Big data and discrimination: perils, promises and solutions a systematic review. J Big Data **6**, 12 (2019)
20. Floridi, L.: On human dignity as a foundation for the right to privacy. Philos. Technol. **29**(4), 307–312 (2016). https://doi.org/10.1007/s13347-016-0220-8
21. Hartley, R.D.: Ethical Hacking: Teaching Students to Hack, East-Carolina University. https://doi.org/10.13140/RG.2.1.3580.8085. Accessed 16 Jan 2022
22. Hautala, L.: Smart toy flaws make hacking kids' info child's play. https://www.cnet.com/home/smart-home/cloudpets-iot-smart-toy-flaws-hacking-kids-info-children-cybersecurity/. Accessed 3 Feb 2022
23. Henschke, A.: The Internet of Things and dual layers of ethical concern. In: Lin, P., Abney, K., Jenkins, R. (eds.) Robot Ethics 2.0, pp. 229–243. Oxford University Press, New York (2017)
24. How GDPR Stops Discrimination and Protects Equalities. https://www.openrightsgroup.org/how-gdpr-stops-discrimination-and-protects-equalities/. Accessed 8 Feb 2022
25. Internet Society: The Trust Opportunity: Exploring Consumer Attitudes to the Internet of Things. https://www.internetsociety.org/resources/doc/2019/trust-opportunity-exploring-consumer-attitudes-to-iot/. Accessed 3 Feb 2022
26. Ivanov, I..: What is a Black Hat Hacker? Techjury. https://techjury.net/blog/what-is-a-black-hat-hacker. Accessed 11 Jan 20222
27. Jaquet-Chiffelle, D.-O., Loi, M.: Ethical and unethical hacking. In: Christen, M., Gordijn, B., Loi, M. (eds.) The Ethics of Cybersecurity. TILELT, vol. 21, pp. 179–204. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-29053-5_9
28. Johnson, B., Stephens, D.: Is 'hacktivism' a force for good … or chaos?, Marketplace. https://www.marketplace.org/2017/04/28/hacktivism-force-good-or-chaos/. Accessed 2 Feb 2022

29. Kapp, M.: Ethical and legal issues in research involving human subjects: do you want a piece of me? J. Clin. Pathol. **59**(4), 335–339 (2006)
30. Kumar, S., Agarwal, D.: Hacking attacks, methods, techniques and their protection measures. Int. J. Adv. Res. Comput. Sci. Manag. **4**(4), 2353–2358 (2018)
31. Larson, S.: FDA confirms that St. Jude's cardiac devices can be hacked, CNN. https://money.cnn.com/2017/01/09/technology/fda-st-jude-cardiac-hack/. Accessed 3 Feb 2022
32. Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, Study for the LIBE Committee, 6 April 2017
33. Levin, S., Wong, J.: Self-driving Uber kills Arizona woman in first fatal crash involving pedestrian. https://www.theguardian.com/technology/2018/mar/19/uber-self-driving-car-kills-woman-arizona-tempe. Accessed 6 Jan 2022
34. Marshall, A.: The lose-lose ethics of testing self-driving cars in public, Wired. https://www.wired.com/story/lose-lose-ethics-self-driving-public/. Accessed 16 Jan 2022
35. Maurer, T., Hinck, G.: What Is the Cloud? In: Cloud Security: A Primer for Policymakers, Carnegie Endowment for International Peace (2020)
36. Milin-Ashmore, J.: What Is Ethical Hacking and Why Is It Important? https://ethical.net/ethical/what-is-ethical-hacking. Accessed 5 Jan 2022
37. O'Leary, A.: Horrified mum hears chilling man's voice on hacked baby monitor saying child is 'cute', Mirror. https://www.mirror.co.uk/news/world-news/horrified-mum-hears-chilling-mans-24959669. Accessed 3 Feb 2022
38. Osborne, C.: Updated Kaseya ransomware attack FAQ: What we know now, ZDNet. https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/. Accessed 2 Feb 2022
39. Palmer, D.: 175,000 IoT cameras can be remotely hacked thanks to flaw, says security re- searcher, ZDNet. https://www.zdnet.com/article/175000-iot-cameras-can-be-remotely-hacked-thanks-to-flaw-says-security-researcher/. Accessed 3 Feb 2022
40. Privacy and Information Technology. Stanford Encyclopedia of Philosophy (2019). https://plato.stanford.edu/entries/it-privacy/. Accessed 4 Feb 2022
41. Pyman T.:'Creepy hacker used baby monitor to SPY on my son': Parents fear restless 15 month-old boy was being woken by 'local man' accessing cot camera after hearing 'deep male voice' at 2.30 am, Mailonline. https://www.dailymail.co.uk/news/article-10287527/Parents-fear-creepy-hacker-used-baby-monitor-spy-son.html. Accessed 3 Feb 2022
42. Redden, M.: Tech company accused of collecting details of how customers use sex toys. The Guardian. https://www.theguardian.com/us-news/2016/sep/14/wevibe-sex-toy-data-collection-chicago-lawsuit. Accessed 16 Jan 2022
43. Right to be informed. https://www.dataprotection.ie/en/individuals/know-your-rights/right-be-informed-transparency-article-13-14-gdpr. Accessed 31 Jan 2022
44. Roberts, P.: Pretty much all consumer internet of things vulnerabilities are avoidable. The Security Ledger. https://securityledger.com/2016/09/pretty-much-all-consumer-internet-of-things-vulnerabilities-are-avoidable/. Accessed 16 Jan 2022
45. Rocchi, M., Murphy, B.: Ethics and cloud computing, data privacy and trust. In: Cloud Computing, pp. 105–128. Palgrave Macmillan, Cham (2020)
46. Ryan, Y.: Anonymousand the Arab uprisings, Al Jazeera. https://www.aljazeera.com/news/2011/5/19/anonymous-and-the-arab-uprisings. Accessed 02 Feb 2022
47. Turilli, M., Floridi, L.: Cloud computing and its ethical challenges. https://dx.doi.org/10.2139/ssrn.3850031. Accessed 24 Feb 2022
48. Turton, W., Mehrotra, K.: Hackers breached colonial pipeline using compromised password, Bloomberg. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password. Accessed 2 Feb 2022

49. Uganda Government websites hacked by anonymous in defense of gay pride: LGBT Rights, Huffpost. https://www.huffpost.com/entry/uganda-government-websites-hacked-anonymous-gay-rights_n_1789623. Accessed 2 Feb 2022
50. Vida, M.: Anonymous group hack reveals hidden government data about COVID-19 cases in Nicaragua. https://globalvoices.org/2020/08/31/anonymous-group-hack-reveals-hidden-government-data-about-covid-19-cases-in-nicaragua/. Accessed 22 Feb 2022
51. Western Governors University: Ethical hacking and how it fits with cybersecurity. https://www.wgu.edu/blog/ethical-hacking-how-fits-with-cybersecurity1908.html#close. Accessed 4 Feb 2022
52. White, T., Gutierrez, B.: Protest or Criminal Activities?. The Ethics of Hacktivism. https://tawhite88.wordpress.com/2014/03/24/protest-or-criminal-activities-the-ethics-of-hacktivism/. Accessed 24 Feb 2022
53. Yoo, C.: Centre for international governance, the emerging internet of things: opportunities and challenges for privacy and security. In: Governing Cyberspace During a Crisis in Trust: An Essay Series on the Economic Potential — and Vulnerability — of Transformative Technologies and Cyber Security, Center for International Governance (2019)
54. Zarley, B.: 'White hat hackers are defending hospitals from rising cyber attacks'. Freethink. https://www.freethink.com/technology/cyber-attacks. Accessed 22 Feb 2022