*Studia Gilsoniana* 11, no. 2 (April–June 2022): 289–323
ISSN 2300–0066 (print)
ISSN 2577–0314 (online)
DOI: 10.26385/SG.110211

**Małgorzata Gruchoła**

# Mass Culture: An Aesthetic Experience or An Experience of Fear?

## Introduction—Theoretical Decisions

The arrival of a mechanical, technology-based means of reproduction of works of art seems to have put an end to an ethereal aura of art, and aesthetic experience started to make its way into the everyday world of mass culture. Thus, in line with Richard Shusterman,[1] it cannot be applied to define high art and determine its boundaries. As Étienne Gilson put it in *La société de masse et sa culture*,[2] an endless reproduction of technical and industrial aspects of a work of art can modify not only the aesthetic experience of which it is an object, but also the culture it is embedded in. By addressing the notions of mass culture and industrialization, he makes a distinction between them, framing them as

Małgorzata Gruchoła, The John Paul Catholic University of Lublin
e-mail: malgorzata.gruchola@kul.pl • ORCID: 0000-0002-2367-0416

[1] Richard Shusterman, "O końcu i celu doświadczenia estetycznego," in *O sztuce i życiu. Od poetyki hip-hopu do filozofii somatycznej*, trans. Wojciech Małecki (Wrocław: Wydawnictwo Atla 2, 2007), 129–151.

[2] Étienne Gilson, *La Société de Masse et sa Culture* (Paris: Librairie Philosophique Vrin, 2002), 7. See: https://www.amazon.fr/Societe-Masse-Sa-Culture/dp/2711602931.

Article — Received: June 10, 2022 • Accepted: June 21, 2022

a complex relation whereby industrialization of mass culture products is merely a means of producing mass culture, becoming both its source and result.[3] Assuming that the internet is the product of mass culture and industrialization which is used to technically reproduce works of art on a massive scale, the result of which is e.g., cybercrime, I cannot disagree with the statement that the internet modifies (mass) culture. Since the industrialization of a cultural product in the form of the internet is a means of generating mass culture, questions could be raised regarding its sources and effects.

The internet is commonly defined as a global computer network. It encompasses three distinct yet complementary layers: technical, social, and informational.[4] For the purposes of this publication, I assume that the technical layer, understood as an extensive computer network made up of interconnected networks, can facilitate the phenomenon of cybercrime (e.g., the infection of devices with malicious software, hacking online social network or mail accounts, cyber-attacks, debit/credit card or online banking fraud). The social layer is defined as a collective group which makes use of the network and develops it, and may foster crime activities. Simultaneously, the results of activities are directed against internet users. The threat of cybercrime may stem from internet users' actions (identity theft, demands for payment in return for getting back control of your device, online fraud where goods purchased are not delivered, fraudulent emails or phone calls asking for your personal details), as well as from the content published by internet users (online child pornography, online materials promoting racial hatred or religious extremism). The informational layer, i.e., a collection of resources, can be both a source and a result of cybercrime.

---

[3] Jan Sochoń, "Piękno nie przekłada się na dolary. Przepowiednie estetyczne Étienne'a Gilsona," accessed June 1, 2022, https://teologiapolityczna.pl/ks-jan-sochon-spoleczenstwo-masowe-i-jego-kultura-przedmowa-1.

[4] Małgorzata Gruchoła, "W pajęczynie globalnej sieci," in *Społeczeństwo i Rodzina* 47, no. 2 (2016): 94–116.

For the purposes of this work, I assume that:

- the internet, and specifically its content and actions taken by internet users, is a source of fear of experiencing cybercrime;
- experiencing cybercrime is a result (and a threat) of using the world wide web;

Today the fear of cybercrime is not only shaped by the personal experience of EU citizens, but is generated and spread by mass culture, leading to the culture of fear. It is in this context that the aim of the paper is to conduct a comparative analysis of EU citizens' perception of cybercrime, treated as a source of experiencing fear, and the level of their personal experience of cybercrime.

The analysis will be performed on the basis of studies of the Eurobarometer carried out in all the EU member countries from 2013 to 2020 at the request of the European Commission. At the beginning of the research process, I formulated the following research questions:

- What is the perception of cybercrime as a form of experiencing fear?
- What is the level of knowledge of the risks of cybercrime activity?
- What are the factors causing fear: fear of experiencing specific cybercrimes communicated in the media discourse, or the personal experiences of EU citizens according to the Eurobarometer reports?

I have adopted the following hypotheses for the research project:

- Citizens of the European Union are more afraid of experiencing technology-based cybercrime rather than human-based crime.
- Citizens of the European Union more often admit to experiencing technology-based cybercrime than human-based crime.
- The level of fear of European Union citizens of experiencing cybercrime is higher than the level of personal experience.
- The aesthetic experience has been replaced by the experience of fear in mass culture.

In line with the philosophy of life (Henri Bergson, William James, John Dewey), aesthetic experience should become a counterbalance to the threats imposed by industrialization. Jan Sochoń observes that in mass culture, it

> became a stronghold of freedom, beauty, sense, in the world limited to materialistic-pragmatic dimensions and hopes pinned to the developments of science and technology.[5]

A question should be raised, however, as to whether in mass culture the aesthetic experience has been replaced by the experience of fear, both perceived physically and generated by new technology (the internet).

## Aesthetic experience

Étienne Gilson, a versatile scholar, was mostly known for his contributions to the fields of the history of philosophy, religion, art, literature, as one of the founding fathers of neo-scholastic Thomism. The areas of culture distinguished in Greek philosophy by Aristotle: *theoría*, *práxis* and *poiesis*, joined by *religio* in the centuries to come, occupied a special place in Gilson's life. He produced *párerga*—short texts (including opinions, journalistic texts, letters), produced radio broadcasts, and was an active member of the cultural life of his era.

Initially he focused only on issues related to promoting the ideas of existential Thomism and on defending it against its fierce critics. His own studies and those by Jacques Maritain emphasized the significance of the category of being (*esse*), so fundamental in Thomas Aquinas' metaphysics. It should be pointed out that issues related to the philoso-

[5] Sochoń, "Piękno nie przekłada się na dolary."

phy of culture from today's perspective were not of particular interest to Thomists, even though together with the studies introduced by Désiré Mercier (1851–1926), the author of neo-scholastic philosophy and the Leuven school, the issues of the object and methodology of humanistic studies attracted a scientific approach.[6] Although Thomas Aquinas did not use the term "culture" since it was not the object of his studies, he

> raised the issue of the philosophy of culture, developing ontic foundations for a relationship between an individual and reality, and in anthropology he laid the foundations of human self-improvement and artistic capability, inherent in people's nature. Other scholars continued his intellectual initiatives (M. Grabmann, B. Reiser, J. Egan, J. Maritain, Ch. Journet), including Gilson, who presented voluminous works on the topic in the 1960s both in America and in Paris. The issues of art, aesthetic experience, and the relationship between religion and literature were of interest to the abovementioned neo-Thomists, especially Maritain and de Wulf.[7]

Étienne Gilson attempted to apply the developed methods of a metaphysical view of reality to the process of explicating artistic issues. He assumed that

> in order to bring 'the existence of artistic works' closer, one needs to learn how to make distinctions between them, and to capture that which defines a given work 'a work of art.' Relying on the method of negative exclusion, he concluded that [...] 'the inside' of a work of art is revealed only in the course of action (*l'orde de la factivité*), underpinned by intellectual virtues, i.e. command of specific artistic principles and a myste-

---

[6] Étienne Gilson, *Społeczeństwo masowe i jego kultura*, trans. Agnieszka Kuryś (Warszawa: Fundacja Świętego Mikołaja, Redakcja "Teologii Politycznej," 2022), 12.

[7] Sochoń, "Piękno nie przekłada się na dolary."

rious, irrational gift of mercy [...]. One needs either to accept its elusive character or be doomed to unavoidable silence, nothingness.[8]

Étienne Gilson, in line with Thomas Aquinas, believed that a *sine qua non* for aesthetic experience is the physical presence of an object that can be experienced by means of the senses (not only through the imagination), producing in the addressees some sort of pleasure, and in its cognitive aspect, appreciation of a sensual and intellectual nature, which one wants to experience. For that to be achieved, one needs to assume a special, structural order being present in the perceived object, which can affect the sensory-cognitive human system.[9] He wanted to reach the essence of aesthetic experience, which is a specific bond between various works of art and their authors. He believed that this notion started losing popularity in the middle of the 20th century, being finally questioned since "beauty is not a characteristic of objects per se, but exists solely in the human mind of the beholder."[10] Gilson aimed to contribute to bringing aesthetic experience back to its proper value in mass culture. He referred to tradition (Plato, Aristotle, Thomas Aquinas), where it played a significant role in philosophical and religious self-awareness.[11]

Today, a tool which can help bring aesthetic experience back to its place in mass culture are information-communication technologies, including the internet. Étienne Gilson discusses various possible forms of reading and receiving works of art by readers of different epochs, mostly those belonging to popular culture. He observes that mass culture intensified the opportunities to have contact with art, music, etc., as

[8] Gilson, *Społeczeństwo masowe i jego kultura*, 13.
[9] *Ibid*., 17.
[10] *Ibid*.
[11] Sochoń, "Piękno nie przekłada się na dolary."

aesthetic experience has expanded and the conditions in which it can be experienced have been modified. Content produced by the media, according to Gilson, "offers not only music, but auditory vision, which is basically another object [...]. Musical reality and its auditory reflection are not the same."[12] An aesthetic value cannot be found in a surplus of messages. Gilson claims that

> we hear a human being in a musician, that is why we applaud them when the music stops. It would not occur to us to applaud the phonograph or the radio that resonates with the transmitting device itself with music without the musician.[13]

Hence, even when we replace a person with the greatest of machines, the aesthetic value is altered, losing its primary nature.[14]

Another threat imposed by mass culture, apart from the ever-changing conditions behind aesthetic experience, is a growing experience of fear implied by internet users' behavior and the content of published messages not necessarily of an aesthetic character. This article will offer an analysis of the fear generated by cybercrime.

## Experience of fear—cybercrime

Classical societies associated fear with a clearly formulated danger: fear of child pornography, fear of identity theft, fear of infection of devices with malicious software. Danger was defined as the object of fear; what caused problems was not a feeling of fear itself, but things feared (child

---

[12] Gilson, *Społeczeństwo masowe i jego kultura*, 21.

[13] *Ibid*., 75.

[14] Sochoń, "Piękno nie przekłada się na dolary."

pornography, theft). Nowadays, many perceive fear as a danger in itself.[15] According to Stefanie Grupp,[16] particular fears are generated by the media and are less frequently a result of direct experience.

> It is the communication of risk rather than personal experience that presently causes the greatest fear.[17]

According to George Gerbner, mass media create a worldview reflecting "repeated premises," and not based on reality.[18] Hence it can be assumed that the perception of cybercrime is not a product of personal experience but rather a result of the range of information on cybercrime perpetuated in media discourse, often being a source of fear.

There are several terms used to describe cybercrime[19] in scientific and public discourse: "computer crime," "crime connected with network systems," or "crime with the use of advanced information tech-

---

[15] Frank Furedi, *Culture of Fear: Risk Taking and the Morality of Low Expectation* (New York, London: Continuum International Publishing Group, 2002); Frank Furedi, *How Fear Works: Culture of Fear in the Twenty-first Century* (London: Bloomsbury Continuum, 2018).

[16] Stefanie Grupp, *Political Implications of a Discourse of Fear* (New York: New York University, 2003), 43.

[17] Christopher P. Guzelian, *Liability and Fear* (Stanford: Stanford Law School, 2004), 712.

[18] Cited in Valerie J. Callanan, "Media Consumption, Perceptions of Crime Risk and Fear of Crime: Examining Race/Ethnic Differences," in *Sociological Perspectives* 55, no. 2 (2012): 95, https://doi.org/10.1525/sop.2012.55.1.93; Małgorzata Gruchoła and Małgorzata Sławek-Czochra, "'The Culture of Fear' of Inhabitants of EU Countries in their Reaction to the Covid-19 Pandemic—A Study Based on the Reports of the Eurobarometer," *Safety Science* 135, article 105140 (March 2021): 1–2, https://doi.org/10.1016/j.ssci.2020.105140.

[19] Małgorzata Gruchoła and Justyna Szulich-Kałuża, "Digital Competence in Cybercrime Behaviours: A Study Based on Eurobarometer Research," in *Zeszyty Naukowe KUL* 65, no. 1 (2022), DOI: 10.31743/znkul.13610.

nologies."[20] Cybercrime is a special manifestation of cyberbullying and is aimed to subdue individuals or groups against their will by means of illegal attacks, with the use of data processing information systems operating in such a way as to achieve their goals and benefits. Both individuals and groups of people can fall victim to cybercrime.[21] According to Debra Shinder and Ed Tilttel,

> [t]he scope of cybercrime, understood as illegal acts committed by means of computer systems or networks, can be examined from the vertical and horizontal perspective.[22]

The vertical approach deals with crimes specific to cyberspace, outside of which they cannot be committed, e.g. hacking (DDoS attacks, botnets, zombies), crimeware (viruses, worms, trojan horses) or spamming. The horizontal approach includes crimes facilitated by the use of computer tools and information technology, e.g., cyberterrorism, child pornography, unauthorized use of credit cards, identity theft (phishing), intellectual piracy, and criminal financial operations on the Internet (cyberlaundering).[23]

There are many types of cybercrime. For instance, identity theft is

---

[20] Sarah Gordon, and Richard Ford, "On the Definition and Classification of Cybercrime," in *Journal in Computer Virology* 20, no. 1 (2006): 17; Małgorzata Gruchoła, "Polityka Unii Europejskiej w zakresie cyberprzestępczości" in *Patologie w cyberświecie*, eds. Sebastian Bębas, Jerzy Plis, and Jan Bednarek (Radom: Wyższa Szkoła Handlowa, 2012), 149.

[21] Peter Grabosky, *Cybercrime. Keynotes in Criminology and Criminal Justice Series* (Oxford: Oxford University Press, 2016).

[22] Debra Shinder, and Ed Tilttel, *Cyberprzestępczość. Jak walczyć z łamaniem prawa w sieci* (Gliwice: Helion, 2006), 35.

[23] David S. Wall, "Cybercrime, Media and Insecurity. The Shaping of Public Perceptions of Cybercrime," in *International Review of Law, Computers & Technology* 22, no. 1 (2008): 45–63.

> an attack that occurs when an individual accesses a computer to glean a user's personal information, which they then use to steal that person's identity or access their accounts (banking, credit cards). Criminals sell identity information on darknet markets, offering financial accounts, as well as other types of accounts (like video streaming services, webmail, video and audio streaming, online auctions).[24]

Personal health information is another target for identity thieves. Software piracy is

> an attack that involves the unlawful copying, distribution and use of software programs with the intention of commercial or personal use (e.g. trademark violations, copyright infringements and patent violations).[25]

Cyberextortion is "the crime involving an attack or threat of an attack coupled with a demand for money to stop the attack."[26] Cryptojacking is "an attack that uses scripts to mine cryptocurrencies within browsers without the user's consent."[27] Credit card fraud is "an attack that occurs when hackers infiltrate retailers' systems to get the credit card and/or banking information of their customers."[28] Cyberespionage is "a crime involving a cybercriminal who hacks into systems or networks to gain access to confidential information held by a government or other organization. Attacks may be motivated by profit or by ideology."[29] Cyberespionage activities

---

[24] Kate Brush, "Cybercrime," accessed Feb. 4, 2021, https://www.techtarget.com/searchsecurity/definition/cybercrime.

[25] *Ibid*.

[26] *Ibid*.

[27] *Ibid*.

[28] *Ibid*.

[29] *Ibid*.

can include every type of cyberattack to gather, modify or destroy data, as well as using network-connected devices, like webcams or closed-circuit TV (CCTV) cameras, to spy on a targeted individual or groups and monitoring communications, including emails, text messages and instant messages.[30]

## Method

In order to verify the hypotheses, I apply the following research methods: a secondary quantitative and qualitative analysis of the collected data in the reports and a comparative method. The comparative method "looks at an object of study in relation to another object"[31] (in research: technology-based cybercrime and human-based cybercrime; fear and personal experiences). The object of the study is compared across space (opinions of EU citizens) and time (2013–2020). I use the comparative method to elucidate patterns of similarities and differences in the frequency and perception of human and technology-based cybercrime, to determine their sources (fear and personal experiences) and to explicate their continuity and change.

In order to address the research issue, I analyze reports: *Europeans' attitudes towards internet security* and *Cyber security*,[32] prepared at the request of the European Commission, Directorate-General for Migration and Home Affairs and coordinated by the Directorate-

[30] *Ibid*.

[31] Norwegian Institute of International Affairs, "Comparative Methods," accessed May 23, 2022, https://www.nupi.no/en/Our-research/Topics/Theory-and-method/Comparative-methods.

[32] Kantar Public Brussels, *Cyber Security. Report No. 404 Special Eurobarometer* (Brussels: European Union, 2013); Kantar Public Brussels, *Cyber Security. Report No. 423 Special Eurobarometer* (Brussels: European Union, 2014); Kantar Public Brussels,

General for Communication, Media Monitoring, Media Analysis and Eurobarometer Unit. The analyzed studies were performed in EU countries, from 2013 to 2020, in groups of 27,498 respondents of the minimum 15 years of age, coming from different social and demographic environments, interviewed face-to-face at their homes, and in their mother tongue.

## Results and Discussion

Étienne Gilson was aware of the historical changes in culture, stemming from globalization and blurring differences between high and low culture. The development of the media and an extension of the addressee list of intellectual goods provided media messages with a new, more entertaining, schematic character. As a result, the media content became more effortless, promoting uniform patterns of behavior, open to constant changes and forms of self-fulfillment, oftentimes breaking with the valid norms and rules of law. It is in this context that Gilson raises questions of the influence of this process on aesthetic experience, referring to mass culture and its addressees.[33]

> The new society is a mass society precisely in the sense that the mass of the population has become incorporated into the society.[34]

---

*Cyber Security. Report No. 464a Special Eurobarometer* (Brussels: European Union, 2017); Kantar Public Brussels, *Europeans' Attitudes Towards Internet Security. Report No. 480-Wave EB90.2 Special Eurobarometer* (Brussels: European Union, 2019); Kantar Public Brussels, *Europeans' Attitudes Towards Internet Security. Report No. 499-Wave EB92.2 Special Eurobarometer* (Brussels: European Union, 2020).

[33] Gilson, *Społeczeństwo masowe i jego kultura*, 19; Sochoń, "Piękno nie przekłada się na dolary."

[34] Edward Shills, "Mass Society and its Culture," in *Daedalus* 89, no. 2 (Spring, 1960): 288.

What can be observed is that impoverished aesthetic experience is more commonly replaced by the experience of fear, implied by the growing phenomenon of cybercrime, both perceived and experienced *de facto*.

Questions need to be addressed relating to the perception of specific cybercrimes, fears of experiencing of a specific cybercrime, and the cybercrime frequency itself.

## CYBERCRIME AND EXPERIENCING FEAR

An important component in cybercrime research is the social perception of particular cybercrime activities by EU citizens. They are unanimous (96%) in their opinion that child pornography is a serious crime; more than eight out of ten (82%) respondents regard it as a very serious crime, with a small group regarding it as a minor crime. The second position was occupied by online banking fraud. The vast majority (95%) of the respondents claim it to be a serious crime, and more than seven out of ten (71%) respondents see it as a very serious crime, while just under a quarter (24%) deem it fairly serious. Almost all (95%) of the respondents view identity theft as a serious crime, and seven out of ten (70%) argue that it is a very serious crime, while a quarter (25%) claim that it is a fairly serious crime. Nine out of ten (91%) of respondents consider cyber extortion as a serious crime. Almost six out of ten (58%) regard it as a very serious crime, a third (33%) regard it a fairly serious crime. The minority views it as a minor crime (6%) and just a few respondents (1%) believe it is not a crime at all. More than nine out of ten (91%) of the participants of the study claim that promoting racial hatred or religious extremism is a serious crime, with more than six out of ten (61%) saying that it is a very serious crime, and three out of ten (30%) regarding it as a fairly serious crime. Just 1% of the respondents claim that it is not a crime at all, however 6% think it is a minor crime. Almost nine out of ten (87%) respondents view cyber-attacks, preventing users from accessing online services, as a serious crime. Almost half (48%) regard this crime as very serious, nearly four in ten (39%) say it

| | Opinion of specific criminal activity | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Criminal activity | Type | Yes, it is a crime | | | | not a crime at all | don't know |
| | | | Total | 1. | 2. | 3. | | |
| 1 | Online child pornography | H | 98 | 82 | 14 | 2 | 1 | 1 |
| 2 | Debit/credit card or online banking fraud | T | 98 | 71 | 24 | 3 | 1 | 1 |
| 3 | Identity theft (somebody stealing your personal data and impersonating you) | H | 98 | 70 | 25 | 3 | 1 | 1 |
| 4 | Online materials promoting racial hatred or religious extremism | H | 97 | 61 | 30 | 6 | 1 | 2 |
| 5 | Demands for payment in return for getting back control of your device | | 97 | 58 | 33 | 6 | 1 | 2 |
| 6 | Hacking online social network or mail accounts | T | 97 | 44 | 41 | 12 | 1 | 2 |
| 7 | Online fraud where goods purchased are not delivered, are counterfeit or are not as advertised | T | 97 | 38 | 46 | 13 | 1 | 2 |
| 8 | Cyber-attacks which prevent you from accessing online services like banking or public services | T | 96 | 48 | 39 | 9 | 2 | 2 |
| 9 | The infection of devices with malicious software | T | 96 | 42 | 41 | 13 | 2 | 2 |
| 10 | Fraudulent emails or phone calls asking for your personal details (including access to your logins, computer, banking or payment information) | T | 96 | 39 | 44 | 13 | 2 | 2 |

Table 1. Perception of cybercrimes (%-EU).

T – technology-based cybercrime
H - human-based cybercrime
1. Very serious crime
2. Serious crime
3. Fairly serious crime

Own study based on the report by Kantar Public Brussels, *Europeans' Attitudes Towards Internet Security. Report No. 480-Wave EB90.2 Special Eurobarometer* (Brussels: European Union, 2019), 89.

is fairly serious. Less than one in ten (9%) regard it is a minor crime, and a small group (2%) think it is not a crime at all. More than eight out of ten (85%) respondents consider hacking online social networks and email accounts a serious crime, with a proportional group seeing this as a very serious crime (44%) or as a fairly serious crime (41%). More than one in ten (12%) believe it to be a minor crime, and almost none of the participants believes it is not a crime at all (1%). The majority (84%) of respondents see online fraud as a serious crime, less than half (46%) regard it as fairly serious, with nearly four in ten (38%) seeing it as a very serious crime. 13% of the respondents believe it to be a minor crime, and 1% of the respondents do not see it as a crime at all. More than eight out of ten (83%) respondents view fraudulent emails or phone calls as a serious crime, simultaneously 39% of respondents regard it as a very serious crime, a similar proportion seeing it as a fairly serious crime (44%). 13% of the respondents regard it as a minor crime, and only 2% think it is not a crime at all.[35]

Among ten cybercrimes surveyed in the group of EU citizens, three are of humanistic character, and seven are technological. The most serious crimes are human-based cybercrimes: online child pornography and identity theft (stealing one's personal data and impersonating them) (98%), and online materials promoting racial hatred or religious extremism (97%). Even though technology-based cybercrimes were ranked lower on the scale, with the exception of debit/credit card or online banking fraud (98%), what should be stressed is the slight difference of three points (96–98) between the first and the last criminal activity as presented in Table 1.

The majority of EU citizens regard cybercrimes as serious crimes, but the proportion of those who regard them as very serious crimes varies significantly between countries. In all the countries, with the

[35] Kantar Public Brussels, *Europeans' Attitudes Towards Internet Security. Report No. 480-Wave EB90.2 Special Eurobarometer* (Brussels: European Union, 2019), 89.

exception of Slovakia (81%), at least nine out of ten respondents claim that child pornography is a serious crime. In twenty-one out of the twenty-eight member countries, at least three quarters of the respondents provided such an answer (NL, MT, DE, FR, IE, SE, CY, EL, UK, DK, ES, FI, PT, EE, BE, HR, LU, LV, SI, CZ, AT), the highest proportions reported in Sweden (94%) and the Netherlands (93%), while in Romania (59%) and Slovakia (57%), less than six out of ten respondents rated it the same way. Only a tiny minority of the respondents regard it to be no crime at all.[36]

In all the countries with the exception of Slovakia (83%) at least nine out of ten respondents regard online banking fraud as a serious crime ("a very serious crime" and "a fairly serious crime"). The respondents' opinions treating online banking as "a very serious crime" vary: beginning from almost six out of ten respondents in Slovakia (56%), Romania (57%), at least six out of ten respondents (BG: 60%, PL: 62%, AT: 64%, EE: 65%, HU: 66%, IT, HR: 68% each), DE: 69%, seven or more respondents out of ten (FR: 70%, BE: 71%, NL, LV: both 72%, LT, ES, SI: 73% each, LU: 76%, CZ, PT, UK: 78% each, CY: 79%), to more than eight out of ten in Denmark (84%), Sweden and Malta (83% each), EL, IE (82% each) and FI (81%).[37]

A majority of respondents coming from all the EU member states consider identity theft, online child pornography and credit/debit card or online banking fraud a very serious crime (98%). These numbers range from more than eight out of ten respondents in Sweden, Denmark (85% each), Malta (83%), Finland and Cyprus (81% each), Greece (80%) to less than six out of ten in Austria, Romania (59% each), Bulgaria (58%) and Slovakia (54%). At least nine out of ten respondents consider identity theft a serious crime in the following countries:

---

[36] Kantar Public Brussels, *Europeans' Attitudes Towards Internet Security. Report No. 480*, 90.

[37] *Ibid*., 90.

EL: 99%; FR, FI, SE: 98% each, MT, DK, IE, NL, CY: 97% each; EE, ES, LT: 96% each; PT, CZ: 95% each; LU, LV, DE, IT: 94% each; HU, PL SI, RO: 93% each, BG: 92%), The figure is somewhat lower in Austria (88%), Croatia (84%) and Slovakia (83%). The highest proportion of the respondents who believe it not to be a crime were observed in Croatia (4%), Slovenia (3%), Austria and Portugal (2% each).[38]

In all the EU member states, at least eight out of ten respondents consider cyber extortion a serious crime, with the lowest rates observed in Austria (84%), Slovakia (81%) and Estonia (80%), and the highest rates observed in the United Kingdom and the Netherlands (96% each), Denmark, Lithuania and Ireland (95% each). There is much more variation when it comes to those who deem it a very serious crime: ranging from more than seven out of ten respondents in Ireland (76%), Denmark (75%), Cyprus (74%), Malta (73%) and the United Kingdom, Sweden, Luxembourg (70%), to less than half of the respondents sharing the same view in Germany, Slovakia (48% each), Bulgaria (45%) and Estonia (42%).[39]

In seven countries (HU: 49%, PT: 46%, CZ: 45%, BG: 43%, HR: 42%, EE: 38%, SK: 35%), a minority of respondents view materials promoting racial hatred or religious extremism to be a very serious crime, less than four out of ten holding this view in Estonia (38%) and Slovakia (35%). In all the EU member states, the majority of respondents view the online dissemination of materials promoting racial hatred or religious extremism as a serious crime: ranging from more than seven out of ten respondents in Croatia (73%) and Slovakia (71%) to almost all the respondents in the United Kingdom, France, Ireland, Spain (96% each). There are larger discrepancies in the number of respondents who consider it a very serious crime. Although in twenty-one EU member states the majority hold this view, the numbers range

[38] *Ibid*., 91.
[39] *Ibid*.

from half (50%) of the respondents in Romania and Poland to three quarters or more in the United Kingdom (77%), Ireland, France (75% each). In almost all the countries, with the exception of Croatia (8%), Slovenia (6%) and SE, PT, FI, RO, AT, EE, CZ, SK (3% each), very few respondents consider it not to be a crime at all (Kantar Public Brussels, 2019, p. 92).

In twenty-three of the twenty-eight member states (LT: 95%; IE, CY: 94% each; MT, DK, EL, NL: all 93%; PT, SE, FI: all 92%; UK, PL: 91% each; FR, BE, HU: 90% each; IT, RO: 89% each, LU: 87%; LV, DE: 84% each, CZ: 83%; SI, ES: 80% each) at least eight out of ten respondents consider cyber-attacks which prevent access to online services as a serious crime (in Lithuania: 95%; Ireland, Cyprus: 94% each). Croatia (61%) stands out in terms of a significantly lower number of respondents who view it as a serious crime. In ten countries (MT: 73%, DK: 67%, CY: 66%, IE: 65%, UK, SE: 61% each, EL: 57%, LT: 56%, NL: 52%, PL: 51%), the majority of respondents perceive cyber-attacks as a very serious crime, with nearly three quarters of respondents in Malta holding this view (73%). On the other hand, less than a third of the respondents in Croatia (29%), Estonia (31%) and Austria (33%) share this view. Croatia also stands out when it comes to the relatively high number of the respondents who consider it not to be a crime at all: 12%. The countries with lower rates are ES: 7%, SI: 5%, AT: 4%, CZ: 3%, PT, EE, SK: all 2% (Kantar Public Brussels, 2019, p. 93).

In twenty-three out of the twenty-eight EU member states, at least eight out of ten respondents (MT: 93%, CY: 92%, IE: 91%, LT, PL: 90% each, EL: 89%, ES, RO: 88% each, IT, FR, HU: 87% each, UK: 86%, LU, LV, DK: 85% each, NL, PT: 84% each, DE, CZ, SI: 82% each, SE: 81%) view hacking online social networks or email accounts as a serious crime. None of the countries stands out for a particularly large number of the respondents who hold this opinion. Respondents who view it as a very serious crime come from Ireland (63%), Cyprus

(66%) and Malta (72%), while in Estonia (26%) and Bulgaria (29%), less than three out of ten respondents think so. The highest proportion of those who consider hacking of online social networks or email accounts not to be a crime comes from Croatia and Slovenia (6% each), Austria (5%), SK (3%) and ES, IT, LU, DK, PT, BG, EE (2% each).[40]

In Malta (62%), Cyprus, and Ireland (60% each), at least six out of ten respondents consider online fraud to be a very serious crime, though in the Netherlands (19%) and Estonia (18%) less than a fifth hold this opinion. In all but four countries (SI: 74%, BG: 69%, EE: 69%, HR: 61%), at least three quarters of the respondents consider online fraud to be a serious crime, and in five cases at least nine out of ten share this view (LT: 93%, EL: 92%, CY: 91%, IE, PL: both 90%). The smallest rates were observed in Croatia (61%) and Estonia (69%). In most countries only a very small proportion of the respondents consider it not to be a crime at all (HR: 8%, SI: 5%, PT: 4%, AT: 3%, BE, BG: 2% each, other countries 1% each).

In all the surveyed countries, the majority of respondents see scam emails or phone calls as a serious crime. The exceptions being Slovakia (65%) and Croatia (57%), in all the other countries at least two thirds of respondents express this opinion. In four countries at least nine out of ten respondents believe it to be a serious crime: MT, LT: 93% each, IE, CY: 91% each. There are large differences in the numbers of those who consider it a very serious crime: in Ireland (62%) and Malta (65%) more than six out of ten respondents hold this view, compared with a fifth of those surveyed in Austria (20%) and Estonia (23%). In Croatia, Austria, and Slovenia there are relatively high numbers of those who do not see this as a crime at all (HR: 14%, AT, SI: both 6%).

The majority of respondents regard the dissemination of malicious software as a serious crime: Cyprus and Ireland (91% each), Belgium and Lithuania (90% each), France (89%), Denmark (88%), Latvia,

[40] *Ibid*., 96.

Malta, UK (87% each), Croatia (55%). Significant differences can be found in the proportion of those who think that this is a very serious crime: Croatia (24%), Austria (26%) and Bulgaria (27%), while in four countries the majority of the interviewees provided such an answer (IE, CY: 58% each, DK: 53%, LT: 51%), with six out of ten doing so in Malta (60%). In Slovakia (7%), Austria (8%), Slovenia (10%) and Croatia (12%) a relatively high number of the respondents believe it not to be a crime at all.[41]

## LEVEL OF KNOWLEDGE VERSUS LEVEL OF EXPERIENCE OF FEAR

> On the one hand, mass culture has a very wide range of infuence. On the other hand, it is characterised by a lack of higher aspirations for development. By referring to the 'lowest instincts,' mass culture reaches a broad range of people thanks to the high level of technological advancement. It offers no place for sublimation or refinement of feelings, which normally occurs by referring feelings to the spiritual.[42]

Educational and aesthetic functions become only secondary to the entertainment function, the consequence of which is a low level of knowledge of EU citizens on threats related to cybercrime.

Having found out the level of social perception of specific cybercrimes among EU citizens, I was particularly interested in the relationship between the level of knowledge of the risks of cybercrime activity and the fear of experiencing specific cybercrimes.

---

[41] *Ibid*., 95–96.

[42] Piotr Jaroszyński, "Kultura masowa czy kultura wysoka? Ideologiczny kontekst sporu o kulturę w Polsce" in *Katolicy i kultura: szanse i zagrożenia*, eds. Monika Kacprzak and Imelda Chłodna-Błach (Toruń: WSKSiM, 2014), 23.

| Level of knowledge of the risks of cybercrime activity | | Date of research | Fear of experiencing specific cybercrime | |
|---|---|---|---|---|
| Total number of those 'well informed' | 52 | October 2019 | Total number of those 'afraid' | 59.1 |
| | 51 | October-November 2018 | | 64.9 |
| | 46 | June – 2017 | | 60.1 |
| | 47 | October 2014 | | 56.5 |
| | 44 | May – June 2013 | | 43.4 |
| Average score | 48 | | Average score | 56.8 |
| Total number of those 'not well informed' | 47 | October 2019 | Total number of those 'not afraid' | 38.5 |
| | 46 | Oct. – Nov. 2018 | | 32.5 |
| | 51 | June – 2017 | | 38.2 |
| | 50 | October 2014 | | 41.3 |
| | 52 | May – June 2013 | | 55.1 |
| Average score | 49.2 | | Average score | 41.1 |
| Those who have no opinion | 1 | October 2019 | Those who have no opinion | 2.4 |
| | 3 | Oct. – Nov. 2018 | | 2.6 |
| | 3 | June – 2017 | | 1.7 |
| | 3 | October 2014 | | 2.3 |
| | 4 | May – June 2013 | | 1.6 |
| Average score | 2.8 | | Average score | 2.1 |

Table 2. Level of social knowledge of the risks of cybercrime activity versus the fear of experiencing specific cybercrimes.

Own study based on the reports of Kantar Public Brussels, *Europeans' Attitudes Towards Internet Security. Report No. 480*, 64-67; Kantar Public Brussels, *Europeans' Attitudes Towards Internet Security. Report No. 499-Wave EB92.2 Special* Eurobarometer (Brussels: European Union, 2020), 57-58, 80.

According to Table 2, in the 2014–2019 period , the level of fear of becoming a victim of specific cybercrimes is 8.8 pp (percentage points) higher than the level of knowledge about the risks of cybercrime activity (in 2014—9,5 pp; in 2017—14,1 pp; in 2018—13,9 pp; in 2019—7,1 pp). The reverse trend was observed in 2013 (—0,6 pp). The higher the level of knowledge of risks connected with cybercrime activities, the higher the fear of becoming a victim in cyberspace. What should also be noted is that, over the last six years, an increase was observed

both in the level of knowledge of the threats related to Internet use (8 pp) and in the level of fear of becoming a victim in cyberspace (15,7 pp). However, in 2019 a decrease of 5.8 pp was observed in the level of fear in comparison with 2018. At the same time, a decrease was observed in the number of groups deemed "not well informed" and "not afraid" (Kantar Public Brussels, 2019, pp. 64–65). The data (Table 2) show that less than half (48%) of EU citizens are aware of cybercrime threats (by assessing positively the level of their knowledge). The level of knowledge is 8.8 pp (56.8%) lower than the level of fear. Slight differences were observed in EU citizens' perception of whether they were informed or not about cybercrime threats (2013: 8 pp; 2019: 5 pp).

In 2019 (Table 3), European Union citizens were mostly afraid of becoming victims of the following cybercrimes: debit/credit card or online banking fraud (67%), infection of devices with malicious software and identity theft (both 66%), hacking online social network or mail account (61%) and fraudulent emails or phone calls asking for personal details (59%). What the respondents feared most was technology-based cybercrime, with the exception of identity theft. A significant difference was observed in comparison to the data obtained in 2018. What the EU citizens feared most then was human-based cybercrime: identity theft (70%), child pornography online (67%), and online material which promotes racial hatred or religious extremism (65%). A decrease in the level of fear was observed in 2019 in all the criminal activities and an increase in the number of those not afraid of cybercrime. It should be noted that in the period of 2013–2018, a reverse trend was observed, i.e., a gradual increase in the level of fear of all types of cybercrime. Even though the highest increase was observed in the level of fear of human-based cybercrime, an increase was also found when it comes to technology-based cybercrime. The values of the increase are as follows:

- 30 pp: "online material which promotes racial hatred or religious extremism" (from 35% to 65%);

| Criminal activity | Fear of experiencing specific cybercrimes | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 2013 | | | 2014 | | | 2017 | | | 2018 | | | 2019 | | |
| | 1 | 2 | 3 | 1 | 2 | 3 | 1 | 2 | 3 | 1 | 2 | 3 | 1 | 2 | 3 |
| Credit/debit card or online banking fraud | 49 | 49 | 2 | 63 | 35 | 2 | 66 | 32 | 2 | 70 | 28 | 2 | 67 | 31 | 2 |
| The infection of devices with malicious software | - | | | 66 | 33 | 1 | 69 | 30 | 1 | 71 | 27 | 2 | 66 | 32 | 2 |
| Identity theft | 52 | 47 | 1 | 68 | 31 | 1 | 69 | 30 | 1 | 70 | 28 | 2 | 66 | 32 | 2 |
| Hacking online social network or mail account | 45 | 54 | 1 | 60 | 38 | 2 | 63 | 35 | 2 | 67 | 31 | 2 | 61 | 37 | 2 |
| Fraudulent emails or phone calls asking for your personal details | 43 | 56 | 1 | 57 | 42 | 1 | 60 | 39 | 1 | 60 | 38 | 2 | 59 | 40 | 1 |
| Cyber-attacks which prevent you from accessing online services like banking or public services | 37 | 61 | 2 | 50 | 47 | 3 | 57 | 41 | 2 | 61 | 36 | 3 | 57 | 40 | 3 |
| Demands for payment in return for getting back control of your device | - | | | 47 | 50 | 3 | 55 | 43 | 2 | 60 | 37 | 3 | 55 | 42 | 3 |
| Online fraud where goods purchased are not delivered or are not as advertised | 42 | 56 | 2 | 56 | 41 | 3 | 58 | 40 | 2 | 58 | 39 | 3 | 54 | 43 | 3 |
| Child pornography online | 44 | 54 | 2 | 52 | 45 | 3 | 53 | 45 | 2 | 67 | 29 | 4 | 53 | 44 | 3 |
| Online material which promotes racial hatred or religious extremism | 35 | 64 | 1 | 46 | 51 | 3 | 51 | 47 | 2 | 65 | 32 | 3 | 53 | 44 | 3 |

Table 3. The level of fear of experiencing specific cybercrimes (2013-2019).

1. Total number of those 'afraid'
2. Total number of those 'not afraid'
3. Total number of those who have no opinion

Own study based on the reports: Kantar Public Brussels, *Cyber Security. Report No. 404 Special Eurobarometer* (Brussels: European Union, 2013)*;* Kantar Public Brussels, *Cyber Security. Report No. 423 Special Eurobarometer* (Brussels: European Union, 2014); Kantar Public Brussels, *Cyber Security. Report No. 464a Special Eurobarometer* (Brussels: European Union, 2017); Kantar Public Brussels, *Europeans' Attitudes Towards Internet Security. Report No. 480*, 79-80, 103; Kantar Public Brussels, *Europeans' Attitudes Towards Internet Security. Report No. 499*, 80.

- 24 pp: "cyber-attacks which prevent you from accessing online services like banking or public services" (from 37% to 61%);
- 23 pp: "child pornography online" (from 44% to 67%);
- 22 pp: "hacking online social network or mail account" (from 45% to 67%);
- 21 pp: "credit/debit card or online banking fraud" (from 49% to 70%).

The performed comparative analysis (Table 4) suggests that the level of fear does not always correlate with the level of social perception. The greatest fear is not always caused by criminal activities perceived as very serious. On the contrary, the infection of devices with malicious software was regarded a very serious crime by only 42% of the respondents, yet it was a source of considerable fear among many respondents. Child pornography, treated as the most serious criminal activity, is a source of fear among 53% of EU citizens.

## FEAR OF EXPERIENCING CYBERCRIME VERSUS FREQUENCY OF EXPERIENCING CYBERCRIME

In the context of the fears expressed by EU citizens and their knowledge of cybercrime, the question arises about the scale of negative experiences resulting from their online activity.

The activities of cybercrime most commonly experienced by those surveyed are the receipt of fraudulent emails or phone calls (2018: 34%, 2019: 36%), discovering malicious software (2018: 33%, 2019: 26%) and online material which promotes racial hatred or religious extremism (2018: 18%, 2019: 13%). The types of cybercrime least experienced by respondents are accidentally encountering child pornography (2018: 7%, 2019: 5%) and identity theft (2018: 7%, 2019: 6%). In all other cases, less than a fifth of those polled report having been a victim of these situations. For all the forms of cybercrime identified, only a small group of European Union citizens claim that they have been a victim of a given form of cybercrime at least once within the last three

| | | | Perceptions of criminal activity | | | | | | Level of fear | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Criminal activity | Type | Yes | | | | non | don't know | yes | non | have no opinion |
| | | | Total | 1. | 2. | 3. | | | | | |
| 1 | Online child pornography | H | 98 | 82 | 14 | 2 | 1 | 1 | 53 | 44 | 3 |
| 2 | Credit/debit card or online banking fraud | T | 98 | 71 | 24 | 3 | 1 | 1 | 67 | 31 | 2 |
| 3 | Identity theft | H | 98 | 70 | 25 | 3 | 1 | 1 | 66 | 32 | 2 |
| 4 | Online material which promotes racial hatred or religious extremism | H | 97 | 61 | 30 | 6 | 1 | 2 | 53 | 44 | 3 |
| 5 | Demands for payment in return for getting back control of your device | | 97 | 58 | 33 | 6 | 1 | 2 | 55 | 42 | 3 |
| 6 | Hacking online social network or mail account | T | 97 | 44 | 41 | 12 | 1 | 2 | 61 | 37 | 2 |
| 7 | Online fraud where goods purchased are not delivered or are not as advertised | T | 97 | 38 | 46 | 13 | 1 | 2 | 54 | 43 | 3 |
| 8 | Cyber-attacks which prevent you from accessing online services | T | 96 | 48 | 39 | 9 | 2 | 2 | 57 | 40 | 3 |
| 9 | The infection of devices with malicious software | T | 96 | 42 | 41 | 13 | 2 | 2 | 66 | 32 | 2 |
| 10 | Fraudulent emails or phone calls asking for your personal details | T | 96 | 39 | 44 | 13 | 2 | 2 | 59 | 40 | 1 |

Table 4. Perceptions of criminal activity versus level of fear.

1. Very serious crime
2. Serious crime
3. Fairly serious crime

Own study based on Table 1 and 3.

years. In most cases, the proportion of those polled who have experienced a given crime once is larger than the proportion of those who have experienced it more often.[43]

Table 5 shows that in 2019 the level of fear of all the analyzed cybercrime activities decreased in comparison with 2018. The greatest decrease (14 pp) was observed when it comes to online child pornography (2018: 67%, 2019: 53%) and (12 pp) online materials promoting racial hatred or religious extremism (2018: 65%, 2019: 53%). The lowest decrease (1 pp) was observed in relation to fraudulent emails or phone calls asking for personal details (2018: 60%, 2019: 59%). A downward trend, except for criminal activity such as phishing (2018: 34%, 2019: 36%), was noted in all the cybercrime activities experienced by EU citizens. The greatest decrease (7 pp) was observed when it comes to the infection of devices with malicious software (2018: 33%, 2019: 26%), while a minimal decrease (1 pp) was observed in three cybercrime activities, i.e., demands for payment in return for regaining control of your device, identity theft and hacking online social network or mail account.

Table 5 shows that EU citizens' fear of experiencing specific cybercrimes does not correlate with their personal experience. The respondents express fear of the following cybercrimes: the infection of devices with malicious software (2018: 71%, 2019: 66%), identity theft (2018: 70%, 2019: 66%), credit/debit card or online banking fraud (2018: 70%, 2019: 67%), online child pornography (2018: 67%, 2019: 53%) and hacking of online social networks or mail accounts (2018: 67%, 2019: 61%). At the same time, a third of the respondents have actually experienced various types of cybercrime (receiving false e-mails or telephone calls: 2018: 34%, 2019: 36%); discovering malware (2018: 33%, 2019: 26%) and receiving online materials promoting racial hatred or religious extremism (2018: 18%, 2019: 13%). In other cases,

[43] *Ibid*., 103.

| Criminal activity | Fear of experiencing specific cybercrimes | | | | | | Frequency of experiencing cybercrimes | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Yes | | No | | Don't know | | Yes | | Never | | Have no opinion | |
| | 2018 | 2019 | 2018 | 2019 | 2018 | 2019 | 2018 | 2019 | 2018 | 2019 | 2018 | 2019 |
| Credit card or online banking fraud (T) | 70 | 67 | 28 | 31 | 2 | 2 | 10 | 8 | 88 | 90 | 2 | 2 |
| The infection of devices with malicious software (T) | 71 | 66 | 27 | 32 | 2 | 2 | 33 | 26 | 65 | 70 | 2 | 2 |
| Identity theft (H) | 70 | 66 | 28 | 32 | 2 | 2 | 7 | 6 | 91 | 92 | 2 | 2 |
| Hacking online social network or mail account (T) | 67 | 61 | 31 | 37 | 2 | 2 | 12 | 11 | 86 | 87 | 2 | 2 |
| Fraudulent emails or phone calls asking for your personal details (T) | 60 | 59 | 38 | 40 | 2 | 1 | 34 | 36 | 64 | 63 | 2 | 1 |
| Cyber-attacks which prevent you from accessing online services (T) | 61 | 57 | 36 | 40 | 3 | 3 | 11 | 8 | 87 | 90 | 2 | 2 |
| Demands for payment in return for getting back control of your device (T) | 60 | 55 | 37 | 42 | 3 | 3 | 9 | 8 | 89 | 90 | 2 | 2 |
| Online fraud where goods purchased are not delivered or are not as advertised (T) | 58 | 54 | 39 | 43 | 3 | 3 | 15 | 12 | 83 | 83 | 2 | 2 |
| Child pornography online (H) | 67 | 53 | 29 | 44 | 4 | 3 | 7 | 5 | 91 | 93 | 2 | 2 |
| Online material which promotes racial hatred or religious extremism (H) | 65 | 53 | 32 | 44 | 3 | 3 | 18 | 13 | 80 | 85 | 2 | 2 |
| Average score | 64.9 | 59.1 | 32.5 | 38.5 | 2.6 | 2.4 | 15.6 | 13.3 | 82.4 | 84.3 | 2.0 | 1.9 |

Table 5. Fear of experiencing specific cybercrimes versus frequency of experiencing cybercrime.

T - technology-based cybercrime
H - human-based cybercrime

Own study based on the reports: Kantar Public Brussels, *Europeans' Attitudes Towards Internet Security. Report No. 480*, 82, 103, 105; Kantar Public Brussels, *Europeans' Attitudes Towards Internet Security. Report No. 499*, 102.

less than a fifth of the EU citizens have experienced cybercrime.

In 2018, the greatest discrepancy between the level of fear and personal experience was noted when it comes to identity theft and online child pornography. The level of fear of experiencing these cybercrimes was twofold higher than the level of personal experience (70% vs 7%; 67% vs 7% respectively). In 2019, the level of fear was eleven times higher than the level of personal experience (identity theft: 66% vs 6%; online child pornography: 53% vs 5%) ([14], p. 82, 103, 105; [15]). A majority of respondents express fear of experiencing cybercrime (2018: 64,9%; 2019: 59,1%), although only the minority have actually experienced such a crime and are aware of this (2018: 15,6%; 2019: 13,3%).

Table 5 shows that EU citizens experienced technological cybercrime more often than human-based cybercrime. In 2018, the former was experienced by 17.7% of the respondents, while human-based

| Date of research | Level of knowledge of the risks of cybercrime activity | | Fear of experiencing specific cybercrimes | | Frequency of experiencing specific cybercrimes | |
|---|---|---|---|---|---|---|
| 2019 | Total number of those "well informed" | 52 | Total number of those "afraid" | 59.1 | Yes | 13.3 |
| 2018 | | 51 | | 64.9 | | 15.6 |
| | Average score | 51.5 | Average score | 62 | Average score | 14.45 |
| 2019 | Total number of those "not well informed" | 47 | Total number of those "not afraid" | 38.5 | Never | 84.3 |
| 2018 | | 46 | | 32.5 | | 82.4 |
| | Average score | 46.5 | Average score | 35.5 | Average score | 83.35 |
| 2019 | Total number of those who have no opinion | 1 | Total number of those who have no opinion | 2.4 | Total number of those who have no opinion | 1.9 |
| 2018 | | 3 | | 2.6 | | 2.0 |
| | Average score | 2.0 | Average score | 2.5 | Average score | 1.95 |

Table 6. A comparative analysis of the level of knowledge, fear and frequency of experiencing specific cybercrimes in the period of 2018-2019.

Own study based on Table 1 and 5.

cybercrime was experienced by 10.7%. In 2019, a slight decrease was observed in both categories (technology-based cybercrime: 15,8%; human-based cybercrime: 8%).

The obtained data suggest that the source of fear is not located in the personal experience of EU citizens, but it stems from other factors, e.g., the level and range of information on cyberspace threats disseminated in mass culture.

The performed analyses show that the level of knowledge of the risks of cybercrime activities is slightly lower (by 8,8 pp) than the level of fear of experiencing specific cybercrimes (in 2014: 9,5 pp; in 2017: 14,1 pp; in 2018: 13,9 pp; in 2019: 7,1 pp).

The level of knowledge of the risks of cybercrime activity is a function of the level and range of the information one possesses. Since the source of fear of experiencing specific cybercrimes is not related to the personal experience of EU citizens (which is confirmed by the analyses), it can be assumed that in mass culture the experience of fear and the culture of fear is shaped by the media. The Eurobarometer reports suggest that the main source of information for EU citizens is content propagated by the media (television news: 66%; social networks and the Internet: 48%; the press: 29%; the radio: 23%.[44])

## Conclusions

Mass culture, imposed by the authorities, spreads a specific form of high culture to the masses.[45] On the basis of the performed analyses, I observe that the industrialization of tools of culture (the internet) is both

[44] Kantar Public Brussels, *Attitudes of European Citizens Towards the Environment. Report No. 501-Wave EB92.4 Special Eurobarometer* (Brussels: European Union, 2020), 29.

[45] Imelda Chłodna-Błach, *From Paideia to High Culture. A Philosophical-Anthropological Approach* (Berlin: Peter Lang GmbH, 2020), 144.

a source and a result of experiencing fear. Despite the fact that mass culture has increased the opportunities of aesthetic experience, it has also modified its conditions. The internet content does not offer art per se but rather its virtual image, hence a distinct object. Technology-based reproduction of works of art not only intensified aesthetic experience but became a cause and effect of cybercriminal activities. Each of the discussed activities that break the rules of law may be indirectly linked to aesthetic experience, either as a source or an effect.

The first hypothesis assumed that European Union citizens are more afraid of experiencing technology-based cybercrime than human-based cybercrime. This hypothesis was not confirmed. In 2018, the greatest number of the respondents expressed fears connected with discovering malware on their devices (71%), identity theft (70%) and fraud connected with credit/debit cards and online banking (70%). However, in 2019, the greatest number of respondents pointed towards credit card or online banking fraud (67%) and the infection of devices with malicious software and identity theft (66% each). The second hypothesis assumed that EU citizens more often admit to experiencing technology-based cybercrime than human-based cybercrime. This hypothesis was confirmed. A difference in the levels of personal experience in relation to technology-based cybercrime (2018: 17,7%; 2019: 15,8%) and human-based cybercrime (2018: 10,7%; 2019: 8%) oscillates around 7 pp.

The third hypothesis, assuming that the level of fear of experiencing cybercrime is higher than the level of personal experience, was confirmed. The performed analysis shows that the level of fear experienced by EU citizens is several times higher, depending on the type of cybercrime activity, than the level of their personal experience. For instance, when it comes to identity theft (66% vs 6%) and online child pornography (53% vs 5%), the level of fear of experiencing these crimes is eleven times higher than the level of personal experience, while in the case of "fraudulent emails or phone calls asking for your personal details," it is almost twofold higher (59% vs 34%).

The public perception of cybercrime, characteristic of a high level of fear of experiencing cybercrime activities (in 2018: 64.9%; in 2019: 59.1%) is not a result of personal experience (in 2018: 15.6%; in 2019: 13.3%) but rather an effect of other factors, e.g., the level and range of information spread by the media. EU citizens' level of knowledge of the risks of cybercrime activity (in 2019: 52%; in 2018: 51%; in 2017: 46%; in 2014: 47%; in 2013: 44%), being synonymous with the level of social awareness, can be related to taking precautions against cybercrime, but may also be related to living in the culture of fear.

Fear of cybercrime does not stem from the personal experiences of EU citizens but is constructed socially and permeated in public discourse by the media, contributing to the development of a culture of fear. Bearing in mind that human responses to threats modify the processes of socialization and cultural learning, it is important to emphasize the significance of media competence as an integral part to critically assessing information about cybercrime, as propagated in the public discourse. Finally, I give the floor to Étienne Gilson:

> Using mass techniques everywhere will pose inevitable problems. It is utopian to think that in every field the elites will uplift the masses to the heights of their art; it seems inappropriate to expect from the elites, when such a mission fails, to curtail their expansion of any intellectual, artistic, and moral activity by means of the mass media, which are increasingly trying to subordinate them to their own ends. It would not be right. The masses are entitled to their own culture and their own means.[46]

[46] Gilson, *Społeczeństwo masowe i jego kultura*, 146.

## Mass Culture: An Aesthetic Experience or An Experience of Fear?

SUMMARY

According to Étienne Gilson, an endless reproduction of the technical aspects of a work of art can modify not only the aesthetic experience of which it is an object, but also the culture it is embedded in. Since industrialization of a cultural product in the form of the internet is a means of generating mass culture, questions could be raised regarding its sources and effects. This article offers three assumptions: 1) the internet, together with its content and actions taken by internet users, is a source of fear of experiencing cybercrime; 2) experiencing cybercrime is a result of using the internet; 3) in mass culture, the aesthetic experience has been replaced by the experience of fear. In order to address the titular question, I performed comparative analyses of EU citizens' opinions on the basis of the Eurobarometer study conducted in EU countries (2013–2020) relating to the social perception of cybercrime, treated as a source of experiencing fear, and the level of their personal experience. A secondary quantitative and qualitative analysis of the collected data were performed, and a comparative method was used.

**Keywords:** aesthetic experience; experience of fear; Eurobarometer; mass culture, technology-based cybercrime; human-based cybercrime

REFERENCES

Brush, Kate. "Cybercrime." Accessed February 4, 2021. https://www.techtarget.com/searchsecurity/definition/cybercrime.

Callanan, Valerie J. "Media Consumption, Perceptions of Crime Risk and Fear of Crime: Examining Race/Ethnic Differences." In *Sociological Perspectives* 55, no. 2 (2012): 93–115, https://doi.org/10.1525/sop.2012.55.1.93.

Chłodna-Błach, Imelda. *From Paideia to High Culture. A Philosophical-Anthropological Approach*. Berlin: Peter Lang GmbH, 2020.

Furedi, Frank. *Culture of Fear: Risk Taking and the Morality of Low Expectation*. New York, London: Continuum International Publishing Group, 2002.

Furedi, Frank. *How Fear Works: Culture of Fear in the Twenty-first Century*. London: Bloomsbury Continuum, 2018.

Gilson, Étienne. *La société de masse et sa culture*. Paris: Librairie Philosophique Vrin, 2002.

Gilson, Étienne. *Społeczeństwo masowe i jego kultura*, trans. Agnieszka Kuryś. Warszawa: Fundacja Świętego Mikołaja, Redakcja "Teologii Politycznej," 2022.

Gordon, Sarah and Ford, Richard. "On the Definition and Classification of Cybercrime" in *Journal in Computer Virology* 20, no. 1 (2006): 13–20.

Grabosky, Peter. *Cybercrime. Keynotes in Criminology and Criminal Justice Series*. Oxford: Oxford University Press, 2016.

Gruchoła, Małgorzata, "W pajęczynie globalnej sieci," in *Społeczeństwo i Rodzina* 47, no. 2 (2016): 94–116.

Gruchoła, Małgorzata, and Sławek-Czochra, Małgorzata. "'The Culture of Fear' of Inhabitants of EU Countries in their Reaction to the Covid-19 Pandemic—A Study Based on the Reports of the Eurobarometer," in *Safety Science* 135, article 105140 (March 2021): 1–9, https://doi.org/10.1016/j.ssci.2020.105140.

Gruchoła, Małgorzata, and Szulich-Kałuża, Justyna. "Digital Competence in Cybercrime Behaviours: A Study Based on Eurobarometer Research," in *Zeszyty Naukowe KUL* 65, no. 1 (2022), DOI: 10.31743/znkul.13610.

Gruchoła, Małgorzata. "Polityka Unii Europejskiej w zakresie cyberprzestępczości." in *Patologie w cyberświecie*, edited by Sebastian Bębas, Jerzy Plis, and Jan Bednarek, 147–165. Radom: Wyższa Szkoła Handlowa, 2012.

Grupp, Stefanie. *Political Implications of a Discourse of Fear*. New York: New York University, 2003.

Guzelian, Christopher P. *Liability and Fear*. Stanford: Stanford Law School, 2004.

Jaroszyński, Piotr. "Kultura masowa czy kultura wysoka? Ideologiczny kontekst sporu o kulturę w Polsce." in *Katolicy i kultura: szanse i zagrożenia*, edited by Monika Kacprzak and Imelda Chłodna-Błach, 21–33. Toruń: WSKSiM 2014.

Kantar Public Brussels. *Attitudes of European Citizens Towards the Environment. Report No. 501-Wave EB92.4 Special Eurobarometer*. Brussels: European Union, 2020.

Kantar Public Brussels. *Cyber Security. Report No. 404 Special Eurobarometer*. Brussels: European Union, 2013.

Kantar Public Brussels. *Cyber Security. Report No. 423 Special Eurobarometer*. Brussels: European Union, 2014.

Kantar Public Brussels. *Cyber Security. Report No. 464a Special Eurobarometer*. Brussels: European Union, 2017.

Kantar Public Brussels. *Europeans' Attitudes Towards Internet Security. Report No. 480-Wave EB90.2 Special Eurobarometer*. Brussels: European Union, 2019.

Kantar Public Brussels. *Europeans' Attitudes Towards Internet Security. Report No. 499-Wave EB92.2 Special Eurobarometer*. Brussels: European Union, 2020.

Norwegian Institute of International Affairs. "Comparative Methods". Accessed May 23, 2022. https://www.nupi.no/en/Our-research/Topics/Theory-and-method/Comparative-methods.

Sochoń, Jan. "Piękno nie przekłada się na dolary. Przepowiednie estetyczne Étienne'a Gilsona." Accessed June 1, 2022. https://teologiapolityczna.pl/ks-jan-sochon-spoleczenstwo-masowe-i-jego-kultura-przedmowa-1.

Shills, Edward. "Mass Society and its Culture." *Daedalus* 89, no. 2 (Spring, 1960): 288–314.

Shinder, Debra, and Tilttel, Ed. *Cyberprzestępczość. Jak walczyć z łamaniem prawa w sieci*. Gliwice: Helion, 2006.

Shusterman, Richard. "O końcu i celu doświadczenia estetycznego," in *O sztuce i życiu. Od poetyki hip-hopu do filozofii somatycznej*, edited by Richard Shusterman, 129–151, trans. Wojciech Małecki. Wrocław: Wydawnictwo Atla 2, 2007.

Wall, David S. "Cybercrime, Media and Insecurity. The Shaping of Public Perceptions of Cybercrime." in *International Review of Law, Computers & Technology* 22, no. 1 (2008): 45–63.