EUMEPLAT

European Media Platforms: assessing positive and negative externalities for European culture

D5.1

Assessing Externalities:

Surveillance and Resistance

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101004488

The information and views in this report are those of the author(s) and do not necessarily reflect the official opinion of the European Union. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein.

Document information

Grant Agreement #:	**101004488**
Project Title:	**EUROPEAN MEDIA PLATFORMS: ASSESSING POSITIVE AND NEGATIVE EXTERNALITIES FOR EUROPEAN CULTURE**
Project Acronym:	**EUMEPLAT**
Project Start Date:	**01/03/2021**
Related work package:	WP5 Power: People and Platforms
Related task(s):	5.1 Assessing Externalities: Surveillance and Resistance
Lead Organisation:	P12: CU - Charles University
Author(s):	Vaia Doudaki (CU) Panos Kompatsiaris (IULM) Dessislava Boshnakova (NBU) Jim Ingebretsen Carlson (UOC) Judith Clares Gavilán (UOC) Contributions by Nico Carpentier (CU) Miloš Hroch (CU)
Status	Final
Submission date:	13/11/2023
Dissemination Level:	Public

Table of Contents

1. Introduction

This deliverable focusses on the thematic area of surveillance and resistance to surveillance, through digital platforms, in Europe. It consists of three main sections. The first section has two parts. Part-one presents a theoretical reflection on surveillance and resistance to surveillance, addressing the interdisciplinary field of surveillance studies. This theoretical reflection elaborates on the multitude of approaches to and definitions of surveillance/resistance[1], presents the main actors, practices and technologies of surveillance/resistance, and further explores political, cultural and social aspects and dimensions of surveillance/resistance, as they are addressed in the international academic literature. Par-two of the first section includes a brief presentation of practices of digital surveillance/resistance in Europe, in specific areas, pertinent to the EUMEPLAT project, namely, economy, migration, gender, health and the environment.

The second section of this deliverable reflects on the research conducted within the EUMEPLAT project and its relevance for surveillance/resistance. This reflective and reflexive part scrutinises the research, data and analyses produced as part of the first four EUMEPLAT work package deliverables (WP1-WP4), and identifies a series of issues, dimensions and debates, pertaining to surveillance/resistance, facilitated through communication and media platforms in Europe.

The third section, which has a future-oriented focus, involves future scenario development and analysis, concerning surveillance/resistance, enabled through communication and media platforms in Europe. Even if the scenarios are fictional and for this reason a number of these scenarios were not considered by their creators as likely to materialise, still, they are highly relevant as they encapsulate visions –that is, hopes and fears– about societies and about Europe. Hence, this section presents the findings of the scenario analysis, by focussing on the scenario creators' visions about the future, without engaging in evaluative judgements about how these creators imagine the future, but by exploring the underlying attitudes, assumptions and ideologies that inform these visions.

[1] Writing 'surveillance/resistance' as a twofold concept connected through a slash reflects the argument that surveillance and resistance to surveillance are two interconnected components, coexisting in an entangled fashion and impacting one another in diverse ways. As Martin and his co-authors (2009) argued, "resistance is not merely an epiphenomenon of surveillance – it is a basic and necessary co-development of surveillance" (p. 216).

The three sections of this deliverable –theoretical elaboration, reflection on EUMEPLAT research, and future scenario development and analysis – allow to: a. deliver a condensed state of the art in surveillance studies, from a communication and media studies perspective, b. address a theoretically informed reflection concerning surveillance/resistance, through digital platforms, in Europe, as it appears in contemporary research (see EUMEPLAT WP 1-4), and c. sketch out future outlooks, in the specific area of study, examining how these visions of the future reflect main assumptions, fears and hopes about Europe.

2. A theoretical reflection

2.1 Approaches to surveillance[2]

Surveillance, which can be performed by state, public, corporate and private actors and entities, refers to the "focused, systematic, and routine monitoring of behavior, activities, or information" (Costanza, 2018, p. 95), "for the sake of control, entitlement, management, influence or protection" (Murakami Wood, 2006, p. 4). Similarly, Lyon (2001a, p. 2) defines surveillance as "any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered". In a later definition, Lyon (2018, p. 6) focusses on "the operations and experiences of gathering and analysing personal data for influence, entitlement, and management", arguing that while surveillance is mostly performed by states and corporations, it "may also be carried out by people in everyday life" (Lyon, 2018, p. 6). The elements of 'experience' and 'entitlement' are important, as they allow to broaden the scope of surveillance, as it concerns its practices, motivations, and involved actors.

The delimitation of what surveillance is and what is not, is not straightforward, and as elaborated later-on, is context-sensitive. Surveillance is generally perceived as a necessary practice of organised societies (Giddens, 1984), and the discussion revolves mainly around legitimate or illegitimate, legal or illegal, ethical or unethical forms of surveillance, rather than whether surveillant-free societies can exist. What is common in evaluations of surveillance, regardless of the specific context, is that several principles are evoked and discussed as un/necessary for surveillance to be justified (see Allen, 2008; Lyon, 2001b; 2003; Macnish, 2014; Marx, 1998; Sewell & Barker, 2001). Macnish (2014), for example, mentions the following principles as required for the justification of surveillance:

> "there must be a justified cause, supported by a correct intention, […] the surveillance must be necessary and have a chance of success, and […] it [needs to] be both

[2] Even though this scholarly review does not address the artistic and literary fields, it still acknowledges art's and literature's significant impact on politics, academic work and popular culture, when it comes to surveillance conceptualisations and imaginaries. For example, the dystopian fiction novels *The Trial* by Franz Kafka (published in 1925), and *1984* by George Orwell (published in 1949), offered the conceptual tools to describe processes and practices of enhanced or absolute state surveillance, used in art, academic work and politics. Orwell's fictional totalitarian leader Big Brother even lent his name to the popular television reality programmes that bear the same title, first launched in 1999 in the Netherlands (Drotner, 2002).

> proportional and subject to formal declaration. In terms of the means employed, acts of surveillance should again be proportionate in the harm that they occasion and they should seek to discriminate as much as possible between legitimate and illegitimate targets" (p. 143).

Such normative considerations show that the discussion around the ethical or legitimate boundaries of surveillance takes the form of an open and ongoing struggle in the fields of academia, legislation, politics, economy and civil society.

Furthermore, perceptions of and responses to surveillance are products of their time and context; hence, surveillance policies, practices and understandings are historically, politically, economically and culturally specific, created in a dynamic interaction with a series of forces and actors, producing unique outcomes (Fernandez & Huey, 2009; Martin et al., 2009). Therefore, one needs to be careful to avoid deterministic or single-factor approaches that are met sometimes when discussing, for example, the role of technology in facilitating surveillance or the (absolute) power of the state in imposing it.

The role of culture, in its broad sense, is of particular importance in understanding how surveillance is perceived and functions, as it is also mediated by specific knowledge systems and epistemological traditions. It shall be acknowledged that the vast majority of the literature that informs the field of surveillance studies bears Western perceptions to surveillance, even though the field is slowly expanding to include non-Western scholarship (Lyon, 2022). Thus, when scrutinising, for example, China's (see, e.g., Hou, 2017; Liu, 2021; MacKinnon, 2011; Stockmann & Gallagher, 2011; Vuori & Paltemaa, 2015) developed systems of surveillance, one should take in consideration how the perceptions of the personal and the collective, and those of the public and the private, are informed by the Confucian or Buddhist cultural traditions, in the country (Ess, 2014, pp. 245-250; Lü, 2005; Hansen & Svarverud, 2010; Nakada & Tamura, 2005).

The scholarly interest on privacy, more specifically, which informs a significant part of the discussions on surveillance, bears largely North-western understandings of privacy. For example, Tavani's (2013, pp. 135-136) broad typification identifies three main types of privacy (of which the first and the third are more directly related to considerations of surveillance): i. accessibility privacy, known also as the right to "being let alone" or being free from intrusion, that was presented already in Warren and Brandeis' landmark article in 1890, claiming that privacy exists as a legal right in the USA; ii. decisional privacy, which relates to the freedom in one's personal choices and decisions, such as contraception, abortion and euthanasia; and iii. informational privacy, which concerns individuals' ability to control information about themselves, that they consider to be of personal nature (Ess, 2014, p. 72). This rights-based typology corresponds to contemporary Western understandings of privacy, but could lead to a condemning evaluation of privacy concerns and practices, in, e.g., non-Western environments and contexts, in rural environments, in highly impoverished areas, or in privacy evaluations of past periods.

The cultural dimension of surveillance shall be considered also under the prism of institutional politics, and the traditions the latter creates. For example, scholars highlight how institutional perceptions and policies of surveillance, in countries of Central and Eastern Europe that have a communist past, are not entirely free from prior communist regimes' logics and culture of organisation, despite conscious efforts to disconnect from the past (Łoś, 2003; Svenonius & Bjorklund, 2018; Svenonius & Tarasiva, 2021).

2.2 State, corporate, public and private actors in surveillant practices

The academic literature on surveillance largely addresses issues that pertain to state-citizen relations and corporate-consumer relations, and their diverse combinations and variations, identifying also rights and duties of the different parties in these relations. These identifications are further intertwined with diverse approaches to benefit and harm – who is harmed and who benefits from surveillance. What is noteworthy, is the state-corporate interaction and collaboration in surveillant practices (Costanza, 2018, p. 104; also, Campbell & Carlson, 2002), contrary to the belief that the state/public/non-profit sector and the corporate/business/for-profit sector engage in largely opposing positions as it concerns surveillance, representing competing interests.

2.2.1 State surveillance

Zooming in on the role of the state, among the main arguments of state surveillance are efficient policy and governance, together with security and protection of the state and its subjects. Systematic data collection and the creation of national databases allow the state to offer to its citizens the services and benefits they are entitled to, as it concerns social welfare (social security, health, education, etc.), and protect the citizens against violence and crime (Clarke, 2005; Koskela, 2000). At the same time, this type of governmentality[3] enables social

[3] For Foucault (2007, p. 108), governmentality can be understood as "[t]he ensemble formed by the institutions, procedures, analyses and reflections, calculations, and tactics that allow the exercise of this very specific, albeit very complex, power that has the population as its target, political economy as its major form of knowledge, and apparatuses of security as its essential technical instrument". Verde Garrido (2015, p. 159) argues that "[g]overnmentality employs knowledge based on political economy to establish the logics and forms of governing that will most optimally exert power over the population through the deployment of apparatuses of security". Biopolitics, or biopower, is among the control apparatuses of

control, and allows for the discrimination against 'undesirable' or 'problematic' citizens, and the exclusion of 'illegal' subjects as non-citizens (Bauman, 2004), through a systematic and even "forcible isolation of people who are different" (Richmond, 1994, p. 206), imposing de facto "segregation and expulsion" (Hintjens, 2013, p. 89). Such processes and practices are systematically enforced, for instance, in anti-migration policies in Europe (Albrecht, 2002; Broeders, 2007; Engbersen, 2001; Engbersen & Broeders, 2009; Topak, 2019; 2014; Topak & Vives, 2020) and in the USA (Coutin, 1993; Koskela, 2011; Newell, 2017).

Facilitated by enhanced technologies and artificial intelligence (AI), which are critiqued for algorithmic bias and unaccountability (Monahan & Murakami Wook, 2022, pp. 327-328), both state and corporate actors develop massive biometric databases on individuals, which are shared for state, corporate and profit-related purposes, profiling people, categorising them as prone to violence and crime, as suitable or unsuitable, entitled or not entitled to have access to services, benefits, goods, or to cross-border movement (Broeders, 2007; Engbersen & Broeders, 2009; Hintjens, 2013). For Lyon (2003), surveillance enables a deeply unjust "social sorting": "Surveillance today sorts people into categories, assigning worth or risk, in ways that have real effects on their life-chances. Deep discrimination occurs, thus making surveillance not merely a matter of personal privacy but of social justice" (p. 1).

The dangers that surveillance poses for democracy, social justice and the rule of law have been recurrently addressed by critical scholars (Costanza, 2018; Monahan & Murakami Wook, 2022, p. 327; Taylor, 2002). Western democracies are equipped with legislations that restrict the use of surveillance practices against their citizens (Taylor, 2002), as these practices are seen as infringing various freedoms and rights. Still, in circumstances where public safety is considered to be at risk, and the state claims that it needs to protect itself and its subjects against external and internal threats and enemies, state authorities have "enhanced ability to collect detailed information on potential threats to society and take preventive measures" (Costanza, 2018, p. 99; also, Coleman, 2004), even without judicial permission, which raises serious concerns related to privacy, civil rights and due process (Cockfield, 2003; Costanza, 2018, p. 99; Freeman, 2006; Richards, 2012; Strossen, 2007).[4]

governmentality, disciplining the populations through policies that regulate the individuals' bodily autonomy (Foucault, 2003; 2008).

[4] The USA PATRIOT (Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) Act, and a series of related laws, following the terrorist attacks in the USA, on 11 September 2001, granted increased powers and jurisdiction to the US law enforcement and counterterrorism agencies (NSA, CIA and FBI) in domestic surveillance, between 2001 to 2016. The Act and its related laws received considerable criticism, for their violation of basic human, civil and democratic rights, especially after Edward Snowden, a former CIA

One other area of investigation concerns state surveillance by authoritarian regimes, aiming to maintain control and curb resistance by oppositional and democratic forces. A lot of efforts concentrate on efficient internet control, with strategies ranging from "totalitarian surveillance" (Akbari & Gabdulhakov, 2019, p. 224), as in the case of Iran –which applies a series of preventive, interceptive and reactive measures (Robertson & Marchant, 2018, p. 26) aimed to repress internet use (Akbari & Gabdulhakov, 2019, p. 225)– to Russia's "strategic surveillance" (Akbari & Gabdulhakov, 2019, p. 226) –which focusses on platform ownership and legislation, aimed at banning 'hostile' platforms and curbing the freedom of expression. Still, one needs to be careful not to focus exclusively on online surveillance and control, but to examine how authoritarian states develop complex surveillant assemblages (Haggerty & Ericson, 2000) of official and non-official actors, organisations and entities, being engaged in online and offline spaces and activities (Akbari & Gabdulhakov, 2019). These surveillant assemblages are supported by organised disinformation, trolling and spying campaigns and practices by non-state and private, online and offline actors (Arteaga, 2017; Lubbers, 2015; Nurik, 2022; Treré, 2016; Yesil & Sözeri, 2017), where offline surveillant networks and practices are equally important in efficient surveillance and control, and are developed not only by authoritarian states, but also by liberal democratic states.

2.2.2 Corporate surveillance

As previously mentioned, one main area of investigation in surveillance studies scrutinises the role of corporate actors, and the broader implications of corporate surveillance for societies (Gandy, 1993). The latter "refers to the organizational practice of monitoring employees, customers, or other corporations to gain tactical and strategic information that will help to further corporate value, sales, and profits" (Costanza, 2018, p. 95).

This strand of scholarship, focussing especially on digital and online platforms and environments, and engaging in critical theory and political economy approaches, describes the contemporary conditions of corporate surveillance through terms such as data capitalism, platform capitalism, surveillance capitalism, dataveillance, etc. (Degli Esposti, 2014; Fuchs, 2014, 2013; Zuboff, 2015; 2019; 2020). These scholars address the exploitative relations the capitalist logic imposes between the powerful telecommunications and media companies that function as monopolies or oligopolies, and the media users/ consumers/

contractor, leaked in 2013, NSA documents that revealed extensive surveillance by the NSA on US citizens (Constanza, 2018; Dencik et al., 2016; Greenwald, 2014; Lyon, 2014).

citizens, and the broader implications of the fundamentally unequal power relations for societies and democracy. [5]

These scholars argue that the users' produced content and behaviour online are harvested to a large degree without the users' knowledge or consent, by corporate actors, who process, reuse and sell these data to third parties (state and corporate) (Fuchs, 2010, 2014). Through these practices, companies not only make profit at the users' expense, but also expose the latter to a series of risks caused by the separation of people and the data they produce, risks which go far beyond privacy harms (Barocas & Nissenbaum, 2014; Degli Esposti, 2014; Fuchs, 2011; Lyon, 2003; 2007; Matzner, 2014; Nissenbaum, 2010; Stalder, 2002; Zuboff, 2015).

It is argued that the increasingly "asymmetrical personal data accumulation" (Cinnamon, 2017, p. 621) of surveillance capitalism, and the "injustices of maldistribution in which data subjects are dispossessed of an increasingly valuable material good, their personal data" (Cinnamon, 2017, p. 621), render people weak, as they are deprived of the agency associated with the ownership of their own data. Hence people are exposed to the risks of misrepresentation and discrimination (Pasquale, 2015; Tene & Polonetsky, 2012), rendering them also "voiceless to challenge any illegal or inappropriate use of their data" (Cinnamon, 2017, p. 622).

2.2.3 Labour surveillance

One field that may involve either state or corporate surveillance is labour surveillance. This form of surveillance has historically been an apparatus employed in the workplace in order to discipline labour, that is to ensure that workers are effectively performing labour tasks according to managerial goals (Newlands, 2021). Workplace surveillance has assumed different forms, from installing cameras and other recording devices in factories and offices, to demanding specific productive quotas from workers within shifts. The spread of digital platforms gave rise to new forms of work associated to casualisation, free-lancing and flexibility, as platform workers can receive income as couriers, taxi drivers, short term

[5] The General Data Protection Regulation (GDPR), adopted in 2016 regulates at the EU level basic features and dimensions of privacy and processing of personal data by companies and third parties, aiming to enhance individuals' control and rights over their personal data. Still, as scholars point out, in conditions where users have limited agency in how to access, navigate and use the online platforms and environments, corporations find ways to harvest data from the platforms' users (Helm & Seubert, 2020), given also GDPR's failure to effectively regulate data transparency (Schade, 2023) and to address the implications of AI (Paal, 2022).

rentiers, language teachers and so on, in the context of the so-called ‘gig economy’ (Woodcock & Graham, 2020). Apart from accelerating labour insecurity, these work regimes develop control and surveillance tools to force workers to adjust their working practices to the requirements and business models of digital platforms.

The conditions and processes of subjectivation associated with platform surveillance and control is a growing field of study that has attracted the interest of critical scholars, policy-makers and labour activists (Trappmann et al., 2020). As scholars explain, worker surveillance and control in platform economies is imposed in various ways, direct and less direct (Sadowski, 2020), and occurs in the context of a customer-centric, ‘gig economy’, which refers to piecemeal and fragmented labour, typically without a stable salary and security guarantees (Vallas & Schor, 2020; Veen et al., 2019; Woodcock & Graham, 2020; Zuboff, 2019).

A less direct instrument of worker surveillance and control is, for instance, the user reviews and the ranking systems, according to which the customer evaluates the worker for their service. With less stars and more negative comments a worker will have less income or even stay jobless. These instruments then discipline the worker to the customer's desire, as, in other words, the customer immediately ‘supervises’ the worker. There is also a more direct surveillance system in platform work related to the disciplining function of algorithms. The algorithms processing data from the mobile phones of platform workers can “determine the allocation, remuneration, chastisement and sometimes even the termination of human labour” (Newlands, 2021, p. 720), disciplining thus flexible labour to mandate productivity. Examining these labour regimes in a food delivering eating app, for instance, Gregory and Sadowski (2021) argue that couriers need to control their physical movement and bodies to the app’s surveillance techniques, growing what they call “perverse virtues” under the mandates of flexibility, vitality and legibility.

In platform supervision, customer surveillance in the form of stars and reviews described above is most often combined with the algorithmic surveillance to ensure labour effectiveness and reliability (Newlands, 2021). In this sense, platforms introduce a regime of control that corresponds to the increasing shift to labour mobility and remoteness. This shift concerns a process entailing the de-spatialisation of labour from physical sites controlled by the company or organisation (e.g., factories, offices) and its re-spatialisation to heterogeneous sites ranging from workers’ homes to the urban space at large.

2.3 Trust and responses to surveillance

Apart from the actors and types of surveillance, another broad area of scholarly attention concerns how surveillance is perceived by people, and how people respond to it. Before addressing people’s responses to surveillance and their practices of resistance, special attention needs to be paid to one key element in the formation of these perceptions and practices, which is trust. Trust is seen as “a primary constituent of the relational dynamic of most surveillance systems” (Ellis et al., 2013, p. 1). It can generally be understood “as the belief and confidence on the part of a person or party (trustor) that another person or party (trustee) will reliably do what they have stated” (Verde Garrido, 2021, p. 223). Scholars identify different types of trust, such as institutional trust (trust in institutions), generalised social trust (trust in fellow human beings and societies in general), and particular social trust (trust in family, friends, neighbours, community) (Björklund, 2021, p. 188; Newton & Zmerli, 2011).

When it comes to surveillance, the attention is usually to aspects of institutional trust, which is evaluated through diverse measurements and evaluators of trust. For Saulnier (2017), it “involves evaluating the perceived intentions of authorities, specifically, reasonableness and benevolence” (p. 292). The institutions that are often considered in such evaluations of trust are the government, the police, intelligence agencies, tax agencies and courts (Björklund, 2021, p. 188; Svenonius & Björklund, 2018).

Empirical studies based on social surveys have found a positive correlation between trust in public institutions and tolerance or acceptance of surveillance (Friedewald et al., 2016; Pavone et al., 2015). As Björklund (2021, p. 183) puts it, these findings show that “trustful citizens allow state authorities to monitor them; or, formulated in a more pejorative way, citizens give legitimacy to (trust) governments, which in turn distrust their citizens”. Similarly, as indicated by Davis and Silver (2003), “trust in government is a crucial permissive condition for allowing the abuse of civil liberties through surveillance” (Viola & Laidler, 2021, p. 10), as “high levels of trust in government make citizens more likely to cede their civil liberty protections and accept government surveillance practices” (Viola & Laidler, 2021, p. 10). Therefore, scholars point to a paradoxical dynamic, where “too much trust can enable the very kind of exploitation and abuse that leads to its erosion” (Viola & Laidler, 2021, p. 10).

On the other hand, low levels of political trust can be seen as a “vital component of maintaining liberty in democracies” (Hall, 2021, p. 50) and may be connected to greater citizen involvement and political engagement (Kaase, 1999), involving the polity in healthier forms of democratic governance, generating trustworthy democratic institutions (Sztompka, 1998; Verde Garrido, 2021). At the same time, there are indications of increasing forms of enhanced general distrust towards the state and major institutions, including the media, science, education and contemporary forms of liberal democracy, which take a fullscale antisystemic character. The people who experience such high levels of institutional distrust share beliefs of being subjects of powerful panoptic surveillance[6], which they attempt to resist or escape through community building with likeminded people, in online and offline echo chambers where they share conspiracy theories and disinformation (French & Monahan, 2020; Marwick & Lewis, 2017), engaging at times in coordinated action. In these cases, these echo chambers seem to be functioning as communities of trust, covering the lack of trust towards the institutions.

2.4 Agency and resistance to surveillance

Scholarly explorations of how surveillance is experienced by citizens tend to consider the latter as the objects or recipients of surveillance. Still, as researchers have pointed out, the primary or exclusive focus on top-down institutional aspects of surveillance overlooks people's experiences of surveillance, their resistant practices, but also their own engagement with surveillant practices (Haggerty & Ericson, 2000; Jansson, 2012; Mann, 2020).

As Jansson (2012, p. 413) argued, "social subjects are drawn into the systems of surveillance [also] through their own desires […] for control, self-expressivity and voyeuristic entertainment". For the author, such practices reflect people's fundamental desire, in late modern societies, "for ontological security and social recognition" (p. 415). It is hence limiting to address the issues and aspects of surveillance through a narrow prism regarding people passive recipients of surveillant practices. To address these complexities, scholars introduced a series of concepts having as a starting point the term "veillance", which is understood as "purposeful sensing" (Mann, 2020, p. 265). They refer, for instance, to "coveillance", defined as "the side-to-side gaze between peers via social media and the like" (Mann, 2020, p. 265; Mann et al., 2003), or "interveillance" referring to "people's mutual practices of mediated expressivity and control, through for example online networking and content circulation" *(*Jansson, 2012, pp. 414-415). Still, one needs to be careful not to argue that the practices of coveillance or interveillance neutralise state/administrative and corporate surveillance, underestimating the force of the latter, and the fundamentally unequal relations of power that they develop.

Surveillance implies unequal, exploitative or extractive relations of power, which need to be scrutinised in explorations of surveillance (Fernandez & Huey, 2009). At the same time, these relations shall not be taken for granted, or be considered unchanged, cemented in fixed positions where the powerful surveils, and the weak is being surveilled, in a panoptical logic[7].

[6] See in Holm (2009) how a logic of paranoia facilitates such attitudes.

[7] Michel Foucault's seminal work *Discipline and punish: The birth of the prison* (1977) (originally published in French, in 1975, with the title *Surveiller et punir: Naissance de la*

Giddens (1984, p. 16) elaborating on the "dialectic of control in social systems", identified "regularised relations of autonomy and dependence between actors or collectivities in contexts of social interaction" arguing that "all forms of dependence offer some resources whereby those who are subordinate can influence the activities of their superiors". Put differently through Foucault's (1990, p. 95) emphatic statement, "[w]here there is power, there is resistance".

Guided by a review of the dictionary definitions of resistance[8], we can define the latter as: the act or power of opposing, withstanding or fighting against something; the ability not to be affected or harmed by something; refusal to accept or comply with an idea, plan, or action; a force that acts to stop an action. Processes and practices of resistance involve, in some combination, action and opposition, intentional or not, recognised or not (Hollander & Einwohner, 2004; Martin et al., 2009, p. 214). When it comes to resistance to surveillance, it can be described as the act or power of opposing, refusing or fighting against the systematic and/or routine monitoring of behaviour and activities, and the gathering and analysis of personal information.

History has shown that in all systematic or extensive practices of surveillance, there are developed practices of resistance (Hollander & Einwohner, 2004; Martin et al., 2009). In effect, both surveillance and resistance to surveillance are constitutive of contemporary societies (Giddens, 1984), and as Martin and his co-authors (2009, p. 216) argued, "resistance is not merely an epiphenomenon of surveillance – it is a basic and necessary co-development of surveillance, existing in many forms that often go unrecognised". Both surveillance and resistance are "situational, contextual, and historically specific" (Fernandez & Huey, 2009, p. 200), dependent on the power dynamics at play each time (Marx, 2003; 2009).

prison) has been highly influential in surveillance studies. Foucault's analysis of Bentham's panoptic prison, seen as exemplary in surveillance architecture, has been used extensively to describe state or government surveillance as a primary disciplining method in contemporary capitalist societies, with scholars both adopting the panopticon metaphor and addressing its limitations when it comes to the contemporary dynamics of surveillance (Dupont, 2008; Haggerty, 2006; Haggerty & Ericson, 2000; 2006; Lyon, 2006; 2017; Wood, 2003).

[8] See e.g.: https://www.merriam-webster.com/dictionary/resistance; https://dictionary.cambridge.org/dictionary/english/resistance; https://www.macmillandictionary.com/dictionary/british/resistance#resistance__11; https://www.oxfordlearnersdictionaries.com/definition/english/resistance?q=resistance

One needs to be careful not to either overestimate or underestimate the force or impact of resistance to surveillance, as both surveillant and resistant practices respond to each other, often in the form of counter-practices. Also, it shall not be forgotten that usually resistance responds to existing practices of surveillance, appearing thus with some delay, as a defensive mechanism, even if pre-emptive strategies are sometimes developed. Still, the power relations between the surveyor and the surveilled are “mobile, reversible, and unstable” (Foucault, 1997, p. 292), and the surveilled has some agency, albeit limited at times.

Resistance to surveillance may be formal, organised, largescale, long-term, but also informal, unorganised, everyday, trivial, ad-hoc and discontinued (Fernandez & Huey, 2009; Marx, 2003; 2009), and may involve “resistors other than the subjects of surveillance” (Martin et al., 2009, p. 217; see also Gilliom’s (2001) and Scott’s (1987) work on ‘peasant resistance’, as cited in Martin et al., 2009). McCahill and Finn (2014, p. 4), drawing on Pierre Bourdieu, introduced the concept of “surveillance capital” to describe “how surveillance subjects utilize the everyday forms of tacit knowledge and cultural know-how that is acquired through first-hand experience of power relations to challenge the very same power relations”. Resistance to surveillance can take many forms. Scholars have been describing processes and practices of counter-surveillance (Monahan, 2006; Huey et al., 2006), meta-surveillance (Introna & Gibbons, 2009), surveillance neutralisation (Marx, 2003; 2009) and sousveillance (Fernback, 2013; Mann, 2004; Mann et al., 2003), to name a few.

Surveillance neutralisation (Marx, 2003; 2009), involves non-compliance to, and interference with, the surveillance practices and artefacts, and is expressed through activities such as avoiding, blocking, distorting, masking, breaking, refusing, and counter-surveilling, and can take place in the workplace, the marketplace, in government and interpersonal relations. “Sousveillance is a form of inverse surveillance in which citizens monitor the surveillors as a means to challenge the surveillance state” (Fernback, 2013, p. 14), by maintaining watchdog web sites or blogs, or monitoring corporations, the military and the government, and exposing the surveillant, unethical and illegal practices of the latter (Mann, 2004; Mann et al., 2003). “Sousveillance embraces the idea of transparency as an antidote to concentrated power in the hands of surveillors” (Fernback, 2013, p. 14), empowering individuals “as active producers of ‘observed’ discourses, images, and data rather than as mere victims of panoptic or synoptic surveillance” (Fernback, 2013, p. 14).

Certain critical scholars argue that the understanding of surveillance as “a party for two”, “an exclusive relationship between the surveyor and her subjects” (Martin et al., 2009, p. 215), “not only ignores some of the actors who resist surveillance, but also excludes the assemblages that conduct the surveillance” (Martin et al., 2009, p. 215). Moving thus away from the exclusive focus on the surveyor–surveilled relationship (Fernandez & Huey, 2009; Martin et al., 2009), these scholars propose to study resistance through multi-actor, multilevel frameworks that allow to sketch resistance assemblages, identifying diverse actors that are engaged in the resistance of surveillance –individuals, groups, institutions, networks– but also "governmental actors at various levels of organisational complexity, surveillance enforcers and technological artefacts" (Martin et al., 2009, p. 222), commercial actors, international actors, trade unions, etc., engaged in complex, multi-directional relationships of surveillance and resistance. This approach allows also to identify non-human actors in these complex relationships, and, informed by actor-network theory (Latour, 2000; 2005) that attributes agency to technology, to consider technology as a potential actor of resistance, to, e.g., intended technological applications by humans.

2.5 Techno-optimism and techno-pessimism in visions of surveillance/resistance

The debates around the force and implications of surveillant practices for individuals and societies, and around the possibilities for resistance are intertwined with specific approaches concerning the role and force of technology, given that surveillance is largely enabled through technological applications and platforms. These approaches may be clustered around two main 'camps', these of techno-optimism and techno-pessimism. Techno-optimism and techno-pessimism inform different visions of how surveillance is orchestrated, enabled, performed and how it can be resisted, instructing in turn different visions of societies.

Techno-optimism relates to the belief that technology is inherently tied to (human) progress, and that technological progress leads to better societies (Königs, 2022; Ridley, 2010), being beneficial for humankind and for the planet. Techno-optimism is partly founded on technological solutionism, the belief that the key to solving societal problems lies in (humans' ingenuity to design and implement) technological applications. The idea that technological progress is the key to human and societal progress and wellbeing often echoes technological determinism, which prioritises technology over any other factors, forces and dimensions in what defines social formation. In technological determinism, technologies are seen as major agents of societal change, determining how societies will be formed and organized. It echoes "the idea that technology develops as the sole result of an internal dynamic, and then, unmediated by any other influence molds society to fit its pattern" (Winner, 1999[1980], p. 29).

When it comes to contemporary media technologies, techno-optimism is reflected in the belief shared during the early days of the internet, that the internet is an open and democratic space, fostering "new forms of direct democracy, increased participation and creativity, and the destabilization of old hierarchies of power" (Lindgren, 2017, p. 51). Negroponte's 'Being Digital' (1995) is among the early key texts of optimism concerning the digital society. His work focusses on the positive change the digital 'revolution' would bring in societies. For Negroponte, by 'being digital', societies would become more decentralised and participatory affording more opportunities for empowerment and collaboration.

Techno-centrism relates to the examination of broad societal phenomena through the prism of (certain types of) technology, positioning these technologies at the core of any associated consideration. Techno-centrism regards the specific properties of a technology -e.g., the internet or social media- as of particular importance in, for instance, how people communicate or socialise, attributing lesser or no relevance to other factors, or to other technologies. This perspective is met in the idea that older forms of technology or media will be fully replaced and die once new ones are established. This is, for example, reflected in the assumption that newspapers would disappear once radio was popularised, or that radio would die once television became popular or that all older media would die with the advent of the internet (Morozov, 2011; 2013). Focussing on *what technology does* and not on *what people, institutions or other actors do with technology*, has a series of implications. In research, this implies that scientists might disregard or downplay people's agency, or the broader socio-political and economic environment in which technology functions.

Contrary to techno-optimism, techno-pessimism relates to the belief that technological progress does not help the wellbeing of societies and that its benefits are less than its harm (Königs, 2022). Techno-pessimists tend to see technologies as harmful or destructive, and when a new form of technology appears they tend to focus on the damage it may cause to particular groups and society at large. Interestingly, something that a lot of the techno-optimists and techno-pessimists share is the belief that technology is very powerful. It can also be argued that under certain conditions techno-pessimists and technophobes attribute more power to technology than techno-optimists.

Neil Postman's 'Technopoly: The surrender of culture to technology' (1992) captures a lot of the techno-pessimist arguments and positions. The author argues: "New technologies alter the structure of our interests: the things we think about. They alter the character of our symbols: the thinks we think with. And they alter the nature of community: the arena in which thoughts develop" (p. 20). For Postman (1992), 'technopoly' describes 'the submission of all forms of cultural life to the sovereignty of technique and technology' (p. 52). This echoes earlier concerns by critical theorists and members of the Frankfurt School, Theodor Adorno and Max Horkheimer (2002[1947]), who argued that popular culture produces standardised cultural products that have lost their artistic authenticity and rigor, offered through the mass media for easy consumption, manipulating society to passivity.[9]

[9] This critique was firstly addressed in the chapter "The Culture Industry: Enlightenment as Mass Deception" of their book *Dialectic of Enlightenment (1947),* where the term 'culture industry' was introduced.

Techno-pessimism may sometimes reflect a technophobic attitude, that is expressed through fear, or aversion of using particularly new forms of technology, as the latter are seen as threatening, harmful and destructive (Brosnan, 1998). Of relevance here is also the concept of luddism. The Luddite movement, in the 19th century, concerned British textile workers who opposed the replacement of skilled workforce by cost-efficient machinery in the textile industry, by destroying the textile machines (Jones, 2006). (Neo)luddism describes today a broader stance against technology, sometimes driven by a romantic vision and desire for a simpler life, and the appeal for a return to nature without the mediation of technology (Fox, 2002), but also by ideas of (anarcho)primitivism. According to Filliss (2019), primitivism is "a counterweight to the pull of technology. Primitivism as a whole is the positioning of a counter-force to the thrust of technological progress". It argues that technology-led civilisation destroys authentic forms of social life, as well as the environment; hence the return to pre-civilisation lifestyles can lead to the liberation of humans and their reconnection with (their) true nature (Aaltola, 2010).

These techno-optimist and techno-pessimist approaches, as will be exemplified later in the future scenario analysis, feed into people's visions of the future, structuring specific imaginings of societies and their assemblages of surveillance/resistance.

3. Practices of digital surveillance and resistance in Europe: Economy, migration, gender, health and environment

Surveillance can be employed by different authorities as a governance tool for achieving short-term or long-term policy outcomes, which are often in turn subject to larger political visions of states or other authorities. In this section, we look at areas upon which surveillance has been exercised in Europe, to support particular goals, policies and political visions.

As mentioned earlier, the imperative for surveillance does not occur in a vacuum but it is often a response to what European political entities or authorities would perceive and construct as a threat, that is as an actual or future problem that concerns Europe, which has to be monitored, immediately or pre-emptively. The public understanding of a threat is subject to the ways that hegemonic and counter-hegemonic discourses frame and speak about a particular subject. The extent to which terrorism, viruses or refugee movements constitute a threat and merit surveillance, to refer for instance to some of the threats against which surveillance in Europe has been implemented, is a matter of how certain phenomena are interpreted by particular authorities. The invocation, thus, of a threat depends on the discursive articulation of specific events taking place within physical space and is always a matter of contestation by antagonistic forces (Carpentier, 2021). We should not overlook also the business opportunities that the development of surveillance equipment can afford to particular corporations (Arbogast, 2016). In this regard, an additional variable that should be taken into consideration when discussing the implementation of surveillance tools as a response to certain phenomena are economic interests and lobbying that can impact on the discursive construction of threats (see also earlier section on corporate surveillance).

As noted, insofar as a phenomenon is constituted as a threat, counter-hegemonic forces may resist or contest this constitution. In this sense, when we speak about surveillance as a tool for state-sanctioned monitoring we should recognise at least two forms of resistance against this surveillance: the possibility of antagonistic actors using similar technological affordances to evade, counter or complicate state-sanctioned surveillance, as well as the voicing of different opinions about what constitutes a threat in the public space through technological affordances. Below, we will briefly consider some areas upon which this choreography between surveillance and resistance takes shape in European space, namely in the fields of economy, migration, gender, health, and environment, which are of particular relevance to the EUMEPLAT research project.

3.1 Economy

In the economic realm, the European Union implements monitoring and surveillance strategies both at the level of individual, day-to-day transactions and at the level of the state-driven management of fiscal affairs (Laffan & Schlosser, 2016). At the level of individual entities, the allocation of tax registration numbers or VAT numbers to citizens and businesses continues to be the main tool for controlling an entity's economic profile. Yet the digital affordances turned economic monitoring much more effective and controllable. Through digital services surveillance can be implemented via e-banking services, cards, and a nationally integrated banking system that is digitally connected with the legal profile of an entity, either individual or business (Troitiño, 2023). Despite the fact that the EU does not have an integrated taxation policy (i.e., it is up to the nation states to determine it), there do exist EU governance bodies overlooking national tax regimes, including groups such as the Code of Conduct on Business Taxation that exists at the level of the Council of Ministers, and in which "EU countries assess each other's tax regimes to identify harmful tax measures" or the Tax Policy Group, which is responsible for issues of double taxation (European Commission, nd). The aim of tracking financial movements of entities is to track tax avoidance as well as maintain citizens' overall financial profiles that can be useful to banks and other financial institutions when for instance a citizen asks for credit.

In turn, at the level of macro- surveillance, EU economic bodies monitor the financial policies of countries in conjunction to the EU's overall free market policy, including the mandates to increase competitiveness, maintain fiscal stability, privatise and remove trade barriers (European Central Bank, nd; Filipiak & Wyszkowska, 2022). Many of these imperatives were decided in the 'Lisbon Treaty' in 2000 and were then updated in the 'The Europe 2020 Strategy', which are both policy documents that prescribe the economic policy for EU nation states. The absence of 'hard' integration between nation states, however, poses often a problem, as the economic reforms can be slower and more chaotic. For instance, institutions like the European Central Bank clearly want a more active and robust role for the European Council so as to implement more effectively different policies: "The Europe 2020 Strategy tries to correct these weaknesses, most importantly by giving the European Council a strong role in steering the implementation of the reform agenda and by reinforcing the surveillance of Member States' reform policies" (European Central Bank, nd).

Resistance to EU monitoring programmes of economic reforms reached a peak during the so-called European debt crisis from 2010 until roughly 2015, which pushed the economic austerity and privatisation agenda among the member states that were hit the hardest by the crisis, including Greece, Cyprus, Portugal, Italy and Spain. These fiscal austerity programmes proved to be very unpopular among the people resulting in daily demonstrations, occupations of buildings and public squares and often riots (Della Porta, 2017; Rüdig & Karyotis, 2014). Despite this popular resistance, states like Greece and Cyprus had to sign painful Memoranda of Understanding with the EU, ECB and IMF that would push neoliberal economic reforms in return for loans for covering external debts. At the level of monitoring everyday transactions electronically, resistance is more scattered and it is related to law-abiding practices or choosing alternative means of payment, such as the digital wallets or bitcoin which are more loosely regulated (Gruber, 2013; Wolf, 2014).

3.2 Migration

As geographical mobility is an essential quality defining humankind, one can imagine that the relationship between Europe, as a geographical space, and migratory movements is old, complex and has historically assumed diverse forms. Increasingly since the 1990s, this relationship is marked by types of prohibitions and surveillance techniques relying on digital technologies to oppose what the European Union perceives as migratory threats, originating especially from the Middle East and Northern Africa (Geddes et al., 2020). At least since the 2000s these movements have been varyingly portrayed by European Union officials and media outlets as potential dangers for European security, economy and culture, resulting in an intense securitisation of the Union's borders (Geddes et al., 2020; Huysmans, 2000; Karamanidou, 2015). Securitisation in the context of border control assumes different forms, including the increased presence of national border police and later the European Border and Coast Guard Agency (Frontex), responsible for halting undocumented migrants, as well as the erection of increasingly more walls around the European borders in order to prevent unauthorised crossing. Indicatively, 19 EU countries, such as Spain, Greece, Poland and more recently Finland, have erected some kind of wall in the last twenty years and between 2014 and 2022 the overall length of these border walls or fences rose from 315 km to 2048 km (European Parliament, 2022, p. 2).

Border policing and fences are technologies that directly interfere with mobility in a given geographical space, but contemporary securitisation relies to a large extent on tracking mobilities from a distance, and on digital surveillance in particular. Digital technologies (as all technologies) enable particular affordances and limitations for social actors, and in the case of migration they enable what Nedelcu and Soysüren (2022) call the "empowerment-control nexus" (p. 1827). For Nedelcu and Soysüren, technologies afford opportunities not only to border control actors that monitor movement, but also to undocumented people who embark on a journey to cross European borders. Regarding the former, digital technologies at least since the 1990s contributed to building a massive apparatus of movement surveillance that can be called "biometrics coupled with databases" (Nedelcu & Soysüren, 2022, p. 1826; see also Broeders, 2009). This can be understood as the cross-feeding between biometrical data taken from states for the issuing of documents to migrants, refugees and asylum seekers, such as fingerprints and face photos, with digital databases that store mobility information. Such examples in the European context are the Eurodac, which is a biometric database for undocumented migrants, and the Schengen Information System and the Visa Information System that ensure mobility within the EU area. These surveillance agencies rely on the digital storage and processing of information that regards individual histories of mobility so as to control who is allowed to enter the European space (Bellanova & Glouftsios, 2022)

In turn, resistance to digital surveillance can take the form of activism directly opposing border securitisation practices through the organisation of solidarity networks and online petitions (Walsh, 2010; 2013) or the usage of digital technologies by migrants themselves for bypassing security controls. Nedelcu and Soysüren, and others (e.g., Gabrielsen Jumbert et al., 2018), note how mobile digital technologies such as smartphones and social media have "transformed journeys in digitally-mediated transnational events" (Nedelcu & Soysüren, 2022, p. 1823). These technologies help refugees and undocumented migrants "to obtain vital information to accomplish their journeys successfully" (Nedelcu & Soysüren, 2022, p. 1823) via "global positioning apps, digital maps, and digital platforms through which experiences are shared within informal networks […] that allow migrants to better cope with the changing (and often hostile) social, political and economic conditions to which they are exposed" (Nedelcu & Soysüren, 2020, p. 1823). In this respect, the digitalisation of border security comes together with new forms of resistance that are enabled by digital technologies as surveillance and resistance are in this case intertwined in the empowerment-control nexus.

3.3 Gender

Under the general framework of equality and equal opportunities that the EU promotes, the EU has implemented monitoring schemes to protect women and more vulnerable groups especially when it comes to migration and labour mobility. While these monitoring schemes are not often conceptualised as surveillance, they do surveil areas of social life so as to achieve particular results. Furthermore, they rely on archiving, categorisation and digital databases that are key tools for surveillance apparatuses. On the domain of migration, for instance, Marchetti and Salihb (2017) argue that there is a "policing" of migration in EU geared towards accepting more women and vulnerable groups that has resulted to a "feminization of migration" (Marchetti & Salihb, 2017, p. 6). This is reflected in 'The European neighbourhood policy' (ENP), which was launched in 2004 "to foster stability, security and prosperity in the EU's neighbouring regions, both in the South and in the East" (EU, nd), allowing female migrants to migrate to the European space more easily than men (Marchetti & Salihb, 2015). There is a similar EU migration policy for persecuted gender and sexual minorities, such as LGBT+ people, who may face discrimination and danger in their countries (Andreassen, 2021).

While there is no organised resistance against such frameworks of 'positive discrimination', there are often critiques levelled against them. For example, Marchetti and Salihb (2015) argue that the ENP framework "reproduces gender ideologies when it restricts women's access to mobility for family reunification and participation in feminised labour sectors (e.g., domestic work)" (p. 141), and by positioning women primarily as caretakers, it reproduces a patriarchal division of labour. As such, while this framework proclaims that it wishes to promote the social and economic improvement of these neighbouring areas, it "operates a selective and strategic use of gender equality and women's autonomy but fails blatantly to enhance opportunities for women's autonomous migratory projects" (Marchetti & Salihb, 2017, p. 7). We should note here that this is not an argument about the surveillance apparatus per se, but against the policies and ideological assumptions that underpin this apparatus.

3.4 Health

Health management is another area upon which surveillance techniques are implemented in Europe, by the European Union and individual states, for the stated purpose of protecting the lives and well-being of populations. Surveillance in the area of health management has been proposed or applied for the administration of different diseases, including cardiovascular ones (Movsisyan et al., 2020), whose monitoring can have preventive results, as well as conditions that may harbour health risks, such as obesity (Spinelli et al., 2021). The most widely debated and in many ways exemplary case of health-related surveillance regards the development of an elaborate tracking apparatus to combat the COVID-19 pandemic, which acquired a global resonance and preoccupied news and public discussions from 2020 to 2022. One of the most debated and contested practices during the spread of the COVID-19 virus in the EU, was the introduction of the EU Digital COVID certificate, the so-called vaccine passport, that is, an electronic document that certifies the vaccination of a person with one of the EU-approved vaccines. The 'green pass', which was the most popular name that these vaccine passports took in the English language, was a digital certificate with a QR code whose scanning would certify that a person had been vaccinated and was thus expected to have developed antibodies against the disease. The successful scanning of the QR code involved the appearance of a green-coloured symbol (usually a tick symbol) in the scanning machine of the surveillance authority, allowing people to access an array of public services ranging from work and concerts to shops and cafés. Although different European states may have had different rules throughout the period of these two years, the COVID-19 surveillance system was integrated at an EU level, namely a vaccinated person could use it to access services throughout all EU member states.

The unprecedented COVID-19 surveillance apparatus that was employed in Europe (and the world) appeared within mainstream public debate as a positive step in order to combat the virus and return to normality. In this sense, we could argue that the COVID-19 pandemic was one of the cases where the demand for increased human surveillance in Europe was articulated as part of progressive politics. To bring an example, debates about reopening educational or other institutions after a period of prolonged lockdown were based around the assumption that an expanded surveillance system was not only necessary but desirable (Mahraj et al., 2021). The demand for increased surveillance was also a way to restart economic activity, which was stalled as a result of the prolonged lockdowns in Europe after the spring of 2020 and the biggest part of 2021. In this regard, the pandemic surveillance apparatus was further implemented in order to protect specific material interests, such as the tourist industry (Renieris, 2021).

In turn, the resistance to these measures portrayed this health-related digital surveillance as a totalitarian measure aimed at considerably threatening the freedom of the population. The movement against the green pass, for instance, perceived the obligatory vaccination as anti-democratic and organised resistance to the anti-COVID-19 measures through street demonstrations, the production of audio-visual material and other actions. Social media platforms both helped the anti-green pass movement to grow by helping it coordinate and gain visibility but also suppressed it, as a lot of the material around anti-vaccination was labelled as disinformation in most mainstream platforms, including YouTube, Twitter and Facebook (Monaci & Persico, 2023). Generally, the implementation of digital surveillance systems during the COVID-19 pandemic in Europe brought to the fore crucial questions involving how the politics of health protection, especially towards more vulnerable parts of the population, can be combined with democratic decision-making.

3.5 Environment

Similar to the previously discussed cases, the implementation of surveillance tools for monitoring the environment is typically a means for protecting society against perceived threats. Environmental surveillance involves the protection of non-human entities including land, rivers, mountains, endangered species and farm animals that are thought to be important for symbolic, ecological or economic reasons. Furthermore, environmental monitoring aims at protecting human societies themselves from human-generated environmental degradation (related, e.g., to pollution and climate change) and nonhuman threats, such as the spread of zoonotic diseases (Tiwari et al., 2023), the pests that threaten farming, and invasive species whose uncontrolled spreading in particular areas can be threatening for the balance of ecosystems (Epanchin-Niell, 2012). Finally, an area where surveillance techniques have been applied for environmental control is food, so as to certify that people do not consume food that comes from polluted areas or has been cultivated in unhealthy conditions (Tripoli & Schmidhuber, 2020).

A common method through which digital technologies can surveil and protect environmental concerns is by tracking systems that are placed in animals that are either under threat (e.g., wildlife) or themselves constitute a threat to the ecosystem (e.g., pests). Animal identifiers can take different forms depending on the purpose of surveillance and the resources of the management agency, such as notches in body parts, branding, tattoos, tags in ears, tails and other parts of the body, electronic devices such as RFID tags, (a type of tracking system that uses electromagnetic waves to identify objects), implants and electronic ear tags, DNA testing and animal passports (see Tripoli & Schmidhuber, 2020, p. 236). These animal identifiers are usually linked to an electronic database that can trace the movement or other animal behaviour and feed it with data about the particular animal population. In this sense, these databases provide raw data to environmental scientists who process it and act accordingly. Animal identification is also extensively used in livestock, cultivation and farming for producers to be in control of the movement of cattle, sheep, fish and other animals (Shroeder & Glynn, 2012). As mentioned above, apart from the protection of animals as the producers' property, surveillance of livestock is additionally practiced to ensure food safety and quality.

While resistance against animal identifiers has been voiced by animal-rights defenders, especially in the context of animal farming, it is worth noting that environmental monitoring and control have also been debated in light of progressive politics as a means to protect ecosystems. In a few cases, environmental activists have been voicing protest on the basis of individual animal rights against science-driven surveillance tactics that aim to restore ecosystem balance. Activist actors then often frame electronic surveillance as part of an overall problem (e.g., animal farming) that has to be resisted.

The framework of environmental management relies on the authority of expert institutions and the scientific community, which are typically responsible for identifying these environmental threats against which action should be taken by policymakers. The discursive constitution of an entity in need of protection from a threat, whether this entity is a geographical space, humans, or nonhumans, is again key for deploying the apparatus of monitoring and control, and making it part of official politics. As a case in point, the paradigmatic entity in need of protection in the framework of the Anthropocene, a period when there is intense human-induced environmental degradation, is planet Earth. To that effect, the European Union approved agreements, such as the Paris Agreement in 2015[10] or the European Green Deal in 2020[11], for taking comprehensive environmental action, including the reduction of carbon emissions and the elimination of greenhouse gases by 2050. Apart from investing in 'green' energy, the implementation of such policies requires the monitoring of different economic activities, including industrial production and the soil used for agriculture.

The 8th Environment Action Programme, entered into force in 2022[12], is the EU's legally agreed common agenda for environmental policy until 2030. This legally binding agenda, which addresses a broad range of areas such as climate change, biodiversity, (soil, water and air) pollution, water management, sustainable production and consumption, etc., incorporates a complex system of monitoring and control for the member states, involving national authorities and independent EU inspecting authorities. One of the instruments the EU uses is the European Earth Observation Programme (Copernicus)[13], which provides satellite observation data on land, marine, atmosphere and climatic conditions, used among others, in the implementation of EU's Common Agricultural Policy. Another monitoring system is the European Pollutant Release and Transfer Register (E-PRTR)[14] which provides environmental data concerning the air, water and land, from thousands of industrial facilities in the EU and other European countries. Despite the ambitious goals set through EU's environmental policy, a set of factors related to diverging priorities by the member states, pressing lobbying interests, and delays and inconsistencies at the national and European levels, have rendered the EU environmental policy more successful in monitoring and registering pollution, degradation and climate change, than preventing it and halting some of the trends of environmental destruction (Hermoso et al., 2022; Knill & Lenschow, 2000).

[10] See https://www.consilium.europa.eu/en/policies/climate-change/paris-agreement/

[11] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1588580774040&uri=CELEX%3A52019DC0640. See also https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal_en

[12] http://data.europa.eu/eli/dec/2022/591/oj

[13] https://www.copernicus.eu/en

[14] https://environment.ec.europa.eu/topics/industrial-emissions-and-safety/european-pollutant-release-and-transfer-register-e-prtr_en

4. What has the EUMEPLAT research added to these debates?

This section addresses a reflection on the EUMEPLAT research and its relevance for surveillance/resistance. To this aim, all reports, collected data and other analyses, that were part of the project's work package deliverables (WP1-WP4), were scrutinised for the identification of findings that bear some relevance to surveillance, control, discipline and/or resistance to surveillance, control, discipline, in Europe, in/through communication platforms. This systematic review brought to the fore a series of issues, dimensions and debates, pertaining to surveillance and resistance to surveillance, facilitated through communication and media platforms across Europe.

4.1 Policy and regulation concerning data management and privacy

In WP1 (T1.4.-D1.4), Volker Graasmuck and Bárbara Thomas (2022) present a detailed overview of the European media policies and legislation between 1990 and 2020. Among these, the EU legislation on data protection that includes the 'Data Protection Directive' (1995) and the 'General Data Protection Regulation' (2016) are of special relevance to issues regarding (digital) platform-enabled surveillance and protection from it.

The strategic principles related to the concern about data protection and personal privacy are referenced already in the 'European Convention on Human Rights' (1950) and the 'Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data' (1981), as well as in the 'Charter of Fundamental Rights of the European Union' (2000), from which 'Article 7. Respect for private and family right' and 'Article 8. Protection of personal data', are of particular relevance. These early provisions show that in Europe privacy has been considered a fundamental human right that merits protection since the early days of European integration, and that data protection is an integral component of it.

The first legislative measures date back to the mid-1990s with the 'Data Protection Directive' (1995). Among its main measures, and in relation to the aspect of surveillance and protection from it, the following articles are of particular relevance: (1) The Protections of individuals with regard to: a) The processing of personal data, and b) the free movement of such data; (2) The concepts of the controller, the processor, and the recipient of data; (3) The principle of the data subject consent; (4) The right to privacy versus freedom of information/of expression (journalism…); (5) The right of access/ the right to rectify the data; (6) The regulation around the algorithmic treatment of data: decisions taken by an algorithm must be subject to human review if it can produce legal effects to a subject; (7) Transfer of personal data to a third country (Art. 25; 26). These articles point to: an (individual) rights-based approach to privacy; an approach to data protection that includes the aspect of data control or management by the individual/the 'producer' and by third parties; the attempt to balance data protection and freedom of expression; and, the attempt to address already in the 1990s the challenges arising from the full digitisation and algorithmisation of information and data.

Two years later, the 'Directive concerning the processing of personal data and the protection of privacy in the telecommunications sector' (1997) was born. This directive regulated, among others, the confidentiality of communications and the exceptional cases in which listening, tapping, storage or other types of interception or surveillance of communications are permissible (national security, defense, public security, and the prevention, investigation and prosecution of criminal offenses). There is a clearer emphasis in this directive on the connection of privacy and data protection, but also the legitimation of state surveillance, at the EU level, identifying areas of national interest, public safety and security.

As technological advances and the adoption of European Union directives in this field progressed, it became necessary to update and implement new legislative measures related to the protection of personal data. In this way, in the 2000s, the 'Regulation on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data' was adopted, by which an independent supervisory authority was established, namely the European Data Protection Supervisor (EDPS) (2004). The role of the authority has been to monitor and ensure that European and Community institutions respect the right to privacy and data protection.

Of relevance is also the 'ePrivacy Directive' (2002) (*The 'cookie Directive')*. It extends to video-on-demand services as well as public services on public networks. With the rise of the internet and the consequent proliferation of cookie consent pop-ups, it was deemed necessary to regulate this field as well, based on the reasoning that the terminal equipment of users of electronic communications networks and any information stored on it are part of the users' private sphere requiring protection under the European Convention of 1981 (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data). The provision of data retention is important in this regard, based on which data must be deleted when no longer necessary for the given purpose (article 6).

Finally, the 'General Data Protection Regulation' (GDPR) of 2016, applicable in 2018 in all EU member states, addresses and updates some of the clauses of the 'Data Protection Directive' of 1995, aiming to harmonise data privacy laws across the EU and to safeguard the privacy of data of EU citizens. This regulation defines more elaborately the areas of data protection, data security, data subjects' consent, and data subjects' privacy rights. The data subjects' rights include the right to be informed, the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object, and rights in relation to automated decision making and profiling. Among the new measures adopted, the ban on data transfers from the European Union to the United States stands out. Likewise, some rights were introduced, such as the right to erasure (or the right to be forgotten), which consists of the right to have private information on individuals which is available in online search engines and other directories, deleted under certain conditions.

The range of applications under GDPR, for which citizens' data shall be protected, is particularly broad, expanding much further than the user-related or user-generated data produced on online platforms (web sites, social media, user applications (apps), tracking applications (cookies), etc.). It applies, for instance, in the case of medical data stored by health-related public and private companies, and covers platforms and services such as bank/credit cards, loyalty cards in shops, micro social networks, listening/micro/voice control permissions (screens and applications), cameras in public spaces, etc. etc. In short, the GDPR applies to all entities processing personal data of EU citizens or residents, or offering goods or services to such people, even if they are not based in the EU. Due to its broad scope and strict provisions in terms of fines for entities that violate the GDPR, the latter is seen as a pioneer regulation and a model to follow by countries outside the EU and Europe that aim to enhance individuals' control and rights over their personal data.

Apart from the EU media and telecommunications sector regulation as it concerns audience/user privacy and data protection, some of the regulatory policies and actions focus on supervision and monitoring of content for the protection of the general population or of vulnerable groups. For instance, the 'Audiovisual Media Services Directive' (2018) adopts measures to monitor the content broadcast by both linear and on-demand audiovisual communication services, as well as the advertising broadcast in them. This directive aims to protect minors from harmful content, and the general public from incitement to discrimination, to hatred or violence against a group or members of a group, and terrorism, based on the grounds mentioned in Article 21 of the Charter of Fundamental Rights of the European Union, or from the dissemination of content that constitutes a criminal offence under EU law.

The reasoning behind these provisions is that these services (linear and on-demand) are used to share information, entertain and educate the general population, in particular through access to programmes and user-generated content (in the case of on-demand services and social networks). From the perspective of the legislator, it is important to protect the citizens, in this case by regulating the power of companies and states that control and use data, as well as the power of media organisations that inform, entertain, and influence people's opinions. This power must be accompanied by the responsibility to guarantee the fundamental rights of citizens and to protect minors from content that may affect their physical, mental, or moral development. It is also important to protect the general population and vulnerable groups in particular from messages (commercial and non-commercial) that may put them at risk or harm them.

4.2 Surveillant practices by media platforms and user resistance

4.2.1 Video platforms' surveillant practices

For the purposes of WP3 that studied patterns of platform video production and consumption in the ten EUMEPLAT partner countries, all EUMEPLAT partners collected and analysed data from big global platforms, such as YouTube, Instagram, TikTok, Netflix, HBO, Disney+, Amazon Prime, Apple TV and Google Play (see Boshnakova et al., 2023a; 2023b). The analysed data point to certain reflections as to how these platforms engage in surveillant practices by collecting and processing user data, aiming to improve, as they argue, their provided services and enhance user satisfaction, and ultimately enhance their profitability.

The platform users, for their part, are aware that these platforms collect data about their behaviour, preferences and choices, and accept the platforms' operation and conditions, to get better and easier choice - what to watch, to listen and to consume as a whole. Netflix, which is the most popular video on demand (VOD) platform in all ten EUMEPLAT partner countries, mentions on its web page: "Whenever you access the Netflix service, our recommendations system strives to help you find a show or movie to enjoy with minimal effort".[15] There are two key aspects for the consumer in this statement – 'enjoy' and 'minimal effort'. For the enjoyment received with minimal effort, consumers yield the information concerning their viewing preferences and activity to the platforms, with no knowledge about how their data is collected and processed and how the platforms use that data.

All platforms have their own systems to collect data from consumers and to offer them content which satisfies their preferences. As these recommendations systems feed from users' viewing behaviour, it is very difficult to promote a film, TV series or any video content in a genre or format different than the preferences of the user. That is where European video content fails. The platforms are global, and working in a similar fashion with the Google search engine, the propositions for new titles are those watched by the highest numbers of users all over the world. So, the platforms in most cases recommend to the users the "trending" titles all over the world. That is why in all platforms for VOD the top ten films and TV series are nearly the same in all ten EUMEPLAT partner countries. Thus, European content is not recommended very often to the users. When European content is

[15] How Netflix's Recommendations System Works, https://help.netflix.com/en/node/100639, accessed on 29/06/2023

recommended by these platforms, it concerns in most cases co-productions by the platform and European producers – an example is ‘Money Heist’ for which Netflix acquired global streaming rights in late 2017.

Amazon Prime Video has a recommendations system too. Amazon’s engineers tweak its content recommendation algorithms, and apply this knowledge on new titles to recommend the latest releases (Roettgers, 2019). This is clearly a trend in all VOD platforms, which have similar systems for recommendation, and they all focus their efforts on newly released content. As an outcome, the most watched films and TV series on these platforms are all produced in the last few years.

In order to increase cultural diversity and promote European content, the updated, in 2018, EU legislation concerning the provision of audiovisual media services proposes that 30% of the content of TV channels and VOD platforms is European. This requirement concerns EU productions and co-productions with European countries that have signed the European Convention on Transfrontier television (European Parliament, 2018). The platforms easily fulfil that condition with European films and TV series produced not only in the last years, but also in the 20th century. Still, the recommendations systems do not find that content to be attractive for users.

The situation is different for the visual storage platforms (VSP), as in most cases users consume content produced from other individuals. In these platforms, language is the main criterion of user selection, with humour, comedy and personal life being the most watched genres. As it concerns TikTok, the highly popular short-video hosting platform, there is controversy with governments in Europe and not only, for issues of cybersecurity. On 23 February 2023, the European Commission stated: “To increase its cybersecurity, the Commission’s Corporate Management Board has decided to suspend the use of the TikTok application on its corporate devices and on personal devices enrolled in the Commission mobile device service”. Regardless of the cybersecurity dispute, TikTok is the most ‘national’ platform in the EUMEPLAT research, as the format and the topics of the videos make the platform a preferred channel for young people to express themselves in their own language.

Resistance from users against the monitoring of their viewing behaviour in these platforms is rather limited. For example, users use Ad Blockers or the paid version, in these platforms, to skip advertisements, as the subscription fees in most VOD platforms guarantee advertising-free content to watch. This can be seen more as a form of agency to control unselected or undesired content, than a strategy of resistance against the platforms’ surveillant practices. Netflix’s and other platforms’ options for users to have their viewing history entirely deactivated as a strategy to avoid being surveilled, is in practice of limited effect. For example, Netflix has the option to hide one’s viewing history, but it may take up to

24 hours for a hidden title to be removed from all user devices, while titles accessed from a Netflix Kids profile cannot be hidden.[16] Furthermore, as soon as the users start watching again, they are given recommendations based on their latest viewing behaviour. Moreover, Netflix requires cookies enabled in Google Chrome and other web browsers to stream videos using these browsers,[17] making it in practice impossible to watch Netflix videos using these browsers, unless cookies are enabled.

Creating more (opportunities for) visibility for European content on these platforms is something to strive for. At the same time, more user-friendly transparency as it concerns how users' data connected to their viewing behaviour are used by the platforms, and meaningful options for opting out in tracking users' behaviour, without the users losing much of the platforms' affordances, are needed as minimal standards of protection for the platform users.

4.2.2 User resistance through piracy

One area of interest in relation to the distribution of media content and its monitoring concerns the unauthorised distribution and the attempts to control and halt it, what is broadly described as piracy. Piracy regards the unauthorised use, copying or distribution of content that is protected by copyright laws, including audiovisual content, music, books and software (see Miconi et al., 2023). In the context of the European and global media industries, piracy is considered intellectual property infringement and a threat to economic returns. As such, different attempts have been made to curb it. Similar to the previous cases, the application of surveillance techniques against the unauthorised consumption of copyrighted content, and the content of audiovisual on demand and streaming platforms in particular, intends to protect the 'common good', which in this case is the protection of the economy and the creators' intellectual property.

From the perspective of the industry, this is a multifaceted phenomenon that exists in different guises and forms, as, for instance, many practices of online sharing (e.g., the case of Netflix passwords) can be discursively constructed as a threat to the economic returns of the industry and subsequently be the subject of surveillance and tracking. From the side of consumers, the reasons for resorting to pirated audiovisual content have mostly to do with the lack of economic resources to buy one or more subscriptions to different streaming services as well as the incomplete cataloguing of these services. In this regard, the data in deliverable D3.4 (see Miconi, et al., 2023) showed that piracy practices vary not only according to 'national habits' but also according to salaries, as maintaining subscriptions to

[16] https://help.netflix.com/en/node/22205

[17] https://itstillworks.com/enable-cookies-watch-netflix-google-chrome-12094903.html

many streaming platforms may be impossible in a country where the average wage is $200, for instance. We should here take into consideration that European (and other) audiences that lack financial ability may use unauthorised sources so as to maintain access to a global cultural public sphere, which is increasingly centred around platform-based audiovisual production (e.g., the drama series Game of Thrones and Squid Game). In the case of Europe, which maintains relatively higher average wages compared to the global average, the data that was examined in WP3 shows that with the development of VODs, unauthorised consumption of audiovisual content has decreased, at least per individual consumer.

Regarding the implementation of surveillance techniques to track unauthorised access and/or use of audio-visual content, the EU authorities and the content industries need to evaluate the resources needed to combat particular unauthorised uses of content. For instance, it is debatable whether it makes sense to track and survey every unauthorised use of video clips in Tik Tok by everyday users. A solution proposed by Jiang et al. (2023) is for platforms to involve the content producers themselves in surveillance through technical instruments, i.e., signing per unit contracts instead of lump sum contracts. In this way, surveillance can be delegated to content producers (or their representatives), as they would receive payment every time their clip is used on Tik Tok or other video creator platforms.

A prevalent way to surveil digital piracy in the EU is by tracking the IP addresses of the users who download unauthorised content, for instance from torrent websites, and sending a fine to a selected number of people as a deterrence strategy. As this fine is linked to the larger digital profile of a citizen, this citizen will need to pay it to avoid further legal problems (this strategy has been implemented in Germany). In this sense, there is a link between the maintenance of digital databases and the implementation of anti-piracy surveillance strategies (Reynolds, 2010). Finally, a common anti-piracy surveillance technique is to track down and eventually arrest the owners of specific platforms where unauthorised content is distributed and consumed, but this requires international cooperation, which due to the often-geopolitical tensions is not always possible.

Users build their own strategies of resistance against surveillance and tracking techniques in order to avoid being persecuted and continue watching unauthorised content, including the countless online 'how to guides' that describe ways to avoid legal consequences (see for instance, Bouliane, 2017). One of the often-suggested resistance strategies of such guides is to download unauthorised content through the use of VPN (virtual private network) services. Piracy has been seen as a form of resistance itself against copyright laws in the first place, as it challenges a financialised understanding of cultural production (Strangelove, 2005; Bakioğlu, 2016). The ones engaging in copying and sharing cultural content make culture open, available and thus more democratic in the sense that larger audiences are able to consume it. This bypasses and in some ways resists the economised relationship with cultural production that is established by the cultural and media industries. Yet the extent to which this resistance is indeed democratic is debatable: bypassing the industry means a reduction in the profits of the sector, which complicates the ways that cultural producers can be compensated for their work.

In any case, the implementation of European surveillance tactics to combat piracy requires not only the mobilisation of significant resources (that need to be backed by research to justify this mobilisation) but also international cooperation, as digital piracy is essentially a phenomenon whose scope is global and multi-centred.

4.3 Perceptions and attitudes towards surveillance on social media platforms

The review of the WP2 related data and analyses pointed to certain noteworthy findings pertaining to how practices of surveillance are perceived by European citizens, how citizens resist such practices, and how their perceptions and attitudes towards surveillance and resistance (to surveillance) are communicated on social media. More specifically, two issues are of relevance in this regard: the first concerns the resistance against the COVID-19 pandemic related measures and restrictions, in numerous European countries, and the second relates to the apprehension of the European Union/Europe as a surveillant apparatus. In both cases, the research captured the debates around these issues, as they took place in the social media platforms of the EUMEPLAT partner countries; thus, these findings reflect social media users' approaches to, and perceptions of, surveillance, and their reactions to these forms of perceived surveillance.

The first area in which resistance to what was perceived as surveillance concerns the resistance against the COVID-19 pandemic related measures and restrictions, and its related anti-vaccination resistance. One of the findings registered in Miconi et al.'s (2022) report on 'Positive and Negative Externalities of News Platformization', was that fake news and/or disinformation posts concerning health and COVID-19 vaccination, were published and shared on Facebook, YouTube and Twitter, in most (if not all), EUMEPLAT partner countries, enjoying in a lot of cases high levels of popularity or virality (pp. 60-66). For example, as it is stated in Cardoso et al.'s (2023) report 'Citizen Journalism in Ten Countries' Facebook posts opposing COVID-19 vaccination were amongst the most popular, in the period studied, in Bulgaria (Cardoso et al., 2023, p. 66, national report for Bulgaria) and in Greece (ibid, p. 114, national report for Greece). Similarly, in Bulgaria, the most viewed video on YouTube, called 'Do not touch the children', concerned an interview "with an infectious disease paediatrician, who became popular for his bold positions against COVID-19 vaccination" (ibid, p. 71, national report for Bulgaria).

Of relevance is also Galeazzi and Zollo's (2021) report on 'Anti-European Fake News and What to do', which analysed a large corpus of Twitter posts published by reliable and questionable sources, in France, Germany, Italy, and the UK, on highly debated topics of European relevance during 2019-2021. Among the findings of the study was that considerable numbers of tracked tweets from questionable sources, were related to disinformation concerning COVID-19 and COVID-19 vaccination, promoting anti-vaccination views (pp. 14-15).

One dimension of the anti-vaccination resistance was directly scientific, spread by self-acclaimed scientists but also medical doctors, whose opinion gained a lot of weight among anti-vaccination online groups. "By citing likeminded sources and pseudo-scientists', such groups function[ed] as 'anti-establishment echo chambers" (Miconi et al. 2022, p. 83), feeding from, and spreading further, disinformation and conspiracy theories, also propagating science denialism. Such responses are likely expressions of broader phenomena of antisystemic resistance, which also targets science (in this case, medicine), seen as a distrusting institution aiming to control people. These findings are in alignment with studies arguing that online disinformation is related with distrust in state institutions and the media, science scepticism, and increased radicalisation (e.g., ethnonationalism) (French & Monahan, 2020; Marwick & Lewis, 2017).

One other dimension concerned the COVID-19 vaccination certificates, which were seen as a major practice of surveillance not only across Europe, but globally. Part of the contestation concerned the centralisation of the certification system for the entire EU, through the EU Digital COVID Certificate. Collecting and then giving the authority to a broad range of public and private third parties to access personal or/and sensitive information, through the scanning of the certificates, was considered a major practice of surveillance. The critique was that these entities were granted authority to control mobility, entry or access (related to transport, travel, shopping, accommodation, restoration, leisure, work, education, etc,), with no further regulation as to how the information included in the certificates would be used in the future. Therefore, the series of the pandemic measures restricting mobility (e.g., the imposed lockdowns and curfews) and the vaccination certificate requirements were presented in some of the data (e.g., in Italy, see Miconi et al., 2022, p. 83), as a surveillant apparatus curtailing citizens' and employed people's freedom, disciplining mobility and work.

The second area of contestation sees the EU as a surveillant apparatus, which is often embedded in a Eurosceptic attitude towards the EU, its politics and its institutions. The findings that point to such an analysis are not visible in all EUMEPLAT partner countries. They are mostly visible in the Czech Republic and, based on the country reports, to a certain extent also in Spain, Bulgaria, and Portugal.

The posts that express these attitudes see the EU as a surveillant apparatus attacking national sovereignty, and curtailing states' and/or citizens' freedoms. Hence, EU legislation, directives and institutions are perceived as surveillant and disciplining structures. For example, as it is stated in the national report concerning the Czech Republic, ''Europe's/EU's regulatory framework, directives, legislation, or legal decisions, [are] often critiqued by the far-right as restricting the country's freedom and sovereignty" (Cardoso et al., 2023, p. 89), against which the states –in this case the Czech state–must resist, even by leaving the EU, as the Czech far-right argues. Also, posts concerning business and the economy "published by Eurosceptics and the far-right [...] stress how much the independence of the national industries is limited or harmed by the European directives and related legislation" (ibid). It shall be mentioned that the research period was a period of parliamentary elections for the Czech Republic, during which Eurosceptic populism was highly vocal and popular on social media in the country.

In some cases, Euroscepticism was expressed through anti-vaccination arguments, stating or implying that the EU wants to control the citizens through a centralised system of surveillance, which in this case was implemented through the EU digital COVID certificates.

The review of the WP2 related reports pointed to findings showcasing European citizens' perceptions regarding surveillance by the EU and/or the states, and their responses of resistance, as they are expressed in social media platforms, often bearing an antisystemic character. This antisystemic resistance, which is not restricted to the political system and its institutions, but seems to be extending to authorities and institutions connected to the media, science, education and the academia, merits further exploration, as it appears to relate to a rising discontent with liberal democracy and to phenomena of increasing intolerance and radicalisation.

4.4 Migration in Europe as an issue of border control

Since the height of what is known as the migration and/or refugee crisis in 2015, the EU has been implementing measures to enhance border controls and migration management[18]. Many such examples were found in the WP4 analysis, that focussed on the representations of migration on Facebook and Twitter, in the ten EUMEPLAT partner countries (Ingebretsen Carlson et al., 2023). A lot of the posts emphasised the need for tighter control of borders, and more efficient management of the migration flows, as indicated in the analyses of the ten

[18] See https://www.consilium.europa.eu/en/policies/eu-migration-policy/

national reports, which is directly related to claims for the need of more enhanced surveillant systems and practices in Europe.

The research period (September – November 2021) was dominated by the tensions on the border between Poland and Belarus with hundreds of migrants and refugees being kept from entering the EU space, which was often described in the analysed material as a border crisis. This event appeared in all EUMEPLAT partner countries' social media discussions. Issues that arose in relation to this event were the 'failure' of the EU to protect its borders, and the need for tighter measures in this direction, but also the questioning of the legality of Poland's harsh measures to close off the border with Belarus during the crisis. Poland's position was welcomed and even celebrated by far-right political voices as exemplary (see, e.g., report for Belgium, in Ingebretsen Carlson et al., 2023, pp. 29, 33; report for the Czech Republic, p. 103; report for Germany, p. 157; report for Sweden, p. 344). At the same time, there were also solidarity efforts by civil society actors and humanitarian groups, as presented in the analysed material, that "demanded that border closure measures and illegal violent pushbacks must be stopped and access by the refugees to the asylum system must be ensured" (report for Germany, pp. 153-154; see also report for Greece, p. 195), directly contesting the tight border control system as violating fundamental human rights and freedoms. Similarly, as it is mentioned in the report for Portugal, pointing to Amnesty International's response shared on social media, "the EU should act firmly to denounce this flagrant abuse of both EU and international law and put an end to the ruthless way in which these people have been treated for several weeks" (p. 277).

The Polish-Belarussian tension was not the only case in which the migration issues were treated as a border crisis for Europe. There were a series of different events in the EUMEPLAT partner countries, that attracted attention on social media at a national or regional, but not pan-European level. For example, the Ceuta migration crisis in Spain in 2021, which had a significant impact on public perception and European migration policy given that for several days in May, there was a large influx of migrants and asylum seekers attempting to cross the border between Morocco and the autonomous city of Ceuta, generating a humanitarian emergency and diplomatic tensions between Spain and Morocco. This event was also connected to the argument for the implementation of more solid surveillance practices in Europe to improve the control of external borders and migratory flows (see report for Spain, p. 297).

Also, in Turkey's and Greece's cases, there were a series of posts regarding the relations of Turkey with Europe, presenting migration as an issue concerning the control of the Turkish-European/EU borders (see, e.g. report for Turkey, p. 371; report for Greece, p. 190). Such posts featuring in Greek and in other countries' social media, critique Turkey for using migrants as a strategic weapon to 'blackmail' Europe, opening its borders and pushing migrants to Europe. There are also posts in the Turkish, Greek and other countries' social media, that critique the Greek authorities, the EU or Frontex for mistreating migrants/refugees or pushing them back to Turkey, in violation of international law (see e.g., report for Greece, pp. 193-196, 207-208; report for Turkey, pp. 379, 381).

What is common in the national report analyses, is that migration is largely addressed as a borders (control) issue for Europe and for the EU that struggles to adopt and implement a joint migration policy for its member states. Human rights and values are evoked, but even in benevolent approaches they become a managerial issue that objectifies the people as passive beneficiaries of Europe's benevolence.

The turn towards systems of tighter control is manifest in the latest EU migration agreement[19], reached on June 8, 2023, which has been expanding its surveillance policies and measures. This agreement foresees, among others, a new system to separate asylum seekers according to the likelihood of being granted asylum, with the aim of streamlining the assessment procedure. The agreement also introduces mandatory border procedures to quickly assess the validity of asylum applications at the EU's external borders and determine their merits or inadmissibility, also establishing mechanisms to balance the burden of asylum applications among EU member states. The regulation also contains measures to prevent 'abuse' of the asylum granting system by asylum seekers, and to avoid secondary movements, establishing obligations for asylum seekers to submit their application in the member states of first entry or legal stay. This measure limits the possibilities of cessation or change of responsibility between member states, which reduces, in practice, the options for applicants to choose the member state where to submit their application.

In this situation, advocates of stricter border controls argue that such measures are necessary to protect the integrity of the Schengen area and ensure the safety of European citizens, as long as no rights are violated. In addition, they argue that tighter border management can contribute to better migration management by allowing a more accurate identification of asylum seekers and a more equitable distribution of available resources.

The already strong appeal for tighter surveillance systems for the control of the borders, but also for the regulation of movement and rights of the migrants and asylum seekers once they have entered into EU territory, appears to be getting stronger and is becoming the main approach as to how to handle migration. These demands seem to be echoed in the social media discussions, as they have been analysed in the EUMEPLAT research, bearing further implications for Europe, its values and its freedoms.

[19] https://www.consilium.europa.eu/en/press/press-releases/2023/06/08/migration-policy-council-reaches-agreement-on-key-asylum-and-migration-laws/

5. Future scenario analysis

5.1 Future scenario building and analysis: Delphi+ workshops and scenario essays[20]

The Delphi method is a method for future scenario-building and forecasting with a long history. To illustrate: Gordon (2009, pp. 1-2) relates this method to the work of RAND in the early 1960s. Developed in the early stages of the Cold War, in order to predict the impact of technology on warfare (San-Jose & Retolaza, 2016, p. 3), its consolidation started with the RAND projects, which were established to predict the probability or intensity of possible enemy attacks. These think tanks, such as RAND, “provided the methods and techniques for the military and strategic planning of US administrations” (Seefried, 2014, p. 3; see also Amadae, 2003). Currently, the Delphi method – as a technique that offers a “systematic means of synthesizing the judgments of experts” (Gordon, 2009, p. 11) – is used across various academic disciplines and fields. There are many variations of the Delphi method itself, but several characteristics are still transversally present. Landeta (2006, p. 468) defines the Delphi method as “a method of structuring communication between a group of people who can provide valuable contributions to resolve a complex problem.” As Gordon (2009, p. 4) summarises it, the Delphi method is grounded in a “controlled debate” which allows for the establishment of consensus among experts, through a series of iterations. This implies that expert-participants can discuss the responses of others and the work of the group as a whole, but also that they can alter their own positions during the process.

Despite its limitations (Winkler & Moser, 2016, p. 63), the Delphi method is often used in future studies, while it is used also in other fields (Poli, 2018). The field of future studies is defined by Inayatullah (2012, p. 37) as “the systematic study of possible, probable and preferable futures including the worldviews and myths that underlie each future.” As a field, future studies has moved “from predicting the future to mapping alternative futures to shaping desired futures” (Inayatullah, 2012, p. 37). These three components refer to three different approaches—with different ontological assumptions—namely, forecasting (to predict the most likely future), scenario-building (to explore alternative futures) and backcasting (to assess the feasibility of a desired future). As it is often emphasised in future studies publications: “Futurists do not know what will happen. They do not claim to prophesy. However, they do claim to know more about a range of possible and desirable futures and how these futures might evolve” (Glenn, 2009; see also Robinson, 1988, p. 325). In the end, future studies, as a field, relates to “thinking the unthinkable” (Kahn, 1962).

[20] This section was written with contributions by Nico Carpentier and Miloš Hroch.

In our case, the Delphi method was adjusted into a 3-and-a-half-hour face-to-face scenario-building workshop, which focussed, apart from surveillance and resistance to surveillance, also to four other pre-given themes pertinent to the EUMEPLAT research (algorithms and choice, toxic debate and pluralistic values, destructive technologies and war, and gender in society). The four workshops[21] had two stages. Stage one consisted of small group discussions, with one moderator for each of the subgroups, with the aim of producing three future scenarios for each theme. In stage two, which was a plenary stage, the participants introduced a selection of scenarios to the entire group. The four workshops were organised in three different European cities, with in total 29 participants (see Table 1 for an overview). As a method, these adjusted (and time-compressed) workshops approximate what Pan et al. (1996) called a mini-Delphi, although we prefer to label these four workshops 'Delphi+' workshops.

Table 1: The EUMEPLAT Delphi+ workshops

Number	Date	Location	Participants
1	5 July 2022	Malmö, Sweden	Science fiction writers and foresight researchers, experts on science communication or philosophy of science, and specialists in digital marketing and applied predictive models (6 participants)
2	4 October 2022	Sofia, Bulgaria	A theatre artist, a Roma activist, a journalist, and a former representative of the Bulgarian government in the field of culture (6 participants)
3	13 April 2023	Rome, Italy	Expertise ranging from cultural relations, bioethics and AI to political science and the futures of electronic music (7 participants)
4	23 June 2023	Sofia, Bulgaria	A film maker and producer, a TikTok influencer, journalists, media studies professors, and chatbot and new media experts (10 participants)

[21] A pilot Delphi+ workshop was held in Prague, on 5 May 2022. These data were not used.

The project included also the writing of future scenario essays by the EUMEPLAT researchers, in all five themes of Work Package 5. The aim of this component was to complement and enrich the diversity of the produced future scenarios, and involve the EUMEPLAT team members in both scenario writing and analysis. All essays were written prior to the initiation of the analysis, and the produced material, apart from broadening the range of scenarios, allowed for reflexivity in research (Alvesson & Sköldberg, 2000) and added an auto-ethnographic dimension (Maréchal, 2010) to the project.

For the purposes of the study, a qualitative content analysis (Saldaña, 2013) was conducted on the Delphi+ workshops and future scenario essays material. More in detail, the material comprised 35 future scenarios[22] coming out the four Delphi+ workshops and four EUMEPLAT partner future scenario essays, totalling 39 future scenarios, all focussing on surveillance and resistance to surveillance. The Delphi+ workshops material consisted of the scenario cards produced during the workshops by the participants, summarising each scenario in keywords, and the transcriptions of the discussions taking place during the workshops. The EUMEPLAT partner future scenario essays were written by some of the authors of this deliverable, and were each 2-4 pages long.

The analysis of the material followed a series of cycles. At first, main issues, topics and dimensions concerning surveillance/resistance were identified through open coding, by registering keywords and illustrative quotes pertaining to:

- definitions of surveillance/resistance;
- forms, practices, platforms, technologies of surveillance/resistance;
- actors of surveillance/resistance;
- evaluation and prediction (surveillance is good, bad, necessary, unavoidable; resistance is (im)possible, etc.)
- definitions of future (in relation to surveillance/resistance)
- role of Europe (in relation to surveillance/resistance)

The preliminary analysis of the open coding was followed by a series of iterations between the empirical material and the theoretical framework, through an abductive approach (Matthews & Ross, 2010). This resulted in the identification of the main dimensions of analysis, structured around the techno-pessimist and techno-optimist visions of surveillance and resistance to surveillance (see Table 2 for an overview).

[22] The numbers of future scenarios per workshop were as follows: Sofia 1: 6 scenarios; Malmö: 10 scenarios; Rome: 9 scenarios; Sofia 2: 10 scenarios.

The analysis is theoretically informed by the scholarly work in the transdisciplinary field of surveillance studies (see, e.g., Lyon, 2007; Martin et al., 2009; Marx, 2003; McCahill & Finn, 2014; Zuboff, 2019) and is enriched by the 'social construction of technology' approach, with a focus on techno-pessimist and techno-optimist debates in media and communication (see, e.g., Königs, 2022; Lindgren, 2017; Negroponte, 1995; Postman, 1992; Ridley, 2010).[23]

5.2. Analysing the future scenarios: Identifying visions of surveillance/resistance

The scenario analysis pointed to two main approaches to technology, the techno-pessimist and the techno-optimist, which feed into how surveillance and resistance are perceived, and how Europe is imagined in these visions of the future. As it is shown through the analysis, the techno-pessimist and techno-optimist visions do not always fit into the dystopian – utopian (or eutopian) dichotomy, as an imagined future driven by a techno-pessimist vision may construct a utopia, or a techno-optimist vision might describe a future not constituting either a utopia or dystopia. At the same time, they are consistent in informing distinct visions of the future, grounded in main assumptions, and echoing main hopes and fears about social organisation and technology, and thus can be seen as glimpses of what to look for, and what to avoid, in societies and in Europe.

[23] For a detailed presentation of the theories and debates that support the future scenario analysis, see Section 2: 'A theoretical reflection'.

Table 2: Overview of techno-pessimist and techno-optimist visions of surveillance/ resistance

Techno-pessimist visions	Techno-optimist visions
Technology	
Technology damaging/ destructive	Technology as enabler/ facilitator
Technology powerful, with agency	Technology powerful, with agency
Surveillance	
Surveillance enhanced/ total	Surveillance regulated/ not uncontrolled / not enhanced/ not absolute
Surveillance unavoidable / impossible to escape	Surveillance moderate and balanced (as much as needed)
Surveillance damaging/ destructive	Surveillance beneficial for societies
Resistance	
Limited agency by people	Non-tech actors have agency
Non-tech actors powerless, not visible/ irrelevant	(Some) resistance possible / Surveillance can partly be avoided/ controlled
Resistance not possible	Literacy as a tool to resistance
	Selective use of technology / Technology avoidance
Technology avoidance /rejection / elimination	
Return to the analogue/ pre-digital / the “noble savage”	No high resistance needed (surveillance beneficial)
Europe	
Europe will lose over companies – enhanced corporate surveillance	Europe regulator of surveillance / facilitator of data collection/ data management
Europe will become authoritarian – surveillance apparatus	Europe protector of people’s rights and freedoms – rule of law
State/Europe-corporate nexus enabling enhanced surveillance	Europe as a democratic model to follow
Europe without digital technology as surveillance-free	

5.2.1 Techno-pessimist visions of surveillance/resistance

The analysis structured around the techno-pessimist visions of surveillance/resistance comprised three main dimensions, namely, technology and surveillance, resistance to surveillance and visions of Europe. These dimensions address how techno-pessimism instructs specific understandings of surveillance and responses to it through forms of resistance, and how these techno-pessimist visions inform also specific visions of Europe, which are guided by a negative or critical disposition toward technology.

Technology and surveillance

In techno-pessimist visions of surveillance, the focus is on the problems technology creates for individuals, and society at large, with technology being apprehended as the optimal tool for surveillance.

Technology is seen as powerful, having agency, and humans as weak. In these techno-centric visions, which are often deterministic, technophobic and dystopian, humans have hardly any agency, being subjected to the force of technology, complying to its demands, or appearing as passive recipients of it. Technology is apprehended as a disabler of people, restricting them to a large extent. Its force and impact are mainly destructive, impacting negatively on people's everyday life, private life, family life, professional and social life. In the most dystopian variants of these visions, humans lose all their freedom, as technology fully controls their lives, and they become slaves of technology (Sofia 2 Delphi+ workshop). In these visions, surveillance becomes absolute, as people's lives are tracked in every detail, through, for instance, emotional tracking, or collection of biometric and DNA data (Malmö Delphi+ workshop).

In such forms of "hyper-surveillance" or "micro-surveillance", not only does people's private sphere completely collapses or disappears (Malmö Delphi+ workshop), but also massive social control is engineered. By developing predictive models of 'good' and 'bad', 'suitable' and 'unsuitable' citizens, extensive 'social sorting' (Lyon, 2003) is put to effect, excluding, punishing, or even exterminating 'unsuitable' individuals, in the name of social order and public safety (Malmö Delphi+ workshop).

All-powerful technology is presented also as blurring the boundaries between the real and the virtual world (Sofia 2 Delphi+ workshop), making it difficult for humans to distinguish between the two. Hence, human consciousness, in this case about people's environment and experiences, is disrupted or determined by advanced technology. Such a blurring or disruption makes humans more vulnerable and susceptible to surveillance, as they cannot fully comprehend or control their environment.

Enhanced or complete surveillance appears in several of the analysed scenarios as impacting or even controlling people's behaviour, bodily performance and consciousness. Two of the scenarios involve implanting a microchip into people's bodies, to achieve "total and absolute social control", in what is described as "QR-codization of life" (Rome Delphi+ workshop). This type of control is corporeal, fully restraining movement, as people will need to continuously scan their microchip, to be allowed mobility and access. This reaches the level of dehumanisation. One of the scenarios is a modified version of the dystopian science fiction television series 'Severance', in which technology-enabled surveillance supports the separation of the self. In the TV series, people's memories are divided between their work and personal lives' memories, leading to people developing distinct consciousnesses and personalities, in work and outside of it. In the future scenario, people's memories are deleted, they forget their lives and how to be human (Sofia 2 Delphi+ workshop).

One other scenario, in this techno-pessimist and technophobic dystopia, focusses on isolation and fragmentation of the social world. In such a "fragmented world" (Sofia 2 Delphi+ workshop) there is no social cohesion; technology-facilitated surveillance will lead to social fragmentation, where "everyone would try to survive by themselves. Manipulation and propaganda will divide people in several groups" (Sofia 2 Delphi+ workshop), there will be no trust in information, in (news) media and in institutions, and the levels of stress will increase for everyone due to a generalised distrust and suspicion.

These conditions of social fragmentation foster, according to some scenarios, different types of conflicts and social divides. One of these types concerns on the one hand the majority of oblivious people who are not resistant to surveillance and have fully complied, not identifying surveillance as a problem, or the ones who do not realise that they are "giving their data away" (Rome Delphi+ workshop) and that they are subjected to surveillance, and on the other hand the small minority of people who are conscious of being surveilled and are resisting. These few, called in the scenario as the "leftovers" of society, are accused by the rest of society of being conspiracy theorists (Rome Delphi+ workshop).

Resistance

The ideas pertaining to resistance in the techno-pessimist visions of surveillance are twofold. One cluster of ideas sees people as lacking agency or as powerless, and another identifies some forms of resistance, which often involve technology avoidance or full rejection.

According to the first approach, as already mentioned, while technology appears as forceful, people appear as weak, with limited agency, or as lacking agency completely. Given techno-pessimism's techno-centrism, non-technology related actors are generally powerless or not visible. Technology is seen as a dominator and enabler of enhanced or total surveillance, either at the individual or at the broader societal level, where resistance is not possible. Such visions are grounded largely in a fear-driven attitude towards technology, in which high interconnectedness creates conditions where there is no escape to surveillance, as non-traceability is impossible. As it is described in one scenario, “trillions of devices will be connected. It will be impossible to be anonymous, go under the radar” (Malmö Delphi+ workshop).

Within this logic of inability, managing or controlling surveillance is also not possible. For instance, granting consent in digital platforms for the collection of users’ data is of limited effect; it is very difficult given that technological applications are purposefully complicated for ordinary users. Furthermore, while the requirement for consent will continue to exist, in practice if users do not share their data, they will not be able to have access to services and social networks, and will be excluded from the social realm: “you can choose to not give your data, but then you won’t have access to basically anything. […] Like if you don’t have a social security number or even the physical ID, you can’t do anything. You basically don’t exist” (Malmö Delphi+ workshop). Developing literacy skills for self-protection is time-consuming and will require extra resources (money) to protect oneself (Sofia 2 Delphi+ workshop); hence the divide between the already socially and economically privileged, the ones possessing cultural and economic capital, and the ones who lack this capital, will deepen.

In the cases where resistance is identified in the techno-pessimist visions, it involves, as mentioned previously, technology avoidance or technology rejection, either at the individual or collective levels, driven by technophobic, or neo-luddite beliefs. For instance, in the scenario of a man who collects and analyses personal data of European citizens, but then becomes paranoid about being surveilled himself, he employs a series of technology avoidance practices, such as deleting his social media accounts, stopping using mobile devices, or cancelling his accounts on video on demand platforms. He gradually engages in more enhanced forms of technology avoidance and technology rejection, such as not using online banking and credit cards, paying only with cash, not having any online activity (going fully offline), and replacing all his digital devices with analogue ones, using, for example, a photo camera with film, a video-cassette player, a Walkman and a gramophone (EUMEPLAT partner scenario essay).

The visions of technology rejection include also a scenario where a neo-Luddite movement called “radical abolitionists” wins power in Europe and abolishes all surveillance. The supporters of the movement advocate “for a return to a world without surveillance” and for an “immediate abolition of all surveillance systems aiming to subjugate the European population to the Machine”’ (EUMEPLAT partner scenario essay). These neo-Luddites ground their views in a broad anti-technological sentiment and “blame technological progress for the misery of poorer populations” (EUMEPLAT partner scenario essay). Resistance in this case is expressed not only through technology rejection, but also through the claim for the elimination of technology. As described in the scenario, "the neo-luddite movement advocated for the immediate physical elimination of all machines and electronic devices capable of harvesting, storing, and processing private data, including computers, smartphones, data centres, and servers" (EUMEPLAT partner scenario essay).

The visions that promote luddism are also embedded in ideas of primitivism, the belief that humankind needs to return to times prior to the industrial society and modern styles of life, described through "Rousseau's archetypical figure of the 'noble savage'", which "signifie[s] an unspoiled, morally superior, and innocent creature that ha[s] not been contaminated by the evilness of modern civilization" (EUMEPLAT partner scenario essay).

Visions of Europe

To a large extent, these techno-pessimist visions are technocentric, focussing on the role of technology as the main or most powerful actor. Still, some of the scenarios do bring to the fore a series of other actors, such as the corporate sector, institutions, nation states, governments, Europe or the EU, and people at large. The focus in these scenarios is on actors that use technology-enabled surveillance (and cause harm) or on the clear repercussions of technology-enabled surveillance to diverse actors.

In these scenarios, there are certain dystopic visions of Europe. One of these visions sees Europe as being defeated in the conflict with the (non-European) corporate sector. In such a scenario, "private companies will have a strong say, [pushing] for deregulation" (Malmö Delphi+ workshop) and Europe will become unable to protect its citizens against corporate surveillance. Moreover, "infrastructure in Europe [will be owned] by foreign owners, enabling them to influence or control sensitive systems like electricity, water supply, etc." (Malmö Delphi+ workshop). In the latter case, the corporate sector will be in a privileged power position to impose enhanced surveillance also through the control of main resources.

In one scenario which focusses on issuing European ID cards for all citizens and abolishing national identity cards, techno-pessimist voices are highly concerned about the collection of data for all European citizens and their use by companies. For some of these voices, "this is a project promoting globalised capitalism, imposed by the big multinational companies" (EUMEPLAT partner scenario essay). According to these critics, "these conglomerates will get access to all European citizens' personal information and use this data in an uncontrolled fashion to enhance their profits, and expand their business activities to a pan-European scale, further damaging local business activity" (EUMEPLAT partner scenario essay). Another dystopic variant sees Europe becoming "subservient to the US", its companies and its institutions (Rome Delphi+ workshop).

These visions see technology as damaging or destroying Europe and some of them incorporate a neo-luddite stance, arguing for the need to return to the past, promoting the disregard of technology in Europe as the solution for happier people and fairer societies. In one of the scenarios,

> “Europe becomes a big ‘Switzerland’ declaring technological non-alignment. EU may disappear and to avoid that, Europe should become neutral and stay out of the race. May go back to agricultural societies, switch off the internet for certain times of the day” (Rome Delphi+ workshop).

In another dystopic variant, Europe will become authoritarian. Citizens will be subjected to enhanced surveillance, their freedoms will be curtailed, and they will be unprotected against the nation states and the European institutions, that will have become surveillant apparatuses. For instance, the resistance against the European ID cards, presented in the relevant scenario, is grounded in the critique by right-wing and nationalist voices that “Europe is being transformed into an apparatus of severe surveillance and control, fiercely attacking the national identity and sovereignty of the nation states” (EUMEPLAT partner scenario essay). For left-wing voices that oppose the European ID cards project, “Europe functions as a supra-state, aiming to surveil and control all individuals”, which “goes against people’s individual identities and freedoms” (EUMEPLAT partner scenario essay). Similarly, in the scenario where a man is secretly “collecting and analysing … personal data of European citizens”, he engages in extensive forms of surveillance which expand into these citizens’ “taste, behaviour and preferences” (EUMEPLAT partner scenario essay).

A warning against the uncontrollable repercussions of surveillance of European citizens is expressed in the European ID cards scenario. As it is argued by human rights advocates, “access to the pan-European ID cards database by third parties will infringe citizen rights and freedoms” (EUMEPLAT partner scenario essay). The danger is greater “in countries with highly networked systems of public administration (e.g., Sweden)”, where “uncontrolled third parties” can “have access to detailed information about individuals, related to income, professional activity, but also to criminal records, health records, etc., exposing individuals to multiple risks connected to the lack of control of their own information” (EUMEPLAT partner scenario essay).

These “uncontrolled third parties” may be either state or corporate entities, something that is shared in a number of the analysed scenarios, which centre around the state/Europe-corporate collaboration as a threat to democracy, leading Europe to giving up its democratic values and becoming more authoritarian. In one of these versions, “the state - corporate nexus intensifies” (Rome Delphi+ workshop), leading to increased control of the European citizens through the state-business collaboration enabled by technology: “[The] social credit system will be intensified, states [will be] collaborating with corporations to deepen social control" and Europe will resemble "more authoritarian states" (Rome Delphi+ workshop). In such a scenario, "Europe, European Union could play a particularly negative role because it's one of the few supernational institutions capable of harmonising social control across nation states". This negative role would relate to "how these policies are harmonised across nation states. […] overseeing the super-state control of information" (Rome Delphi+ workshop).

Similarly, the establishment of the neo-Luddite movement that wins power in Europe and abolishes all surveillance, as it described in the related scenario, is a response to a state/Europe-corporate collaboration that allowed for enhanced surveillance, in a dystopian, techno-pessimist future. As it is explained in the scenario,

> "a secret, state-backed, and privately operated programme was monitoring citizens through microchip implants that were inserted voluntarily into their bodies to help them with everyday decision-making. The data from these implants was automatically sent and stored in a vast data factory in Greenland and was then sold to advertisers and governments around the world without the users consent" (EUMEPLAT partner scenario essay).

However, not all techno-pessimist visions of Europe are dystopian. For example, in neo-luddite apprehensions of technology, the abolition of technology and the return to pre-industrial lifestyles would lead to a better and surveillance-free Europe, where "the exaltation of natural life, agriculture, and the archaic roots of European civilization" would help create a new European identity, of the pure, morally 'clean' "new European noble savage" (EUMEPLAT partner scenario essay).

5.2.2 Techno-optimist visions of surveillance/resistance

The analysis of the techno-optimist visions of surveillance/resistance comprised the same three dimensions, as in the techno-pessimist visions, namely, technology and surveillance, resistance to surveillance and visions of Europe. However, as the analysis shows, these visions are constructed through fundamentally different understandings of surveillance, practices of resistance, and imaginings of Europe, fed by a positive disposition toward technology.

Technology and surveillance

In the techno-optimist visions of surveillance, the focus is on the positive and empowering aspects and forces of technology. Technology is put to the service of people and societies, and surveillance appears as either a neutral reality (neither positive or negative) or as desirable and beneficial for societies and for the greater good. There are instances where a warning is raised against potential threats or potential harm caused by technology-enabled surveillance, but these concerns are countered by the belief in control or regulation of surveillance by societies.

Even if the techno-optimist visions tend to be also technocentric, echoing sometimes technological solutionism, there is a clearer focus on what people do or what Europe does with technology, to improve people's lives and societies at large. Technology is powerful, but people can use it in ways that will benefit them. It is thus perceived more as an enabler or facilitator of people and societies, than a threat.

In the techno-optimist visions of surveillance, the latter is not perceived as enhanced or total, but rather as regulated and controlled, by elaborate regulatory frameworks and societies at large. There is also an emphasis on surveillance being moderate and balanced, leading to societies having as much surveillance as needed. This vision promotes "a balanced and completely ethical approach where you only have the surveillance you need. And no more, no less" (Malmö Delphi+ workshop). In such a vision there are incentives for voluntary engagement in surveillance, where responsible citizens have "opt-out options, voluntary opt-in and opt-out". This model of voluntary surveillance "would be […] harmonised with the governance structure in each society or community" (Malmö Delphi+ workshop). Still, it shall be noted that such apprehensions of surveillance apply to democratic societies, which, in the analysed scenarios are often contrasted to authoritarian regimes, where surveillance is overwhelming and absolute and does not function to the benefit of societies, but to the maintenance of power by the undemocratic rulers.

In similar scenarios, surveillance can contribute to safe societies, in a model where the state is not imposing severe control, but societies are self-governed: "Society can value more security […] [and surveillance] can be performed in [a] more human form. [The] state is not controlling individuals, but society is governing itself" (Sofia 1 Delphi+ workshop). The systematic collection of information concerning the citizens will allow, among others, for policy planning and regulations concerning, for instance, better health control and the prevention of health crises and "climate disasters" (Malmö Delphi+ workshop).

Technology-facilitated surveillance is seen also as an enabler of inclusion, participation, democracy and civic engagement, and contributes to the vision of social justice. In this vision, surveillance is beneficial as it helps to build responsible societies, promoting "accountability and solidarity", "fairness", "equity", the protection of diversity and human rights, as well as the "protection of vulnerable groups" and their inclusion in the social realm (Rome Delphi+ workshop). Such conditions of enacted social justice will facilitate the reduction of societal conflicts and will result in "power distributed democratically" in societies (Malmö Delphi+ workshop).

Such visions of socially responsible surveillance see the latter as “human-centric” and “value-driven”, where there is a strong emphasis on individual and collective ethics (Malmö Delphi+ workshop). For instance, the scenario of “decentralised accountability” sees surveillance as “a system of solidarity where people are accountable for each other”, taking “into account the […] diversity of experiences of different socioeconomic groups” and the “individual situations of people” (Rome Delphi+ workshop). This scenario argues that, as people and groups are affected in different ways from models of social organisation, their rights and perspectives need to be considered when designing and implementing systems of control.

Resistance

The ideas pertaining to resistance in the techno-optimist visions of surveillance are clustered around two main approaches: one expresses the view that people have the agency to resist surveillance, and the other that there is no need for strong opposition to surveillance, as the latter is mostly beneficial for societies. The latter approach is embedded in considerable levels of societal and institutional trust (Björklund, 2021; Newton & Zmerli, 2011), which are not met in a lot of the techno-pessimist visions, in which distrust towards the institutions is expressed, among others, through resistance to state control (Ellis et al., 2013).

In the techno-optimist visions, people have different degrees of agency and control over technology and over their lives. Also, in these visions, there are always ways of negotiating, managing, controlling or resisting surveillance. Even in the most dystopian scenarios where humans have implanted microchips that control mobility and behaviour, resistance can be performed by having the microchips removed (Rome Delphi+ workshop).

One important aspect is technological and digital literacy. If people develop literacy skills and are critical towards digital technologies, they can use technologies in beneficial ways and can control parts of surveillance. According to one scenario, “algorithmic literacy” (Rome Delphi+ workshop) will lead to the increase of “individual resistance” to surveillance (Rome Delphi+ workshop). In general, digital literacy appears as being up to people’s interest and active engagement. Thus, the ones who are interested can develop skills that enable them to control surveillance and use media and communication platforms to their benefit.

Literacy helps people become aware of how surveillance functions and allows them to maintain some control in this process, still acknowledging that they cannot avoid surveillance completely:

> “[the] recognition that […] there is a compromise made between convenience and surveillance. […] it’s a recognition that you can never be completely off-grid, but a much greater literacy around the exposure of being on-grid [allows to decide] how much of the trade-off you’re willing to make” (Malmö Delphi+ workshop).

Instrumental and selective use of technology grounded in informed decisions, is coupled also with technology avoidance, which however requires enhanced skills and financial resources: “People who can, want, will afford to use non-algorithmic social media, which doesn’t spy on them but is expensive” (Sofia 2 Delphi+ workshop).

Literacy in the form of a continuous education for citizens is seen as a mechanism of corporate self-regulation, due to societal pressure. Such a literacy would support “the rise of critical currents that would foster resistance and pressure companies to adopt self-regulation measures”, “motivated by the demands of society and consumers” (EUMEPLAT partner scenario essay). Furthermore, it is connected with citizen responsibility and accountability in a vision where the self-governance of societies will replace top-down surveillance: “of course to make this work it is necessary to foster critical thinking through education and active participation of people instead of just having policies to control … to exert surveillance from the top” (Rome Delphi+ workshop). In such a vision of socially responsible surveillance, “resistance has turned into organised unions constructing civil engagements, data literacy, participatory designs, cooperation and inclusion” (Malmö Delphi+ workshop).

Visions of Europe

In the techno-optimist visions of surveillance, Europe appears as having a generally positive or constructive role. It sometimes appears in a rather neutral fashion as a regulator of surveillance or facilitator of data collection and management.

In more clearly eutopian techno-optimist visions, Europe appears as an active protector of people’s rights and freedoms, fighting (successfully) against companies that aim to monitor people’s behaviour in online platforms for profit-oriented purposes. The vision of Europe as a powerful legislative regulator adheres to ideas of Europe governed by the rule of law, based on which people’s privacy and freedoms have priority over corporate interests, and are rightfully protected. In this vision, in which “European states take competitive advantage of a more ethical use of data” and technology (Malmö Delphi+ workshop), the role of the nation states and of the European institutions is more powerful than that of the companies.

Such techno-optimist visions of surveillance present Europe as the democratic paradigm, the example to follow in the USA and in other parts of the world. Some of the analysed scenarios, “recognise the role of European values and European institutions […] in equal rights or human rights and gender” (Malmö Delphi+ workshop) and emphasise the need for a “European model of an ethical governance of data” (Malmö Delphi+ workshop), that will prioritise values and freedoms over profit or political gain. For instance, one of the scenarios promotes the idea of a “European social contract for ethical use of surveillance for health and sustainability” (Malmö Delphi+ workshop).

For the techno-optimists, the European ID cards project, which would require the collection and processing of information for citizens at a pan-European level, is seen "as an opportunity for the (pan-)European citizen, and for a Europe for all which will be more inclusive and solidary than the EU" (EUMEPLAT partner scenario essay). Issuing the identity cards, according to supporters of the project, would allow the European citizens "to access services in different European countries", and it is seen as a means "to enhance mobility and boost the economy", but also as a way "to ease the trauma of the war in Ukraine and the broader tensions and conflicts in Europe […] signifying a pan-European vision" (EUMEPLAT partner scenario essay). For these groups, which exhibit considerable trust in the national and European institutions, "the ID cards project does not constitute a surveillance threat per se, as long as access to the collected information is protected and supervised by independent authorities" (EUMEPLAT partner scenario essay).

6. Concluding remarks

The review of the EUMEPLAT research, as conducted through the work packages 1-4 of the project, and the future scenario development and analysis conducted within work package 5, point to a series of issues, dimensions and debates, pertaining to control, supervision, surveillance, and resistance to surveillance, facilitated through communication and media platforms in Europe. As it was highlighted throughout this deliverable, these issues are indicative of, and connected to, broader tensions and challenges in Europe, meriting attention and further research.

Firstly, the elaborate European/EU policy and regulatory frameworks for the protection of individuals' privacy through complex and extended regulations point to a preoccupation with the protection of European citizens' freedoms and rights, since the early days of European integration (see WP1). These ideas are reflected in the expectation –and demand– that Europe/EU functions as a paragon of democracy also as it concerns the regulation of surveillance and the protection from it.

The EU General Data Protection Regulation (GDPR) has been presented as an example in this direction, and as a model to follow in other parts of the world. Still, even if the benefits of the GDPR have been broadly recognised, there is substantial critique by civil society and regulators, that there is insufficient monitoring of how the collected data is actually used by the companies and other entities, that big companies find ways to harvest user/consumer/people's data with minimal/no consent, and that the GDPR is too complicated for the general public, leading people to give up on their privacy rights. This becomes evident, as the EUMEPLAT research shows (WP3), in the case of video-on-demand platforms. In the latter case, both a. meaningful options for users to opt out from having their viewing behaviour tracked, without losing much of the platforms' affordances, and b. user-friendly transparency as it concerns how users' viewing behaviour data are used by the platforms, are in practice inadequate.

One other area of interest in the EUMEPLAT research concerns the European citizens' perceptions regarding surveillance by the EU and/or the nation states, and the citizens' responses of resistance, as they are expressed in social media platforms (WP2), which often bear an antisystemic character. One issue that merits further exploration is how European citizens perceive surveillance, at the national and European level, taking into account the dimension of trust (in the state, the EU, civil society, etc.). Distrust in authorities may be connected to citizens' beliefs that they are subjected to (enhanced) surveillance. Thus, citizens' disobedience against state and authorities' control, expressed as antisystemic resistance, may be related to their feeling of distrust towards authorities and institutions, and might be complemented, or not, with trust in fellow citizens, communities or civil society.

Low levels of political or institutional trust, as literature suggests, may be related to high citizen engagement and involvement in democratic governance (see, e.g., Hall, 2021; Kaase, 1999; Verde Garrido, 2021). At the same time, the echo chambers of disinformation which flourish online, and which sometimes activate forms of resistance to what is considered as control and surveillance, point to trust being displaced from state/authorities and institutions, such as science, education and academia, to anti-science/pseudoscience and alternative fields of knowledge creation. The anti-vaccination resistance, which was highlighted in the EUMEPLAT research, is one example that illustrates how citizens resist and develop acts of disobedience against state/ EU/authorities' control, using social media platforms as networking spaces where they can consolidate their views, but also coordinate forms or resistance. In this regard, disinformation may be a (conscious) act of resistance against state/ authority /science/ EU control and discipline, which merits further exploration. Of course, resistance against the EU/state/authority extends the logics and boundaries of resistance to surveillance, but the latter is an integral part of the former.

Another area of consideration is how Euroscepticism develops and how it intersects with diverse concerns and claims, such as surveillance and protection from it. The EUMEPLAT research showed that the EU is sometimes seen as a surveillant assemblage and Euroscepticism takes the form of resistance to a surveillant EU. Hence, Euroscepticism may be part of a broader scepticism against authorities (that impose surveillance), founded in libertarian, left-wing or anarchist ideologies, while in other cases, it may be founded in ethnocentric or right-wing nationalist ideologies, constructing an antagonism of Europe/EU versus 'our' state/nation, based on which Europe/EU surveils us aiming to control and dominate our state/nation.

Of relevance for further consideration is also the EUMEPLAT research that highlights that migration in Europe is addressed on social media mainly as an issue of border control (WP4). These discussions on social media seem to be echoing the strong appeal for tighter surveillance systems of control of the European borders, and for the regulation of movement of the migrants and asylum seekers within the European/EU territory. These findings are in alignment with research pointing to an increase in the securitisation discourse in Europe (Geddes et al., 2020; Huysmans, 2000; Karamanidou, 2015).

As the EUMEPLAT research showed, while the public discussion on migration still addresses human rights and values, there seems to be a shift in the focus of the discussion -from human rights to border controls – which has series of implications that extend the debates on how to manage the migration flows. It points to a change in the qualities of democratic dialogue and in the prioritisation of what are considered as the European values of tolerance, inclusion and solidarity. Furthermore, this appeal for tighter controls of the migration flows, and restriction of migrants' and asylum seekers' mobility once they have entered the EU space, enabled through sophisticated surveillance systems, is likely to have broader implications for Europe. The demands for more 'order and security' might impact on the broader organisation of the European space, and thus on the freedoms of mobility and movement, principles on which the idea of Europe as an open and shared space has been built.

The analysis of the future scenarios pertaining to surveillance/resistance in Europe (WP5) highlighted one important aspect, namely how people's visions of surveillance/resistance are fed by their attitudes towards technology. As the analysis showed, the scenarios imagining surveillance/resistance are anchored in techno-pessimist or techno-optimist approaches that construct specific visions of the future. The techno-pessimist visions tend to imagine more enhanced forms of surveillance and less opportunities for resistance. These visions also express concerns regarding the future of Europe, as either succumbing to corporate pressures, failing thus to project its citizens from enhanced forms of corporate surveillance, or as becoming more authoritarian, giving up some of its democratic freedoms and values. Of particular interest in these dystopic visions is the state/Europe-corporate nexus gaining prominence and leading to enhanced forms of surveillance in conditions of shrinking democracy and powerful corporate interests that will leave citizens highly exposed and unprotected.

Even if the scenarios that are anchored in techno-pessimism are more frequent, and also more detailed in their often-dystopian descriptions of the future, some of the scenarios and their visions of the future, anchored in techno-optimism do leave space for a more democratic, inclusive and socially fair Europe. These visions imagine increased levels of participation by the citizens in social organisation, and enhanced social responsibility. Such visions are related to considerable levels of societal or institutional trust, but also to higher levels of compliance to forms of what is perceived as socially responsible surveillance.

The series of issues that have been identified through the EUMEPLAT research and have been addressed in this deliverable are indicative of broader tensions and challenges in Europe, as it concerns the debates concerning supervision, control and surveillance, as there are pressures for both more and less control in Europe and the EU. These debates and tensions concern mainly the following expectations and demands:

- Europe should exercise more control over the corporate sector
- Europe should exercise less control over its subjects/citizens/nation states
- Europe should exercise more control over its borders

In these debates, there are also diverging positions –for instance the argument that Europe should exercise more control over its citizens or less control over its borders– but these positions appear to be less prominent in public discourse. The different debates around surveillance and control are also connected to different levels of trust and distrust in European institutions /Europe, being part of the struggles over what constitutes Europe, and over the desired and undesired futures for Europe.

7. References

Academic references

Aaltola, E. (2010). Green anarchy: Deep ecology and primitivism. In B. Franks and M. Wilson (eds), *Anarchism and moral philosophy*. Basingstoke: Palgrave Macmillan. pp.161–185.

Adorno, T., & Horkheimer, M. (2002 [1947]). *Dialectic of Enlightenment*. Stanford: Stanford University Press.

Akbari, A., & Gabdulhakov, R. (2019). Platform surveillance and resistance in Iran and Russia: The case of Telegram. *Surveillance & Society, 17*(1/2), 223–231.

Albrecht, H.-J. (2002). Fortress Europe? – Controlling illegal immigration. *European Journal of Criminal Law and Criminal Justice*, *10*(1), 1–22.

Allen, A. L. (2008). The virtuous spy: Privacy as an ethical limit. *The Monist, 91*(1), 3–22.

Alvesson, M., & Sköldberg, K. (2000). *Reflexive methodology. New vistas for qualitative research*. London: Sage.

Amadae, S. M. (2003). *Rationalizing capitalist democracy: The cold war origins of rational choice liberalism.* Chicago: University of Chicago Press.

Andreassen, R. (2021). Social media surveillance, LGBTQ refugees and asylum: How migration authorities use social media profiles to determine refugees as 'genuine' or 'fraudulent'. *First Monday 26*(1), DOI: https://dx.doi.org/10.5210/fm.v26i1.10653.

Arbogast, L. (2016). *Migrant detention in the European Union: a thriving business*. Brussels: Migreurop/Rosa Luxemburg Stiftung.

Arteaga, N. (2017). Mexico: Internal security, surveillance, and authoritarianism. *Surveillance & Society, 15*(3/4), 491–495.

Bakioğlu, B. S. (2016). The gray zone: Networks of piracy, control, and resistance. *The Information Society*, *32*(1), 40-50.

Barocas, S., & Nissenbaum, H. (2014). Big data's end run around anonymity and consent. In J. Lane, V. Stodden, S. Bender and H. Nissenbaum (eds.), *Privacy, big data, and the public good: Frameworks for engagement* (pp. 44–75). New York: Cambridge University Press.

Bauman, Z. (2004). *Wasted lives: Modernity and its outcasts*. Cambridge, MA: Polity.

Bellanova, R., & Glouftsios, G. (2022). Controlling the Schengen Information System (SIS II): The infrastructural politics of fragility and maintenance. *Geopolitics*, *27*(1), 160-184.

Björklund, F. (2021). Trust and surveillance: An odd couple or a perfect pair? In L. A.Viola and P. Laidler (eds.), *Trust and transparency in an age of surveillance* (pp. 183-200). London: Routledge.

Boshnakova, D., et al. (2023a). Deliverable 3.2. Patterns in platform video production in ten countries. EUMEPLAT. https://www.eumeplat.eu/wp-content/uploads/2023/05/D3.2_Patterns-in-Platform-Video-Production-in-ten-Countries.pdf

Boshnakova, D., et al. (2023b). Deliverable 3.3. Patterns in platform video consumption in ten countries. EUMEPLAT. https://www.eumeplat.eu/wp-content/uploads/2023/05/D3.3_Patterns-in-Platform-Video-Consumption-in-ten-Countries.pdf

Bouliane, N. (2017). How to stream or torrent movies in Germany, All About Berlin. https://allaboutberlin.com/guides/pirating-streaming-movies-in-germany (Accessed July 7, 2023).

Broeders, D. (2009). *Breaking down anonymity: Digital surveillance of irregular migrants in Germany and the Netherlands*. Amsterdam: Amsterdam University Press.

Broeders, D. (2007). Irregular migrants, the new digital borders of Europe: EU databases and the surveillance of irregular migrants. *International Sociology,* 22(1), 71–92.

Brosnan, M. (1998). *Technophobia: The psychological impact of information technology*. London: Routledge.

Campbell, J. E., & Carlson, M. (2002). Panopticon.com: Online surveillance and the commodification of privacy. *Journal of Broadcasting & Electronic Media, 46*(4), 586–606.

Cardoso, G., et al. (2023). Deliverable D2.2. Citizen journalism in ten countries. EUMEPLAT. https://www.eumeplat.eu/wp-content/uploads/2023/03/D2.2_Platformisation-of-News-in-10-Countries.pdf

Carpentier, N. (2021). The European assemblage: A discursive-material analysis of European identity, Europaneity and Europeanisation. *Filosofija. Sociologija*, *32*(3), 231-239.

Cinnamon, J. (2017). Social injustice in surveillance capitalism. *Surveillance & Society, 15*(5), 609–625.

Clarke, R. V. (2005). Seven misconceptions of situational crime prevention. In N. Tilley (ed.), *Handbook of crime prevention and community safety* (pp. 39–70). Abingdon: Routledge.

Cockfield, A. J. (2003). Who watches the watchers – A law and technology perspective on government and private sector surveillance. *Queen's Law Journal, 29*, 364–407.

Coleman, R. (2004). Images from a neoliberal city: The state, surveillance and social control. *Critical Criminology, 12*(1), 21–42.

Costanza, S. (2018). Surveillance. In A. Treviño (ed.), *The Cambridge handbook of social problems, Vol. 2* (pp. 95–108). Cambridge: Cambridge University Press.

Coutin, S. B. (1993). *The culture of protest: Religious activism and the US sanctuary movement*. Boulder, CO: Westview Press.

Davis, D. W., & Silver, B. D. (2003). Civil liberties vs. security: Public opinion in the context of the terrorist attacks on America. *American Journal of Political Science, 48*(1), 28– 46.

Degli Esposti, S. (2014). When big data meets dataveillance: The hidden side of analytics. *Surveillance & Society, 12*(2), 209–225.

Della Porta, D. (2017). Political economy and social movement studies: The class basis of anti-austerity protests. *Anthropological Theory*, *17*(4), 453-473.

Dencik, L., Hintz, A., & Cable, J. (2016). Towards data justice? The ambiguity of anti-surveillance resistance in political activism. *Big Data & Society*, *3*(2), 1–12.

Drotner, K. (2002). New media, new options, new communities?. *Nordicom Review*, *23*(1/2), 11–22. shorturl.at/mzJU3

Dupont, B. (2008). Hacking the panopticon: Distributed online surveillance and resistance. In M. Deflem and J. T. Ulmer (eds.), *Surveillance and governance: Crime control and beyond* Bingley: Emerald Publishing, pp. 257–278.

Ellis, D., Harper, D., & Tucker, I. (2013). The dynamics of impersonal trust and distrust in surveillance systems. *Sociological Research Online* 18(3), 8, DOI:10.5153/ sr0.3091.

Engbersen, G. (2001). The unanticipated consequences of panopticon Europe: Residence strategies of illegal immigrants. In V. Guiraudon and C. Joppke (eds.), *Controlling a new migration world* (pp. 222–246). London: Routledge.

Engbersen, G., & Breeders, D. (2009). The state versus the alien: Immigration control and strategies of irregular immigrants. *West European Politics, 32*(5), 867–885.

Epanchin-Niell, R. S., Haight, R. G., Berec, L., Kean, J. M., & Liebhold, A. M. (2012). Optimal surveillance and eradication of invasive species in heterogeneous landscapes. *Ecology letters*, *15*(8), 803-812.

Ess, C. (2014). *Digital media ethics*. Cambridge: Polity.

European Central Bank. (2023). *About*. [Retrieved from https://www.ecb.europa.eu/ecb/html/index.en.html]

European Commission (2023, February 23). Commission strengthens cybersecurity and suspends the use of TikTok on its corporate devices. Press Release. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_1161

European Commission (n.d.). Press Corner, European Commission. Retrieved August 29, 2023, from https://ec.europa.eu/commission/presscorner/detail/%20en/ip_23_3565

European Commission (n.d.). *Walls and fences at EU borders*. Europa.Eu. [Retrieved from https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733692]

European Parliament (2018, September 26). Audiovisual media: MEPs approve new rules fit for a digital age. https://www.europarl.europa.eu/news/en/headlines/society/20180920STO14026/audiovisual-media-meps-approve-new-rules-fit-for-a-digital-age

Fernandez, L. A., & Huey, L. (2009). ls resistance futile? Some thoughts on resisting surveillance. *Surveillance & Society, 6*(3), 198–202.

Fernback, J. (2013). Sousveillance: Communities of resistance to the surveillance environment. *Telematics and Informatics*, *30*(1), 11–21.

Filipiak, B. Z., & Wyszkowska, D. (2022). Fiscal stability in EU countries. *Wiadomości Statystyczne. The Polish Statistician*, *67*(8), 17-40.

Filliss, J. 2019. What is Primitivism? https://web.archive.org/web/20190730185307/http://www.primitivism.com/what-is-primitivism.htm [accessed 9 September 2023].

Foucault, M. (2008). *The birth of biopolitics: Lectures at the Collège de France, 1978-1979*. New York: Palgrave Macmillan.

Foucault, M. (2007). *Security, territory, population: Lectures at the Collège de France, 1977-1978*. New York: Palgrave Macmillan.

Foucault, M. (2003). *'Society must be defended': Lectures at the Collège de France, 1975-76*. New York: Palgrave Macmillan.

Foucault, M. (1997). *Ethics: Subjectivity and truth* (P. Rabinow, ed.). New York: The New Press.

Foucault, M. (1990). *The History of Sexuality. Vol 1: An Introduction*. New York: Vintage Books. (Original work published 1978)

Foucault, M. (1977). *Discipline and punish: The birth of the prison*. New York: Random House.

Fox, N. (2002). *Against the machine: The hidden Luddite tradition in literature, art, and individual lives*. Washington: Island Press.

Freeman, M. (2006). Terrorism and civil liberties in the United States: How to have both freedom and security. *Democracy and Security, 2*(2), 231–261.

French, M., & Monahan, T. (2020). Editorial: Dis-ease surveillance: How might surveillance studies address COVID-19?. *Surveillance & Society, 18*(1), 1-11.

Friedewald, M. et al. (2016). The context-dependence of citizens' attitudes and preferences regarding privacy and security. In S. Gutwirth et al. (eds.), *Data protection on the move: Current developments in ICT and privacy/data protection* (pp. 51-74). Dordrecht: Springer.

Fuchs, C. (2014). *Social media: A critical introduction*. London: Sage.

Fuchs, C. (2013). Political economy and surveillance theory. *Critical Sociology, 39*(5), 671–687.

Fuchs, C. (2011a). Web 2.0, prosumption, and surveillance. *Surveillance & Society, 8*(3), 288–309.

Fuchs, C. (2011b). How to define surveillance? *MATRIZ- es*, *5*(1), 109-133.

Fuchs, C. (2010). Labor in informational capitalism and on the internet. *The Information Society, 26*(3), 179–196.

Gabrielsen Jumbert, M., Bellanova, R. & Gellert, R. (2018). Smart phones for refugees. Tools for survival, or surveillance?. PRIO Policy Brief, 4. Oslo: PRIO.

Galeazzi, A., & Zollo, F. (2021). Deliverable D2.5. Anti-European fake news and what to do. EUMEPLAT. https://www.eumeplat.eu/wp-content/uploads/2022/11/D2.5 Anti-European-Fake-News-and-What-to-Do.pdf

Gandy, O. H. (1993). *The Panoptic sort: A political economy of personal information*. Boulder, CO: Westview Press.

Geddes, A., Hadj-Abdou, L., & Brumat, L. (2020). *Migration and mobility in the European Union*. London: Bloomsbury Publishing.

Giddens, A. (1984). *The Constitution of Society: Outline of the theory of structuration*. Cambridge: Polity Press.

Gilliom, J. (2001). *Overseers of the poor: Surveillance, resistance, and the limits of privacy*. Chicago: University of Chicago Press.

Glenn, J. C. (2009). Introduction to the Futures Research Methods Series. In J. C. Glenn and T. Gordon (eds.), *Futures research methodology — Version 3.0.* Washington: The Millennium Project, pp. 1-106.

Gordon, T. (2009). Delphi. In J. C. Glenn and T. Gordon (eds.), *Futures research methodology — Version 3.0.* Washington: The Millennium Project, pp. 1-29.

Grassmuck, V., & Thomass, B. (2022). Deliverable D1.4. European media legislation: Overview - Milestones in European Media policies and legislation, 1990-2020. EUMEPLAT. https://www.eumeplat.eu/wp-content/uploads/2022/03/D1.4_European-Media-Legislation.pdf

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA and the surveillance state*. London: Hamish Hamilton.

Gregory, K., & Sadowski, J. (2021). Biopolitical platforms: the perverse virtues of digital labour. *Journal of Cultural Economy*, *14*(6), 662-674.

Gruber, S. (2013). Trust, identity and disclosure - Are Bitcoin exchanges the next virtual havens for money laundering and tax evasion? *Quinnipiac Law Review*, *32*(1), 135–208.

Haggerty, K. D. (2006). Tear down the walls: on demolishing the Panopticon. In D. Lyon (ed.), *Theorizing surveillance* (pp. 37–59). Devon: Willan Publishing.

Haggerty, K. D., & Ericson, R. V. (eds.). (2006). *The new politics of surveillance and visibility. Toronto*: University of Toronto Press.

Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *The British Journal of Sociology, 51*(4), 605–622.

Hall, M. (2021). A neo-republican critique of transparency. The chilling effects of publicizing power. In L. A. Viola and P. Laidler (eds), *Trust and transparency in an age of surveillance* (pp. 47-64). Oxon: Routledge.

Hansen, M. H., & Svarverud, R. (2010). *iChina: The rise of the individual in modern Chinese society*. Copenhagen: Nordic Institute of Asian Studies (NIAS).

Helm, P., & Seubert, S. (2020). Normative paradoxes of privacy: Literacy and choice in platform societies. *Surveillance & Society, 18*(2), 185–198.

Hermoso, V., et al. (2022). The EU Biodiversity Strategy for 2030: Opportunities and challenges on the path towards biodiversity recovery. *Environmental Science & Policy, 127*, 263-271.

Hintjens, H. M. (2013). Screening in or out? Selective non-surveillance of unwanted humanity in EU cities. *Surveillance & Society, 11*(1/2), 87–105.

Hollander, J., & Einwohner, R. (2004). Conceptualizing resistance. *Sociological Forum, 19*(4), 533–554.

Holm, N. (2009). Conspiracy theorizing surveillance: Considering modalities of paranoia and conspiracy in surveillance studies. *Surveillance & Society 7*(1), 36–48.

Hou, R. (2017). Neoliberal governance or digitalized autocracy? The rising market for online opinion surveillance in China. *Surveillance & Society, 15*(3/4), 418–424.

Huey, L., Walby, K., & Doyle, A. (2006). Cop watching in the downtown eastside: Exploring the use of (counter)surveillance as a tool of resistance. In T. Monahan (ed.), *Surveillance and security: Technological politics and power in everyday life* (pp. 149–165). New York: Routledge.

Huysmans, J. (2000). The European Union and the securitization of migration. *JCMS: Journal of Common Market Studies*, *38*(5), 751-777.

Inayatullah, S. (2012). Futures studies. Theories and methods. In F. Gutierrez Junquera (ed.) *There's a future: Visions for a better world*. Madrid: BBVA, pp. 37-65.

Ingebretsen Carlson, J., et al. (2023). Deliverable D4.2. Representation of immigration in ten countries. Work package 4 – Analysing the Europeanisation and platformization of media representations. EUMEPLAT. https://www.eumeplat.eu/wp-content/uploads/2023/05/D4.2_Representation-of-Immigration-in-ten-Countries.pdf

Introna, L., & Gibbons, A. (2009). Networks and resistance: Investigating online advocacy networks as a modality for resisting state surveillance. *Surveillance & Society, 6*(3), 233–258.

Jansson, A. (2012). Perceptions of surveillance: Reflexivity and trust in a mediatized world (the case of Sweden). *European Journal of Communication*, *27*(4), 410-427.

Jiang, Z. Z., Cui, S., He, N., Li, K., & Tian, L. (2023). Contract selection and piracy surveillance for video platforms in the age of social media. *Production and Operations Management*, *00*, 1–17. https://doi.org/10.1111/poms.13990

Johnston, H., & Land-Kazlauskas, C. (2019). Organizing on-demand: Representation, voice, and collective bargaining in the gig economy. Geneva: International Labour Organization. https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---travail/documents/publication/wcms_624286.pdf

Jones, S. E. (2006). *Against technology: from the Luddites to Neo-Luddism*. New York: Routledge.

Kaase, M. (1999). Interpersonal trust, political trust and non- institutionalized political participation in Western Europe. *West European Politics, 22*(3), 1– 21.

Kahn, H. (1962). *Thinking about the unthinkable*. New York, NY: Horizon Press.

Kaine, S., & Josserand, E. (2019). The organisation and experience of work in the gig economy. *Journal of Industrial Relations*, *61*(4), 479–501.

Karamanidou, L. (2015). The securitisation of European migration policies: Perceptions of threat and management of risk. In G. Lazaridis and Wadia, K. (eds), *The Securitisation of Migration in the EU: Debates since 9/11*. Houndmills: Palgrave Macmillan, pp. 37-61.

Knill, C., & Lenschow, A. (eds.). (2000). *Implementing EU environmental policy: New directions and old problems*. Manchester University Press.

Königs, P. (2022). What is Techno-Optimism?. *Philosophy & Technology* 35, 63 https://doi.org/10.1007/s13347-022-00555-x

Koskela, H. (2011). 'Don't mess with Texas!' Texas Virtual Border Watch Program and the (botched) politics of responsibilization. *Crime, Media, Culture, 7*(1), 49–65.

Koskela, H. (2000). 'The gaze without eyes': Video-surveillance and the changing nature of urban space. *Progress in Human Geography, 24*(2), 243–265.

Laffan, B., & Schlosser, P. (2016). Public finances in Europe: Fortifying EU economic governance in the shadow of the crisis. *Journal of European integration*, *38*(3), 237-249.

Landeta, J. (2006). Current validity of the Delphi method in social sciences. *Technological Forecasting and Social Change*, *73*(5), 467–482.

Latour, B. (2005). *Reassembling the social*. Oxford: Oxford University Press.

Latour, B. (2000). When things strike back: a possible contribution of 'science studies' to the social sciences. *British Journal of Sociology, 51*(1), 107–123.

Lindgren, S. (2017). *Digital media and society*. London: Sage.

Liu, C. (2021). Chinese public's support for COVID-19 surveillance in relation to the West. *Surveillance & Society, 19*(1), 89–93.

Łoś, M. (2003). Crime in transition: The post-communist state, markets, and crime. *Crime, Law and Social Change, 40*(2/3), 145–169.

Lü, Y. H. (2005). Privacy and data privacy issues in contemporary China. *Ethics and Information Technology*, *7*(1), 7–15.

Lubbers, E. (2015). Undercover research—Corporate and police spying on activists. An introduction to activist intelligence as a new field of study. *Surveillance & Society, 13*(3/4), 338–353.

Lyon, D. (2022a). Reflections on forty years of 'surveillance studies'. *Surveillance & Society, 20*(4), 353–356.

Lyon, D. (2022b). Surveillance. *Internet Policy Review*, *11*(4). https://doi.org/10.14763/2022.4.1673

Lyon, D. (2018). *The Culture of surveillance*. Cambridge: Polity Press.

Lyon, D. (2017). Bentham's Panopticon: From moral architecture to electronic surveillance. In D. Wilson and C. Norris (eds.), *Surveillance, crime and social control* (pp. 13–34). London: Routledge.

Lyon, D. (2014). Surveillance, Snowden, and big data: Capacities, consequences and critique. *Big Data and Society, 1*(2), 1–13.

Lyon, D. (2007). *Surveillance studies: An overview*. Cambridge: Polity.

Lyon, D. (ed.). (2006). *Theorizing surveillance: The panopticon and beyond*. Cullompton: Willan Publishing.

Lyon, D. (ed.). (2003). *Surveillance as social sorting. Privacy, risk and automated discrimination*. London: Routledge.

Lyon, D. (2001a). *Surveillance society: Monitoring everyday life*. Buckingham: Open University Press.

Lyon, D. (2001b). Facing the future: Seeking ethics for everyday surveillance. *Ethics and Information Technology, 3*, 171–181.

MacKinnon, R. (2011). China's networked authoritarianism. *Journal of Democracy, 22*(2), 32–46.

Macnish, K. (2014). Just surveillance: Towards a normative theory of surveillance. *Surveillance & Society, 12*(1), 142-153.

Mahraj, K., Chaiyachati, K. H., Asch, D. A., Fala, G., Do, D., Lam, D., Miller, A., Mannion, N., Stoloff, V., Halbritter, A., & Huffenberger, A. M., (2021). Developing a large-scale Covid-19 surveillance system to reopen campuses. *NEJM Catalyst Innovations in Care Delivery*, *2*(6), DOI: DOI: 10.1056/CAT.21.0049.

Mann, S. (2020). Wearables and sur(over)-veillance, sous(under)-veillance, co(so)-veillance, and metaveillance (veillance of veillance) for health and well-being. *Surveillance & Society 18*(2), 262-271.

Mann, S. (2016). Surveillance, sousveillance, and metaveillance. In The IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops, Las Vegas, NV, June 26–July 1, 1408–1417. https://doi.org/10.1109/CVPRW.2016.117.

Mann, S. (2004). Sousveillance: Inverse surveillance in multimedia imaging. *MULTIMEDIA '04: Proceedings of the 12th annual ACM international conference on Multimedia*, 620–627. https://dl.acm.org/doi/10.1145/1027527.1027673

Mann, S., Nolan, J., & Wellman, B. (2003). Sousveillance: Inventing and using wearable computing devices for data collection in surveillance environments. *Surveillance & Society, 1*(3), 331–355.

Marchetti, S., & Salih, R. (2017). Policing gender mobilities: interrogating the 'feminisation of migration' to Europe. *International Review of Sociology*, *27*(1), 6–24.

Marchetti, S., & Salih, R. (2015). Gender and mobility across Southern and Eastern European borders: "Double standards" and the ambiguities of European neighbourhood policy, *Instituto Affari Internazionali*, 1-25.

Maréchal, G. (2010). Autoethnography. In A. J. Mills, G. Durepos & E. Wiebe (Eds.), *Encyclopedia of case study research* (vol. 2), (pp. 43–45). Thousand Oaks, CA: Sage.

Martin, A. K., Van Brakel, R., & Bernhard, D. (2009). Understanding resistance to digital surveillance: Towards a multi-disciplinary, multi-actor framework. *Surveillance & Society, 6*(3), 213–232.

Marwick, A., & Lewis, R. (2017). *Media manipulation and disinformation onlin*e. New York: Data & Society Research Institute.

Marx, G. T. (2009). A tack in the shoe and taking off the shoe: Neutralization and counter-neutralization dynamics. *Surveillance & Society*, *6*(3), 294–306.

Marx, G. T. (2003). A tack in the shoe: Neutralizing and resisting the new surveillance. *Journal of Social Issues, 59*(2), 369–390.

Marx, G. T. (1998). Ethics for the new surveillance. *The Information Society, 14*, 171–185.

Matthews, R., & Ross, E. (2010). *Research methods: A practical guide for the social sciences*. Harlow: Pearson Education.

Matzner, T. (2014). Why privacy is not enough privacy in the context of 'ubiquitous computing' and 'big data'. *Journal of Information, Communication and Ethics in Society, 12*(2), 93–106.

McCahill, M., & Finn, R. (2014). *Surveillance, capital and resistance: Theorizing the surveillance subject*. New York: Routledge.

Miconi, A., et al. (2022). Deliverable D2.3. Positive and negative externalities of news platformization. EUMEPLAT. https://www.eumeplat.eu/wp-content/uploads/2022/11/D2.3_Positive-and-Negative-Externalities-of-News-Platformization.pdf

Miconi, A. et al. (2023). Deliverable D3.4. Catalogue of best practices and main obstacles to Europeanisation. EUMEPLAT. https://www.eumeplat.eu/wp-content/uploads/2023/03/D3.4_Catalogue-of-Best-Practices-and-Main-Obstacles-to-Europeanisation.pdf

Monaci, S., & Persico, S. (2023). Who's fuelling Twitter disinformation on the COVID-19 vaccination campaign? Evidence from a computational analysis of the green pass debate. *Contemporary Italian Politics*. DOI: 10.1080/23248823.2023.2182735.

Monahan, T. (2006). Counter-surveillance as political intervention? *Social Semiotics, 16*(4), 515–534.

Monahan, T., & Murakami Wood, D. (2022). Revitalizing dissent: Imperatives for critical surveillance inquiry. *Surveillance & Society, 20*(4), 326–332.

Morozov, E. (2013). *To save everything, click here*. New York: Public Affairs.

Morozov, E. (2011). *The net delusion*. New York: Public Affairs.

Movsisyan, N. K., Vinciguerra, M., Medina-Inojosa, J. R., & Lopez-Jimenez, F. (2020). Cardiovascular diseases in central and eastern Europe: A call for more surveillance and evidence-based health promotion. *Annals of Global Health*, *86*(1), DOI: doi: 10.5334/aogh.2713.

Murakami Wood, D. (ed.). (2006). *A Report on the Surveillance Society.* Surveillance Studies Network. https://rb.gy/pkuejq

Nakada, M., & Tamura, T. (2005). Japanese conceptions of privacy: An intercultural perspective. *Ethics and Information Technology*, *7*(1), 27–36.

Nedelcu, M., & Soysüren, I. (2022). Precarious migrants, migration regimes and digital technologies: The empowerment-control nexus. *Journal of Ethnic and Migration Studies*, *48*(8), 1821-1837.

Negroponte, N. (1995). *Being digital*. New York: Knopf.

Newell, B. C., Gomez, R., & Guajardo, V. E. (2017). Sensors, cameras, and the new 'normal' in clandestine migration: How undocumented migrants experience surveillance at the U.S.-Mexico border. *Surveillance & Society, 15*(1), 21–41.

Newlands, G. (2021). Algorithmic surveillance in the gig economy: The organization of work through Lefebvrian conceived space. *Organization Studies*, *42*(5), 719-737.

Newton, K., & Zmerli, S. (2011). Three forms of trust and their association. *European Political Science Review, 3*(2), 169– 200.

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford, CA: Stanford University Press.

Nurik, C. L. (2022). Facebook and the surveillance assemblage: Policing Black Lives Matter activists & suppressing dissent. *Surveillance & Society, 20*(1), 30–46.

Paal, B. (2022). Artificial intelligence as a challenge for data protection law: And vice versa. In S. Voeneky, P. Kellmeyer, O. Mueller and W. Burgard (eds.), *The Cambridge handbook of responsible artificial intelligence: Interdisciplinary perspectives* (pp. 290–308). Cambridge: Cambridge University Press.

Pan, S. Q., et al. (1996). A mini-Delphi approach: An improvement on single round techniques. *Progress in Tourism and Hospitality Research*, *2*(1), 1-109.

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Cambridge, MA: Harvard University Press.

Pavone, V., Degli- Esposti, S., & Santiago, E. (2015). Key factors affecting public acceptance and acceptability of surveillance- oriented security technologies (SOSTs). SurPRISE project deliverable 2.4. Florence: European University Institute. DOI: 10.13140/2.1.2400.8003

Poli, R. (2018). A note on the classification of future-related methods. *European Journal of Futures Research, 6*(1), 1-7.

Postman, N. (1992). *Technopoly: The surrender of culture to technology*. New York: Knopf.

Ramiro Troitiño, D. (2023). Mapping E-governance in the EU. In D. Ramiro Troitiño, T. Kerikmäe and O. Hamuák (eds.), *Digital Development of the European Union: An Interdisciplinary Perspective.* Cham: Springer International Publishing, pp. 303-317.

Renieris, E. M. (2021). What's really at stake with vaccine passports. *Surveillance & Privacy. Center for International Governance Innovation* [Retrieved from https://www.cigionline.org/articles/whats-really-stake-vaccine-passports/].

Reynolds, G. (2010). Pirate Bay on English Bay? Bittorrent file sharing and copyright infringement in the Supreme Court of British Columbia. *University Of British Columbia Law Review*, *43*(1), 193-204.

Richards, N. M. (2012). The dangers of surveillance. *Harvard Law Review, 126*, 1934–1965.

Richmond, A. (1994). *Global apartheid: Refugees, racism and the new world order*. Oxford and New York: Oxford University Press.

Ridley, M. (2010). *The rational optimist: How prosperity evolves*. New York: Harper Collins.

Robertson, B., & Marchant, J. (eds.). (2018). *Revolution decoded: Iran's digital landscape*. Small Media. https://smallmedia.org.uk/revolutiondecoded/a/RevolutionDecoded.pdf

Robinson, J. B. (1988). Unlearning and backcasting: Rethinking some of the questions we ask about the future. *Technological Forecasting and Social Change*, *33*, 325-338.

Roettgers, J. (2019, June 5). How Amazon recommends movies on Prime Video. *Variety*, https://variety.com/2019/digital/news/amazon-prime-video-algorithms-1203233844

Rüdig, W., & Karyotis, G. (2014). Who protests in Greece? Mass opposition to austerity. *British Journal of Political Science*, *44*(3), 487-513.

Sadowski, J., (2020). The internet of landlords: Digital platforms and new mechanisms of rentier capitalism. *Antipode*, *52*(2), 562–580.

Saldaña, J. (2013). *The coding manual for qualitative researchers* (2nd ed). London: Sage.

San-Jose, L., & Retolaza, J. L. (2016). Is the Delphi method valid for business ethics? A survey analysis. *European Journal of Futures Research*, *4*(1), 1-15.

Saulnier, A. (2017). Surveillance as communicating relational messages: Advancing understandings of the surveilled subject. *Surveillance & Society, 15*(2), 286-302.

Schade, F. (2023). Dark sides of data transparency: organized immaturity after GDPR? *Business Ethics Quarterly,* 1–29. doi:10.1017/beq.2022.30

Schroeder, T. C., & Tonsor, G. T. (2012). International cattle ID and traceability: Competitive implications for the US. *Food Policy*, *37*(1), 31-40.

Scott, J. C. (1987). Resistance without protest and without organization: Peasant opposition to the Islamic Zakat and the Christian Tithe. *Comparative Studies in Society and History, 29*(3), 417–452.

Seefried, E. (2014). Steering the future. The emergence of 'Western' futures research and its production of expertise, 1950s to early 1970s. *European Journal of Futures Research, 2*(1), 29.

Sewell, G., & Barker, J. R. (2001). Neither good, nor bad, but dangerous: Surveillance as an ethical paradox. *Ethics and Information Technology, 3*, 183–196.

Spinelli, A., Buoncristiano, M., Nardone, P., Starc, G., Hejgaard, T., Júlíusson, P. B., Fismen, A. S., Weghuber, D., Musić Milanović, S., García-Solano, M., & Rutter, H. (2021). Thinness, overweight, and obesity in 6-to 9-year-old children from 36 countries: The World Health Organization European Childhood Obesity Surveillance Initiative—COSI 2015–2017. *Obesity Reviews*, *22*, DOI: 10.1111/obr.13214

Stalder, F. (2002). Privacy is not the antidote to surveillance. *Surveillance & Society, 1*(1), 120–124.

Stockmann, D., & Gallagher, M. (2011). Remote control: How the media sustain authoritarian rule in China. *Comparative Political Studies, 44*(4), 1–32.

Strangelove, M. (2005). *The empire of mind: Digital piracy and the anti-capitalist movement*. Toronto: University of Toronto Press.

Strossen, N. (2007). Freedom and fear post-9/11: Are we again fearing witches and burning women? *Nova Law Review, 31(2),* 279–314.

Svenonius, O., & Bjorklund, F. (2018). Explaining attitudes to secret surveillance in post-communist societies. *East European Politics, 34*(2), 123–151.

Svenonius, O., & Tarasiva, E. (2021). 'Now we are struggling at least': Change & continuity of surveillance in post-communist societies from the perspective of data protection authorities. *Surveillance* & *Society, 19*(1), 53–68.

Sztompka, P. (1998). Trust, distrust and two paradoxes of democracy. *European Journal of Social Theory, 1*(1), 19–32.

Tavani, H. (2013). *Ethics and technology*: *Ethical issues in an age of information and communication technology* (*4th* ed.). Hoboken, NJ: Wiley.

Taylor, N. (2002). State surveillance and the right to privacy. *Surveillance & Society, 1*(1), 66–85.

Tene, O., & Polonetsky, J. (2012). Big data for all: Privacy and user control in the age of analytics. *Northwestern Journal of Technology and Intellectual Property, 11*(5), 239–273.

Tiwari, A., Adhikari, S., Kaya, D., Islam, M. A., Malla, B., Sherchan, S. P., Al-Mustapha, A. I., Kumar, M., Aggarwal, S., Bhattacharya, P., & Bibby, K. (2023). Monkeypox outbreak: Wastewater and environmental surveillance perspective. *Science of the Total Environment, 856*, DOI: 10.1016/j.scitotenv.2022.159166.

Topak, Ö. E. (2019). Humanitarian and human rights surveillance: The challenge to border surveillance and invisibility? *Surveillance & Society, 17*(3/4), 382–404.

Topak, Ö. E. (2014). The biopolitical border in practice: Surveillance and death at the Greece-Turkey borderzones. *Environment and Planning D: Society and Space, 32*(5), 815–833.

Topak, Ö. E., & Vives, L. (2020). A comparative analysis of migration control strategies along the Western and Eastern Mediterranean routes: Sovereign interventions through militarization and deportation. *Migration Studies*, *8*(1), 66–89.

Trappmann, V., Bessa, I., Joyce, S., Neumann, D., Stuart, M., & Umney, C. (2020). Global labour unrest on platforms. *The case of food delivery workers, Berlin:* FES.

Treré, E. (2016). The Dark side of digital politics: Understanding the algorithmic manufacturing of consent and the hindering of online dissidence. *IDS Bulletin, 47*(1), 127–138.

Tripoli, M., & Schmidhuber, J., (2020). Optimising traceability in trade for live animals and animal products with digital technologies. *Rev. Sci. Tech*, *39*(1), 235-244.

Vallas, S., & Schor, J. B. (2020). What do platforms do? Understanding the gig economy. *Annual Review of Sociology*, *46*, 273–294.

Veen, A., Barratt, T., & Goods, C. (2019). Platform-Capital's 'App-etite' for control: A labour process analysis of food-delivery work in Australia. *Work, Employment and Society, 34*(3), 388–406.

Verde Garrido, M. (2021). Why a militantly democratic lack of trust in state surveillance can enable better and more democratic security. In L. A. Viola, and P. Laidler (eds.), *Trust and transparency in an age of surveillance* (pp. 221-240). Oxon: Routledge.

Verde Garrido, M. (2015). Contesting a biopolitics of information and communications: The importance of truth and sousveillance after Snowden. *Surveillance & Society, 13*(2), 153–167.

Viola, L. A., & Laidler, P. (2021). On the relationship between trust, transparency, and surveillance. In L. A. Viola, and P. Laidler (eds.), *Trust and transparency in an age of surveillance* (pp. 3-18). Oxon: Routledge.

Vuori, J. A., & Paltemaa, L. (2015). The lexicon of fear: Chinese internet control practice in Sina Weibo microblog censorship. *Surveillance & Society, 13*(3/4), 400–421.

Walsh, J. (2013). Remapping the border: Geospatial technologies and border activism. *Environment and Planning D: Society and Space*, *31*(6), 969-987.

Walsh, J. (2010). From border control to border care: The political and ethical potential of surveillance. *Surveillance & Society*, *8*(2), 113-130.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, IV*(5), 193–220.

Winkler, J. & Moser, R. (2016). Biases in future-oriented Delphi studies: A cognitive perspective. *Technological Forecasting and Social Chang*e, 105, 63–76.

Winner L (1999 [1980]). Do artifacts have politics? In D. MacKenzie and J. Wajcman (eds), *The Social Shaping of Technology*. Maidenhead: Open University Press, pp. 28-40.

Wolf, R. A. (2014). Bitcoin and EU VAT. *The international VAT monitor*, *2014*(8), 254-257.

Wood, D. (2003). Foucault and panopticism revisited. *Surveillance & Society, 1*(3), 234–239.

Woodcock, J., & Graham, M. (2020). *The gig economy. A critical introduction.* Cambridge: Polity.

Yesil, B., & Sözeri, E. K. (2017). Online surveillance in Turkey: Legislation, technology and citizen involvement. *Surveillance & Society, 15*(3/4), 543–549.

Zuboff, S. (2020). Caveat usor: Surveillance capitalism as epistemic inequality. In K. Werbach (ed.), *After the digital tornado: Networks, algorithms, humanity* (pp. 174–214). Cambridge: Cambridge University Press.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. London: Profile Books.

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology, 30*(1), 75–89.

Other references

Charters and Conventions

European Convention on Human Rights (1950). https://www.echr.coe.int/documents/d/echr/Archives_1950_Convention_ENG

Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (1981). https://rm.coe.int/1680078b37

Charter of Fundamental Rights of the European Union (2000). http://data.europa.eu/eli/treaty/char_2012/oj

EU Decisions, directives, regulations

Communication from the Commission: The European Green Deal (COM/2019/640 final, 11.12.2019). https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1588580774040&uri=CELEX%3A52019DC0640

Decision (EU) on a General Union Environment Action Programme to 2030 (2022/591, 06.04.2022). http://data.europa.eu/eli/dec/2022/591/oj

Directive (EC) on the protection of individuals with regard to the processing of personal data and on the free movement of such data (95/46/EC, 24.10.1995). http://data.europa.eu/eli/dir/1995/46/oj

Directive (EC) concerning the processing of personal data and the protection of privacy in the telecommunications sector (97/66/EC, 15.12.1997). http://data.europa.eu/eli/dir/1997/66/oj

Directive (EC) concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive) (2002/58/EC, 12.07.2002). http://data.europa.eu/eli/dir/2002/58/oj

Directive (EC) on the obligation of carriers to communicate passenger data (2004/82/EC, 29.04.2004). http://data.europa.eu/eli/dir/2004/82/oj

Directive amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view (2018/1808/EU, 14.11.2018). http://data.europa.eu/eli/dir/2010/13/oj

Directive (EU) on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (DSMD) (2019/790/EU, 17.04.2019). http://data.europa.eu/eli/dir/2019/790/oj

Regulation (EC) on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (45/2001/EC, 18.12.2000). http://data.europa.eu/eli/reg/2001/45/oj

Regulation (EU) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016/679/EU, 27.04.2016). http://data.europa.eu/eli/reg/2016/679/oj