Does the end justify the means?

Information systems and control society in the age of pandemics

Aurélie Leclercq-Vandelannoitte[1*] and Jeremy Aroles[2]

[1] CNRS, LEM (URM 9221), IESEG School of Management, 59000 Lille, France. Email: a.leclercq@ieseg.fr

[2] Durham University, Durham University Business School, Mill Hill Lane, DH1 3LB, Durham, UK. Email address: Jeremy.aroles@durham.ac.uk

[*] Corresponding author

Abstract

As the COVID-19 pandemic unfolds, governments across the globe are enforcing various Information Systems (IS)-based systems of control that, we contend, augur a new organization of our freedoms, raising concerns related to issues of surveillance and control. Presented as ways to curb the immediate progression of the pandemic, these systems have progressively appertained our lives, thus becoming the new "normal". Drawing from the concept of "control societies" developed by Deleuze, we explore how, through a logic of "the end justifies the means", these new systems are being normalized. Beyond Deleuzian studies that describe modern society as a control society, we contend that Deleuze provides useful insights to critically analyse the progressive "normalization" of new forms of digitally-enabled control, as well as the implications of this normalization process. The analysis of this normalization process highlights the ways in which the current pandemic and its response (i.e. new forms of technological control) are *"sociomaterially constructed"* through a *historic, discursive and material process*. Contributing to MIS research on privacy and surveillance, this reflection on the sociomaterial construction of the control society and of its digitally-enabled control systems during the current COVID-19 crisis paves the way to possible forms of resistance and solutions.

Keywords: Control society; Deleuze; Information Systems; Normalization; Pandemics; Information Technology-based control; Surveillance; COVID-19 crisis; Sociomaterial construction

Introduction

On the grounds of health imperatives, new applications, technological devices and digital information infrastructures have been deployed in many countries to face the on-going COVID-19 crisis. These digital "solutions" range from Apps tracking contacts, movements and the spread of the virus, to drones reporting lockdown breaches and helping to enforce lockdown measures. Governments, public institutions, companies and increasingly individuals justify and legitimise the use of these systems for the sake of safety, thus auguring a new organization of our (henceforth much surveilled) freedoms. Unfortunately, the quick spread and impending nature of the virus have not given us the time and space required to step back and reflect on the far-reaching consequences of the deployment of these newly developed systems on individuals and society. Recent research has started to discuss the control and surveillance aspect of the COVID-19 crisis and of its technological solutions (Calvo et al., 2020; French & Monahan, 2020; Kitchin, 2020; Pingeot, 2020), leading us to wonder whether we can really give up our freedoms (momentarily) through the deployment of new forms of IT-based control and then expect to be able to get them back soon after.

In this paper, we aim to reflect on and conceptualize the development of new forms of IT-based control in response to the current pandemic and analyse their long-term implications, begging the question of whether the end can actually justify the means. To address this question, we draw from Gilles Deleuze's (1992, 1995, p. 174) concept of "societies of control". A great deal of research in Management of Information Systems (MIS), sociology and Management and Organization studies (MOS) has mobilized Deleuze's work to describe modern society and its pervasive, natural inclination to observe, survey and control people through digital technologies (see Brivot & Gendron, 2013; DeSaulles & Horner, 2011; Galic et al., 2016; Haggerty & Ericson, 2000; Leclercq-Vandelannoitte et al., 2014). However, while the parallel between modern societies and societies of control is now new *per se*, the

process through which such control societies become normalised has received less attention. We contend in this paper that the COVID-19 crisis constitutes a unique opportunity to understand the normalization process of control societies, and long-term implications of their digitally-enabled control systems. Beyond existing Deleuzian studies that define and describe control societies, we look in this paper at how the latter are constructed and normalized, through a focus on the current COVID-19 crisis, by asking the two following questions: To what extent do the new forms of digitally-enabled control developed to fight the COVID-19 crisis contribute to the development of a control society? How do this new type of society and underlying control systems become normalised?

We believe that Deleuze's (1990, 1992, 1995) conceptualization of control societies, coupled with his developments on deterritorialization and surveillance (Deleuze & Guattari, 1987), offers an insightful conceptual frame to critically explore the progressive "normalization" of new forms of control driven by technologies in the age of pandemics. A Deleuzian approach helps us analyse the founding mechanisms at the heart of the logic of societies of control. In particular, by highlighting the mechanisms through which newly developed systems draw the contours of a "control society" (Deleuze, 1992), and analysing how the current pandemic and its solution (i.e. new forms of digitally-enabled control) are gradually made 'normal', this paper highlights the *sociomaterial construction* of the crisis and of its response. We show how this process of *sociomaterial construction* relies on underlying operating methods (Deleuze, 1992) that constitute both the very problem (the fight against this invisible enemy) and its solutions (IT-based control), which are legitimized as appropriate forms of surveillance. By doing so, this paper contributes to MIS research on privacy, surveillance and digitally-enabled control, by relating the actual practices of individuals (which are often at odds with claims valuing privacy – Pavlou, 2011) to the normalization process of the control society conceived of as a *sociomaterial construction*.

We first present our Deleuzian conceptual framework, which revolves around control societies and how they tend to be normalized, thus making individuals accept this new system of domination. In line with Deleuzian studies that have explored modern society as a control society, we then analyse the crisis we are facing through the prism of "control societies". We further specify three mechanisms at the heart of the normalization of the current control society, highlighting the ways in which the current pandemic and its response (i.e. new forms of technological control) are "sociomaterially constructed" through a *historic, discursive and material process*. Finally, we discuss our contributions to MIS research on surveillance, control and privacy, and propose three main recommendations, derived from our Deleuzian framework, which echo wider calls and concerns in the MIS field to attend to these questions.

Deleuze's societies of control

From disciplinary to control societies

In his famous "Postscript on the societies of control", Gilles Deleuze (1992) explores how we moved from what Michel Foucault (1977, 1978) described as "disciplinary societies" towards "societies of control". In Deleuze's words, disciplinary societies relied on the organization of vast spaces of enclosure and confinement in dedicated environments, where "the individual passes from one closed environment to another" (1992, p. 3), with the primary objective of making bodies docile. Disciplinary societies proceeded with large groups made visible by architecture (in schools, hospitals, prisons, factories) and a grid pattern (inherited from the management of the great plague epidemics) that allowed these structures to monitor individuals. They relied on specific architectural forms, instrumental uses of space and planned configurations that aimed to concentrate in space and order in time, confining people while exposing them to view.

By contrast, control societies are no longer restrained by structures of enclosure and walls. Reflecting on the shift towards electronic forms of surveillance and the production of control societies, Deleuze identified new places of control and diffuse forms of power relations that play a central role in what he describes as a technologically-driven environment. In control societies, space is no longer intended to enclose or identify. Presenting themselves as a form of freedom, control societies proceed from a flow model enabling action at distance on individuals, who carry with themselves the data that identify and control them through the mediation of technology (Lazzaretto, 2006). The shift from disciplinary to control societies seems particularly at work in contemporary societies, marked by a quantitative increase in surveillance enabled by the proliferation of digital technologies of control (Haggerty & Ericson, 2000; Galic et al., 2016). The current pandemic context and the possible advent of a control society enjoin us to reread Deleuze's exploration of the operating methods of the control society and its normalization process, as a prerequisite for thinking about renewed forms of resistance. To that end, we first highlight the main characteristics of control societies, before specifying how control societies, as a new system of domination, gradually become the new normal.

Four characteristics of control societies

Continuous control and instant communication – Control societies no longer operate by physically confining people, but "through continuous control and instant communication, enabled by developments in material technologies" (Deleuze, 1995, p. 174). Reflecting on the transition from disciplinary to control societies, Deleuze (1992) highlights that each type of society is connected to a particular kind of machine, or technology. If disciplinary societies were characterised by "machines involving energy", societies of control rely on "machines of a third type, computers" (Deleuze, 1992, p. 6). The Internet (which was in its infancy when

Deleuze wrote those lines), smartphones as well as digital technologies are clearly at the core of control machines. In this context, as explained by Deleuze (1992, p. 7),

"The conception of a control mechanism, giving the position of any element within an open environment at any given instant (whether animal in a reserve or human in a corporation, as with an electronic collar), is not necessarily one of science fiction".

Thus, while a disciplinary society relied on a centralized focal point enabling surveillance of activities (the classic "Panopticon", Foucault, 1977), a control society is based on a diffuse matrix of technologies gathering, tracking and encoding information. Recent research has pointed to the emergence of more mobile, distant, and free-floating forms of control enabled by the use of new information technologies, characterized by their pervasiveness and ubiquity potential (De Saulles & Horner, 2011; Leclercq-Vandelannoitte et al., 2014; Martinez, 2011). These technologies enable subtle forms of distributed and indirect control, based on continuous interactions and communication flows with other connected people (Haggerty & Ericson, 2000; Martinez, 2010). In this context, the control enabled by technology has become short-term, but also continuous and without limit.

Modulation – Control societies are characterized by the principle of "modulation", which is enabled by technologies. Through the principle of "modulation", Deleuze (1992) explains that individuals in control societies have become fragmented, just like society itself. In this context, control constantly re-invents itself and assumes different forms, thus fragmenting individuals. As such, "one is never finished with anything" (Deleuze, 1992, p. 5) for that public institutions are part of the same modulation. Deleuze (1992, p. 5), for example, highlights the replacement of the school by perpetual training, and of the examination by continuous control. This Deleuzian notion marks a post-Foucauldian direction, as it directs the gaze of surveillance not towards individuals as complete beings, but rather towards

individuals as undulatory entities with many fragmented roles, represented in many different places and embedded in a continuous network (Galic et al., 2016).

Dividuals and data bodies – Deleuze (1992) further notes that control societies rely on and enact a numerical language, which can be understood as the "datafication" of individuals (Galic et al., 2016). In other words, control societies no longer revolve around the mass/individual pair but are concerned and regulated with codes. In Deleuze's (1992, p. 5) words, this means that "individuals have become 'dividuals', samples, data, markets, or 'banks'". In control societies, individuals no longer matter as objects of surveillance but rather what matters are the individuals' representations, such that the data created by individuals (data bodies) become more important than their real bodies. This evolution reveals a turn in the conceptualization of surveillance in modern society (Galic et al., 2016). Increasingly, the focus of visibility and watching is no longer on individuals (Deleuze, 1992) but on their data doubles (Haggerty & Ericson, 2000, p. 611), through the traces they leave behind, that are then reassembled to achieve specific purposes.

Internalization of social expectations and control of access – In this vein, control societies rely on the a priori internalization of social expectations and the a-posteriori control of certain borders, such that individuals can move freely within those limits, but not without (Bogard, 2006; Galic et al., 2016). In a context where walls are opened, it is no longer necessary to have individuals "on hand", but rather to control accesses (which is largely favoured by the numerical language of control, made of codes that enable or reject access). As Deleuze explains (1992, p. 7), "What counts is not the barrier but the computer that tracks each person's position", which can be licit or illicit. Control societies are thus characterized by a shift in terms of power towards controlling "access" (as shown in places such as airports and borders, conceived of by Deleuze as new "access points" or "checkpoints").

Normalization process of a new system of domination

Deleuze (1992, p. 3) highlights the risky implications of control societies, which he conceives of as "a new monster", epitomizing the progressive normalization and dispersed installation of a new system of domination. Rather than expressing a new freedom, the end of disciplinary societies and spaces of enclosures could "participate in mechanisms of control that are equal to the harshest of confinements" (Deleuze, 1992, p. 3). While in disciplinary societies, the goal was to create in people's minds the feeling that they might be under surveillance at any given moment, conveying a sentiment of invisible omniscience, such a feeling seems discouraged in control societies, leading to a progressive normalization of surveillance. Individuals are encouraged, and conditioned, not to worry or think about surveillance, but rather to accept it as the new normal (Crain, 2013). Deleuze (1990, 1992) invites us to consider three dimensions of this normalization process that makes individuals accept this new system of domination as an unconscious reality.

Embedding societies of control in a broader historic perspective – First, the emergence of control societies needs to be understood as a result of long-term, historic evolutions that have led to the gradual institution of new forces (Deleuze, 1992, p. 1). The large-scale shift from one type of society to the other (for example from sovereign, to disciplinary and then to control societies) is due to evolutions in the goals and functions of each society, translated in different socio-economic conditions of living and type of machines on which they rely. According to Deleuze (1992), the types of machines that are used in each type of society point to those specific social forms that are capable of generating and using them. Thus, it is important to take a step back and adopt a historical perspective on the development of societies of control, which are rooted in a deeper mutation of capitalism and

society. The evolution towards societies of control is coupled to the emergence of a technological revolution (with the advent of the computer), which has impacted, more profoundly, our way of living and relating with others (Deleuze, 1992, p. 5). This approach suggests that the understanding of the normalization process of societies of control implies considering the broader historic, socio-economic and technological context that conditions people's willingness to accept such a type of society and its (potential) associated system of domination.

Exploring the underlying logic of the emergence of control societies – Second, Deleuze (1992, p. 2) calls for a better understanding of the means of the progressive "normalization" of control societies and the natural inclination of the population to accept it as a normal reality. The objective of control societies is no longer to make bodies docile (as in disciplinary societies), but to condition and mould individuals' perceptions, by making them accept this society as normal. In particular, Deleuze (1990) explains that societies of control are characterized by a dominant discourse, which is both constituting and constituted by societies of control. In a society dominated by new technologies and instant communication, viewed as a "pure flow of communication", there is a significant risk, explains Deleuze (1990), in seeing the emergence and progressive normalization of a unique discourse, which could impose itself naturally and be recognized by all as truthful. It could therefore be extremely difficult to resist, respond or object to this discourse, because it would fall under the evidence (Deleuze, 1990). It is thus necessary to develop a critical, "socio-technological study of mechanism of control" (Deleuze, 1992, p. 7) to understand the normalization process of "control societies, often considered and presented as an almost "familiar mutation".

Considering the embeddedness of control societies in diffuse power relations – Third, we need to consider the reliance of control societies on specific, diffuse forms of power ramified throughout society. Control societies emerge as a kind of society brought forth by the

power of "deterritorialization" (see Deleuze & Guattari, 1987), where despite the appearance of an unparalleled freedom, the diffusion of power enables the constitution of a powerful "rhizomatic assemblage of surveillance" (Haggerty & Ericson, 2000). Rhizomatic assemblages of surveillance rely on the proliferation of digital control devices and networked surveillance practices at the level of society, often in conjunction with other institutions. They imply that individuals, groups, organisations and governments are continuously involved in the development of new forms of control (Brivot & Gendron, 2011). In this vein, literature in sociology, MIS and MOS on surveillance, control, and technology has pointed to a potential shift in the nature of the control in modern society, characterized by a more diffuse and "rhizomatic" model (Bogard, 2006; Brivot & Gendron, 2011; Haggerty & Ericson, 2000), involving multiple and networked relationships. Haggerty and Ericson (2000) for example develop the concept of "surveillant assemblage", based on specific sociomaterial combinations of humans and technology that exert novel forms of surveillance, which have become more malleable, through simultaneous and overlapping networks of digitalized information (Martinez, 2011).

Such evolutions mark the beginning of a new trend in surveillance theory towards the recognition of societies of control, which seems particularly at stake in the context of the ongoing COVID pandemic.

An analysis of current pandemic through Deleuze's concept of control societies

The Covid-19 crisis: The epitome of the control society

Deleuze's conceptualisation of "control societies" seems particularly resonant and relevant today, with the current state of health emergency and the technological responses adopted by many governments worldwide to fight against COVID-19, which seem to reinforce the advent of a control society (see French & Monahan, 2020). Deleuze's approach can provide useful

insights to reflect on the management of the ongoing crisis, which we analyse through the four main dimensions characterizing societies of control.

Continuous control and instant communication – The focus on continuous control and instant communication, emphasized by Deleuze (1992), is obvious in the present situation. To fight the COVID-19 pandemic, individuals and governments increasingly rely on the deployment of various IT-based systems (Calvo et al., 2020; Chamola et al., 2020; Oleinik, 2020; Pingeot, 2020; Ting et al., 2020) and their networked, connected methods of surveillance. Everywhere, technologies are used to fight coronavirus and its spread; smartphones equipped with applications coupled to geolocation have been developed worldwide, enabling to identify infected people, track contacts, movements and the spread of the virus. This includes, for instance, the Alipay Health Code App used in China, COVIDSafe in Australia, Smittestop in Denmark, TraceTogether in Singapore. While our lives depend on the digital, a fortiori in times of social distance, to communicate, get information, educate and work (Coeckelbergh, 2020), our technologies also appear as control machines that support instant communication and enable continuous forms of control. With these newly digital systems, enabling "instant communication" and "continuous control", we have never been so close to being watched into the privacy of our lives and homes.

Modulation – Similarly, the principle of modulation (Deleuze, 1992, p. 7) is particularly salient in the current context. For Deleuze (1992), control has become more insidious, as it radiates through the social body, and thus conjures up new forms of subjugation and monitoring. Here, miscellaneous technologies, developed during or repurposed for this crisis, materialize continuous (and remote) forms of control that assume different variations but are ultimately manifestations of the same modulation. The list of technologies (adapted to the situation of each country) is extensive, modulable and further develops and adjusts as the situation unfolds and depending on the context (Kitchin, 2020).

The type of tracking apps (and the process underlying their creation) varies significantly between countries (Parodi et al., 2020), with new partnerships formed, changes in the type of data collected as well as how they are processed and used. As a result, control constantly re-invents itself and assumes different forms, through technologies that effect a universal modulation.

Dividuals and data bodies – Importantly, the prevalence of information and communication technologies in the current context (for example through the use of applications and the intensification of Internet uses - messages, videos, images - enabling data collection) prompts the emergence of changing social relations and expectations, and ultimately new symmetries of power. Part of this process entails the datafication of individuals, where dividuals and data bodies become more important that individuals themselves (Deleuze, 1992; Galic et al., 1996). For example, newly deployed systems contribute to the constitution of dividuals-based data banks, where bodies are constituted as sources of data and information. Technology enable to measure, track, and regulate bodies (French & Monahan, 2020). As a result, data on bodies are constantly generated (e.g. number of infected cases, number of deaths are regularly listed) and seem to count more than individuals themselves – individuals are nothing more than numbers or dots on maps and graphs. Furthermore, this datafication plays a key role in shaping political answers and corporate agendas (e.g. a decrease in cases, or an increase in the number of tests conducted per day, being interpreted as an effective governmental response).

Internalization of social expectations and control of access – In this context, the current management of the pandemic crisis largely relies on the principles of internalization of social expectations and control of access. According to Deleuze (1992) the datafication of individuals enables a closer monitoring of their activities and a control of access, for instance determining what areas can, or cannot, be accessed. To fight the ongoing crisis, governments

have enforced new rules around social distance and interactions, with individuals having to self-discipline (i.e. individuals are responsibilised in behaving like good citizens). Technologies have been deployed worldwide to ensure the internalization of specific rules and control accesses (Leslie, 2020): for example, helmets equipped with dispositives are able to take temperature and to allow or reject accesses, while CCTV cameras detect the use of masks and the respect of norms of social distance (as social expectations). The public space worldwide has quickly become a warzone, with closed boundaries and accessible under strict conditions. In Europe, America and Asia, drones, helicopters and planes, equipped with loudspeakers or infra-red cameras, have been patrolling to locate transgressors, track movements and control accesses.

In the end, the current COVID-crisis epitomizes the advent of a control society (see Table 1), with a new form of control – based on *continuous control and instant communication*, *modulation*, the constitution of *dividuals and data bodies*, as well as the *internalization of social expectations and control of access* – emerging and imposing itself.

Principles of control societies	**Description**	**Applications to COVID crisis**	**References**
Continuous control & Instant communication	Control societies no longer operate by physically confining people, but rely on "continuous control and instant communication, enabled by developments in material technologies" (Deleuze, 1995, p. 174).	Development of networked, connected methods of surveillance to fight the COVID-19 crisis. Use of new types of technologies and of connectivity (from Apps tracking contacts, movements and the spread of the virus) exerting continuous control at a distance. Use of technologies as support of control and of instant communication (in times of social distance, connectivity and instant are also what enables to get information, continue to work, provide education to children and maintain our psychological and even physical stability).	Calvo et al., 2020; Chamola et al., 2020; Oleinik, 2020; Ting et al., 2020
Modulation	Control societies are characterized by the principle of "modulation", enabled by technologies (Deleuze, 1992, p. 5).	Exercise of control through various modular means, which take adjustable forms, and adapt to the situation, as the ultimate manifestations of the same modulation.	Kitchin, 2020; Parodi et al., 2020
Dividuals and data bodies	Control societies rely on a numerical language, enabled by the use of computing technology, which implies that "individuals have become 'dividuals', samples, data, markets, or 'banks'' (Deleuze, 1992, p. 5).	Datafication of individuals through technological uses and constitution of dividuals-based data banks. Constant generation of data on bodies (e.g. number of infected cases, number of deaths seem to count more than individuals themselves). Constitution of bodies as sources of data and information.	Calvo et al., 2020 ; Pingeot, 2020
Internalization of social expectations & Control of access	Control societies rely on the a priori internalization of social expectations and the a-posteriori control of access (Deleuze, 1992, p. 7).	Internalization of new social expectations (such as norms of social distance, self-discipline as an individual and collective responsibility, and IT-based control). Technology-enabled limitation and control of accesses (e.g. drone-based forms of control helping enforce lockdown measures to systems or used to report lockdown breaches). Restoration of boundaries between countries, limitations of moves within the scope of certain boundaries and constraints.	French & Monahan, 2020; Leslie, 2020

Table 1. Application of Deleuze (1992)'s control societies to current age of pandemics

A possible normalization of digitally-enabled control?

In line with past research on surveillance, control and technology relying on a Deleuzian approach (DeSaulles & Horner, 2011; Galic et al., 2016; Haggerty & Ericson, 2000), this analysis helps us identify some of the risks caused by the advent of a control society. The danger caused by these technologies, which enable the collection and analysis of massive amounts of data, are multifaceted through their effects on the core notions of freedom, privacy, and respect (Martin & Freeman, 2003). Existing research has noted risks of misuse, extension of access or extension of purposes of these systems, whether by public authorities or private actors (e.g. employers, insurers), or perverse effects leading to new forms of social discrimination, stigmatization and whistleblowing (Lyon, 2003b; Munro, 2018).

However, beyond the largely shared dystopian imaginary of a digital "control society" crystallizing anxieties and fears, we contend that the real concern is elsewhere. The rapid deployment of these digital systems raises the important question of a possible "normalization" of new forms of control driven by technologies, now and later, as envisioned by Deleuze (1992). On the grounds of health and safety, our society has become replete with newly developed or repurposed systems and technologies that aim to fight against the pandemic. In this regard, the COVID-19 crisis clearly fuels on-going techno-disciplinary dynamics that largely preceded it (see Best, 2010). With these changes, a new "normality" is slowly and somehow quietly built and settled. Yet, while these changes do not go unnoticed, they do not seem to be widely questioned. Who would/could have thought, a few months ago, that we would be witnessing the materialisation of scenes seemingly straight out of science-fiction films with, for instance, drones flying over cities to issue warnings to the population? Who is in charge of making sure that these systems do not collect and share more data than intended (as recently shown in France – see Delacroix, 2020) and that they never will? Can

we give up our freedoms (momentarily) and then expect to be able to get them back, as if this crisis was just a bad dream that would soon come to an end?

Despite the echo found by Deleuze's approach in MIS and MOS studies, few papers have explored the normalization process underlying the development of control societies as a "new system of domination" (Deleuze, 1992, p. 1). Some research has highlighted that this post-panopticon era (Boyne, 2000) signs a profound shift, arguing that surveillance is no longer a power technique, but rather a "cultural tool" internalized by individuals (Galic et al., 2016). Others note that the nature and scope of surveillance have changed and propose alternative theoretical frameworks for capturing surveillance, highlighting that surveillance has become a daily routine in the individuals' daily lives (Galic et al., 2016). But they have not investigated the underlying mechanisms and foundations of this normalization process as such. Thus, beyond existing studies that have investigated the advent of control societies, we intend to go further in the analysis of their potential normalization, through the analysis of the specific, unprecedented, case of COVID-crisis, which offer us a unique opportunity to explore the nature, underlying logic and implications of control societies (Deleuze, 1992).

An analysis of the normalization process of new forms of digitally-enabled control

Digitally-enabled control: analysis of a new "normal"

Embedding new forms of digitally-enabled control in a broader perspective – First, Deleuze invites us to consider the socio-technological study of mechanisms of control, grasped at their inception, and to embed societies of control in a broader historic perspective. From a historical perspective, it seems that we have been progressively "conditioned" to accept new forms of IT-based surveillance associated to the control society. Research on surveillance control and technology has highlighted that, historically, several striking events (such as the development of global risks, threats and terrorism since 9/11) have vastly

increased, in the recent years, IT-based control and surveillance industry both in form and content (Bigo, 2006; Galic et al., 2016; Lyon, 2003a; Packer, 2006; van der Ploeg, 2003). Such risks and the recent resurgence of terrorism in Europe and in the US have modified the landscape of information exchange (Smith et al., 2011) and led to the proliferation of digital control devices and surveillance practices at the level of society (de Vaujany et al., 2018), often in conjunction with other institutions (Deleuze & Guattari, 1987; Haggerty, 2006), such as commercial parties and service providers (Zuboff, 2019). The number and type of technologies of control have thus largely increased, as well as the variety and scope of individuals and spaces under surveillance (Galic et al., 2016). As a result, people have gradually been accustomed to the deployment of technologies of control that are characteristic of "societies of control", as a diffuse matrix of technologies gathering, tracking and encoding information. In this vein, safe cities, in which governors constitute new IT-based assemblages of surveillance (for example through omniscient systems of facial recognition, equipped with sensors and "smart" video surveillance" controlling citizens) appear as ultimate forms of this social control (see Wong & Dobson, 2019, on the social credit system in China).

In this way, the COVID-19 crisis tends to fuel a dynamic that was initiated some years ago, such that the deployment of these systems can be placed in a broader historic, socio-economic context that conditions people's willingness to accept this control society and explains a natural inclination to accept this reality as the new normal. In addition, this inclination appears as a new, modern form of voluntary servitude (La Boétie, 1997), as people directly contribute to the co-constitution of this new system of domination through their digital practices. As shown by the well-known "privacy paradox" in MIS research (where claims valuing privacy are often at odds with actual practices, Dinev, 2014; Pavlou, 2011), more and more individuals, in the current crisis, willingly sacrifice some of their freedoms in the name of the health imperative. For example, in the United Kingdom or in Australia,

millions have downloaded an application that provides health data to the public health system, thus accepting such an IT-based "continuous control" and "instant communication" as unconscious but normal conditions of their lives.

Exploring the underlying logic of emergence of control societies - Second, Deleuze invites us to explore the underlying logic of the emergence of control societies, in particular the ways in which individuals' perceptions are moulded, such that they implicitly adhere to *the* dominant discourse and accept a new system of domination as normal. The COVID-19 crisis epitomizes this logic by showing how IT-based control is rendered possible by the "emergency state" that has been adopted by many governments worldwide. In some countries (e.g. France, US, Italy, UK), a polemological discourse has been adopted by public authorities to fight the COVID-19 crisis, presented as a "war" against an invisible enemy. Discourses around the "emergency state" and "war" are likely to justify and facilitate the establishment, on the long term, of new forms of digital control, initially presented as a derogatory regime. For example, after the 2015 attacks in France (also presented at that time by the French Prime Minister as a "war"), the "state of emergency" was extended six times, before a number of its measures were overturned in ordinary law. The exception thus became the rule.

Likewise, the state of health emergency observed now in many countries (in Europe and in the US) could last longer than expected, implying that its main dispositive (e.g. IT-based control), which was initiated on an experimental or overriding basis, is likely, because of habituation and normalization effects, to become permanent. Such an extension of this state of urgency could ultimately threaten our freedoms in the long term. On the grounds of a supposed state of war, the use of "exceptional" means (e.g. IT-based control) could be justified without any justification (see Cooper, 2003) all the more that it is extremely difficult to resist such dominant discourses. Built around the notion of an "emergency state" and "war", these discourses not only legitimize the recourse to new forms of IT-based control, but

also sensitize and involve every citizen in this fight, by making them implicitly adhere to the merits of these newly developed systems. The risk is high then to observe a "normalization" of IT-based control, with the danger of transforming public policies into a security version of the "control society".

Consider the embeddedness of control societies in diffuse power relations – In the case of the COVID-19 crisis, new forms of surveillance and digitally-enabled control are increasingly embedded in networked forms of power, associating public institutions, companies and health authorities, that build its legitimation process. Newly developed systems are increasingly presented as the "right solutions" and increasingly legitimized as they are based on extensive alliances developed between corporations and states that are publicly justified on the grounds of health. Technology-enabled control is constituted by governments, in conjunction with companies, as relevant way of fighting the propagation of the virus. To fight against the sanitary crisis, the ecosystem at the heart of these systems now operates in a somewhat legitimized, visible, and almost natural manner, in contrast with past alliances which tended to be more opaque and concealed. Research has shown recently how states and corporations have increasingly used digital traces to conduct various monitoring of citizens (Flyverbom et al., 2019), as recently manifested in revelations of the US government's illegal global mass surveillance programs (Munro, 2018), provoking huge media storms and heightening the tone of political discourse (Dinev, 2014). Recent research has highlighted the hidden entanglement of companies in the governance of public and political processes – for example, Flyverbom et al. (2019) assert that the (invisible) collusion of corporations and governments has existed for a long time, especially in oppressive regimes (e.g. Google's experience in China), though also in liberal democracies (e.g. Snowden case).

However, in contrast with these observations where alliances between private and public actors was voluntarily hidden from public view, today's complicity between companies

(e.g. data brokers) and governments in the construction of new forms of digitally-enabled control, is increasingly made transparent, justified, and even encouraged. For instance, companies (such as Palantir Technologies, or NSO Group Technologies) have openly solicited governments, for the sake of safety, to respectively analyse their hospital data, or measure the contagiousness of their citizens. Similarly, the IT-based solutions deployed by most European countries rely on a contact tracing technology launched by Google and Apple, as claimed by big tech themselves, "through close cooperation and collaboration with developers, governments and public health providers"[1]. Similarly, data brokers, who, in the past, used to be hidden in the shadows, now largely influence public policies by graciously providing information that were usually sold "under the counter". In this way, at the end of March 2020, a data visualization company (Tectonix GEO) used anonymous location data from smartphones to develop a map showing how young "spring breakers" potentially spread the virus across the east coast of the US (See Appendix – Screenshots 1 & 2). Similar examples can be found in France (see next section).

These public-private alliances, which are normalized and made natural to everyone's eyes, not only legitimize this digitally-enabled control, but also tend to produce a conformist political discourse (as envisioned by Deleuze, 1990, who highlighted in this permanent communication flow the possible emergence of a unique discourse, self-imposing itself, which ends up making people accept these new forms of digitally-enabled control as an unconscious reality). The collusion between technological companies, health authorities and public institutions thus raises, in addition to concerns about complicity, a troubling question about the substitution of one by the other in the creation of a political discourse, enabling some corporations to attain some forms of public, or state power…which, in turn, reinforces the legitimation process of the recourse to these newly digital forms of control.

[1] https://www.apple.com/uk/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/

The sociomaterial construction of the crisis and of its solution: A historic, discursive and material process

Highlighting the mechanisms through which newly developed systems draw the contours of a "control society" (Deleuze, 1992), and analysing how the current pandemic and its solution (i.e. new forms of digitally-enabled control) are gradually made normal, this study highlights the *sociomaterial construction* of the crisis and of its response.

The analysis of the "normalization" process of these new forms of IT-based control first sheds lights on the ways in which this pandemic and digitally-enabled control sytems are embedded in a broader historical context that tends to condition and mould individuals' perceptions and receptions of these new technologies of control. Second, we highlight how the crisis is constructed socially though various discourses (Barnard-Wills, 2011; Webster et al., 2020) that aim to produce specific social effects and to justify some means (i.e. make people accept this control society as normal). Third, this analysis sheds light on the extensive alliances that materialize, make visible and reinforce the legitimation process of this digitally-enabled control, materially embedded in a specific network of power relations.

As such, the current pandemic and its technology-driven response can be conceived of as a *sociomaterial construction process*, as they are historically, discursively and materially constructed in ways that justify the advent of a society of control. Modern subjects are inclined to accept naturally IT-driven assemblages of surveillance (Haggerty & Ericson, 2000) that have long been used to regulate society, whose legitimacy is built through discourses that are organized in certain directions to directly form perceptions, shape realities and norms, and embedded in specific power relations (e.g. private-public alliances) that materialize and reinforce the legitimation process of renewed forms of control.

This "sociomaterial construction" process thus relies on underlying operating methods (Deleuze, 1992) that constitutes both the very problem (the fight against this invisible enemy) and its solutions (IT-based control), which are legitimized as appropriate forms of surveillance. Ultimately, we highlight that the sociomaterial construction (as an historic, discursive and material process) of the crisis and of digitally-enabled control system aims at normalizing a new regime of power. This new regime of power is enacted in new digital systems, i.e. the "control society" (Deleuze, 1992), which is constituted as a necessary, and maybe soon "ordinary", manner of living. We present hereafter an illustrative case to make sense of these arguments.

An illustrative case: The example of Covimoov in France

On March 16th 2020, French President Emmanuel Macron declared "We are at war with an invisible, elusive enemy"[2]. He ordered people to stay at home, closed the country's borders and highlighted that while these measures were unprecedented, they were nonetheless needed.

In this context, the company Geo4cast, specializing in modelling flows and behaviours, launched the application "Covimoov", which was presented to the French government as a tool to fight the COVID-19 crisis. Compiling data provided by public authorities, health institutions, partners and geolocation data automatically generated, or generated by different applications (downloaded by users), Covimoov produced three maps: one related to the

[2] https://www.bbc.com/news/av/51917380/coronavirus-we-are-at-war-macron

availability of intensive care beds (using data provided by public health authorities); a second related to the dissemination of respiratory syndromes (thanks to a partnership established with OpenHealth, a company that collected receipts from 12,000 French pharmacies to detect epidemic peaks based on the purchase of paracetamol or antitussive syrups); and a third focused on people's moves on the French territory. The former raised some controversial issues, as it enabled to highlight, in a very precise manner, a loosening of compliance with confinement from people in some departments, between March 26 and April 2, 2020 (Cherrier, 2020). Social media, TV and the press resumed it in one voice.

Following the results, some mayors in France took such information at face value: they demanded, from the French government, the support of the army to bring their supposedly recalcitrant citizens back into line, thus contributing to the creation of a political, dominant discourse (resulting from this private-public partnership) (See Appendix-Screenshot 3). The ultimate goal was to calculate a "risk score", by combining the three maps, leading to a possible responsibilization of each citizen at the local scale and internalization of social norms. Such an individual responsibilization raised some ethical issues and perverse effects (e.g. social discrimination and stigmatization). In the end, a simple application innocently downloaded by people imposed and turned itself into a privacy vacuum cleaner and control machine, without necessarily people noticing it.

This case illustrates the development of a digitally-enabled control system, enabling *instant communication and continuous control* (e.g. through the constant generation of data from mobile devices); enabling a form of *modulation* (e.g. control being exerted on varying aspects, from the spread of the virus to the respect of lockdown measures, as shown by the different maps); based on the *datafication of individuals* (e.g. data being constantly produced on people's bodies); coupled to the *internalization of norms* of behaviours (e.g. respect of

confinement and social distancing) and *control of accesses* (e.g. through curfews ordered on all the territory and closing of borders).

This case not only shows how this newly digitally-enabled system draws the contours of a control society, but also how a problem (i.e. the fight against the crisis) and its solutions (i.e. the new forms of IT-based control) are constructed as "the necessary tool" to strengthen the safety of the population and stop the spread of the virus. As the population was already largely equipped with, and used to, technological devices (94% of French population are considered as mobile users[3]), such digital systems emerged in quite a natural manner (from *an historic perspective* that considers France's historic industrial strategy that constituted IT as a central focus, Estabrooks, 1995); they were justified by an unprecedented context presented as a war (i.e. *underying logic and discursive construction of the problem*); and further materialized and legitimized by a so-called "vast ecosystem of innovation[4]" (e.g. *diffuse and networked power relations*), gathering corporate and business partners (companies specialized in dedicated technologies, such as geolocation, real-time, artificial intelligence and real-life programmatic), health institutions (hospitals and pharmacies), public authorities (regional council of Ile-de-France) as well as academic partners (universities and engineering schools)[5].

Discussion and concluding thoughts

We precise hereafter how this research contributes to MIS research on privacy and surveillance, in ways that advance our understanding of nature and implications of the current pandemic and of its solution (e.g. digitally-enabled control systems), and then propose three sorts of solutions derived from our Deleuzian framework.

[3] https://wearesocial.com/fr/blog/2020/01/digital-report-2020
4 https://www.geo4cast.ai/partners/
[5] https://www.geo4cast.ai/partners/

A critical exploration of the control society contributing to MIS research on privacy & surveillance

MIS scholars may contribute to the global effort to address current pandemic, not through direct solutions that would be immediately applicable, but by providing knowledge, conducting critical investigations and garnering insights that might be helpful in the fight against this (and future) pandemic(s). MIS researchers have recently been called to develop innovative and critical ways of thinking (see Myers & Klein, 2011; Rowe, 2010) and to explore alternative approaches to produce socially relevant knowledge. Philosophy offers some valuable insights towards this end (see Hassan et al., 2018; Leclercq-Vandelannoitte & Bertin, 2018; Markus & Saunders, 2006; Mingers & Willcocks, 2004; Rowe, 2012, 2018). In particular, the Deleuzian approach developed in this paper helps critically explore the current pandemic and its response by shedding light on issues of surveillance and privacy, which are key concerns in the MIS community (see Belanger & Crossler, 2011; Li, 2011; Pavlou, 2011; Smith et al., 2011 for comprehensive reviews). These concerns have recently become pervasive issues in MIS research (Dinev, 2014; Smith et al., 2011), with the explosion of data collection and analysis, especially in the context of "government surveillance" (Dinev et al., 2006; Lyon, 2001; Munro, 2018; Flyverbom et al., 2019), raising a dilemma between the search for security and risks for privacy, with some paradoxical consequences (e.g. "the privacy paradox", where privacy claims are at odds with actual practices, Pavlou, 2011).

In that regard, this paper contributes to MIS research on privacy and surveillance by critically exploring the development of a control society and the possible "normalization" of new forms of technological control in the age of pandemics. MIS research has explained the well-known "privacy paradox" by advancing various reasons, anchored either in interpretive or positivist views: some reasons are for instance related to human behaviours, psychology, and emerging individual interactions with technology (as the pure product of ongoing human

interpretations and preferences, such as convenience, or deliberate and more or less rational choice), while others are related to exogenous drivers (e.g. technological factors, economic or cross-cultural reasons), having more or less determinate effects on individual practices. In addition to these reasons, this paper embeds the privacy paradox in the normalization process of control society, conceived of as an inherent *sociomaterial construction*, where meanings and materialities are enacted together in practices (Introna, 2007; Suchman, 2007), constituting and legitimizing both the crisis and technologies of control (in line with the sociomaterial view in MIS research that considers the social and the material as inseparable; Introna, 2007; Orlikowski, 2010). Thus, we highlight indeed that the privacy paradox can be embedded in a finer-grained critical examination of the "control society" (Deleuze, 1992), in particular through an analysis of the progressive "normalization" of new forms of technological control, as a sociomaterial construction developed through an historic, discursive and material process, which sheds light on why more and more individuals, in the current crisis, may willingly sacrifice some of their freedoms in the name of the health imperative.

The current situation is too complex to fully understand its consequences; yet it calls for a response (French and Monahan, 2020, p. 7). In this regard, the Deleuzian approach adopted in this paper invites us to pay attention to the risks and long-term implications of such a possible "normalization" of the control society. While technologies, digital systems and infrastructures also have adverse effects on health-related matters (see Laato et al., 2020; Wang et al., 2019), they are obviously at the centre of the fight against global pandemics (see Galetsi et al., 2019) and can provide innovative opportunities to tackle the current crisis. But the crisis and the newly developed systems in response to this crisis can also be grasped as a sociomaterial construction, such that both the problem (i.e. the fight against the crisis) and its solutions (i.e. the new forms of IT-based control) are constructed as "the necessary tool" to

strengthen the safety of the population (Dinev, 2014), leading to a potential, self-imposing and natural acceptation of these new means (Deleuze, 1992), justified by the end.

It is thus pivotal to critical reflect over their conception and use, in particular in light of the emergence of control societies. Our analysis sheds some light on the pragmatic and ethical grounds that justify politically mobilizing opposition to surveillance (Lyon, 2003b), and calls for the development of some solutions and practical recommendations. One limitation to our argument though concerns the degree to which tracking devices have been used around the world. For instance, in many countries, individuals have actually not been using their tracing apps since their use has not been enforced. In Australia and New Zealand, less than 10% of the population has been using a tracking app. In Singapore, downloading the tracing app was voluntary. However, beyond this limitation, we hope to have provided some insights into the risks raised by a possible normalization of control societies in the age of pandemics. Deleuze indeed invites us to explore the operating methods of control societies, as a prerequisite for critically thinking about possible forms of resistance.

Three sorts of solutions derived from our Deleuzian framework

Questioning our sense of collective responsibility – First, since the emergence of the current control society needs to be placed in a broader, historic context, we call for a deep reflection on the locus of our "collective responsibility" in the broader development of our control society. This society is made of increasingly complex surveillant assemblages of control that have been fuelled by on-going techno-disciplinary dynamics that largely preceded it. The increasing reliance on digital technologies (in the past and in current context to tackle the crisis) seems to have blurred our understanding of the boundary between "good and bad" or "right and wrong". Therefore, while imputing responsibility is crucial, it has also become increasingly difficult in this digital context, as we rely on ever-expanding, disembodied

networks of human and technological agencies (in more than human assemblages), which extend but also somehow dissolve responsibility (Aroles et al., 2020). For example, behind each newly developed system or application, there is an algorithm created and patented by engineers, who may also need to be sensitized to the societal implications of their innovations. We thus call for a more comprehensive understanding of the scope of collective responsibility in the current context, and highlight that there is, maybe, a role for MIS research in that regard.

Raising people's awareness about digitally-enabled control systems – Second, since the normalization of control societies is also a social and discursive construction process, it seems vital, beyond discourses that attempt to shape individual's perceptions and receptions of the crisis and of its solutions, to raise potential users' awareness of the risks and implications of adopting the technologies of this control society. People often use digitally-enabled control systems without being aware of the implications of their practices (e.g. as in the case of Covimoov or Corona 100m in South Korea). As shown by MIS research, individuals are often concerned with their privacy, but are not always aware of the extent, mechanisms and implications of data collection (Dinev, 2014). It is crucial thus to investigate whether all implications of such systems been aptly considered before decisions were made, and whether individuals fully understand their ramifications. MIS research thus has a role to play in making things transparent and accessible, to help individuals fully understand the ramifications of the control systems they co-construct through their voluntary behaviours. This implies sensitizing and educating people to the consequences of their actions (Leclercq-Vandelannoitte & Bertin, 2018), whether to help them adopt stricter behaviors or to enable them to recognize their uses as "sociomaterial practices," enmeshed with technical features and individual practices.

Regulating partnerships between state authorities and companies – Third, since control societies rely on complex networked assemblages of surveillance, and in light of the complex networks of power that currently support the development and legitimation process of new digitally-enabled control systems, we suggest regulating partnerships between state and companies (e.g. data brokers), with the support of MIS scholars who can meaningfully help frame the political discourse and regulations across countries. Following Flyverbom et al. (2019) who problematized the roles and responsibilities of public and private actors, we call for more research on the interactions of businesses, states and other actors (e.g. universities) in shaping, developing, and governing digital information infrastructures, *a fortiori* in the age of pandemics. This is all the more important in that the complicity between governments and companies may lead to the production of a legitimized, political discourse, enabling some corporations to attain some forms of public power, thus requiring more regulation, for example by third (potentially supranational) parties involving MIS researchers. MIS research has shown that, despite recent revelations about breaches to data privacy, there has not been a "considerable bottom-up political and societal pressure to change the practices of government surveillance and data collection by the private businesses" (Dinev, 2014, p. 97). Following a rationale of surveilling those doing the surveillance (Marx, 2003), novel forms of regulation may also entail "countersurveillance" (Monahan, 2006, p.515), performed by individuals, investigative journalists, and social movements, in ways that foster accountability and render transparent potential abuses (in terms of privacy) by companies and authorities (Swed, 2020). In addition, more than ever, it seems vital that MIS researchers supervise the developments of digitally-enabled control systems to frame them with serious counter-powers, and not to abandon them to companies that could somewhat routinely violate the privacy of citizens, seeing in this tragic crisis a mere financial opportunity. As emphasized

by Deleuze (1992, p. 1), in light of the risks presented by the normalization of societies of control, “there is no need to fear or hope, but only to look for new weapons”.

References

Aroles, J., de Vaujany, F.X., Leclercq-Vandelannoitte, A. (2020). The Narrative of Responsibility: Imputability in the Digital Era. *OAP workshop*, UC Berkeley.

Barnard-Wills, D. (2011). UK news media discourses of surveillance. *The Sociological Quarterly*, *52*(4), 548-567.

Belanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS Quarterly*, *35*(4), 1017-1041.

Best, K. (2010). Living in the control society: Surveillance, users and digital screen technologies. *International Journal of Cultural Studies*, *13*(1), 5-24.

Bigo, D. (2006). Security, exception, ban and surveillance. In D. Lyon (Ed.), *Theorising surveillance: The panopticon and beyond* (pp. 46–68). Portland: Willan Publishing.

Bogard, W. (2006). Surveillance assemblages and lines of flight. In D. Lyon (Ed.), *Theorising surveillance: The panopticon and beyond* (pp. 97–122). Portland: Willan Publishing.

Boyne, R. (2000). Post-panopticism. *Economy and Society*, *29*(2), 285-307.

Brivot, M., & Gendron, Y. (2011). Beyond panopticism: on the ramifications of surveillance in a contemporary professional setting. *Accounting, Organizations and Society*, *36*(3), 135–155.

Calvo, R. A., Deterding, S., & Ryan, R. M. (2020). Health surveillance during covid-19 pandemic. *BMJ*, 369, m1373.

Chamola, V., Hassija, V., Gupta, V., & Guizani, M. (2020). A Comprehensive Review of the COVID-19 Pandemic and the Role of IoT, Drones, AI, Blockchain, and 5G in Managing its Impact. *IEEE Access*, *8*, 90225-90265.

Cherrier, S. (2020). Respect du confinement : les Français se relâchent. Le Journal du Dimanche. https://www.lejdd.fr/Societe/exclusif-respect-du-confinement-les-francais-se-relachent-3959914

Coeckelbergh, M. (2020). The postdigital in pandemic times: A comment on the Covid-19 crisis and its political epistemologies. *Postdigital Science and Education*, 1-4.

Cooper, S. (2003). Perpetual war within the state of exception. *Arena Journal*, *21*, 99-125.

Delacroix, G. (2020). StopCovid, l'appli qui en savait trop. Mediapart. https://www.mediapart.fr/journal/france/150620/stopcovid-l-appli-qui-en-savait-trop

Deleuze, G. (1990). Les conditions de la question : qu'est-ce que la philosophie ?. *Chimères. Revue des schizoanalyses*, *8*, 1-7.

Deleuze, G. (1992). *Postscript on the Societies of Control.* October, 59, 3-7.

Deleuze, G. (1995). *Negotiations: 1972-1990.* New York: Columbia University Press.

Deleuze, G., & Guattari, F. (1987). *A thousand plateaus: Capitalism and schizophrenia.* Minneapolis: University of Minnesota Press.

De Saulles, M., & Horner, D. S. (2011). The portable panopticon: morality and mobile technologies. *Journal of Information, Communication and Ethics in Society*, *9*(3), 206-216.

De Vaujany, F. X., Leclercq-Vandelannoitte, A., Munro, I., Nama, Y., Holt, R. (2018). Organizational Control and Surveillance of New Work practices. Call for papers, Special Issue, *Organization Studies*.

Dinev, T. (2014). Why would we care about privacy?. *European Journal of Information Systems*, *23*(2), 295-316.

Dinev, T., Belloito, M., Hart, P., Russo, V., Serra I., & Colauiti, C. (2006). Privacy calculus model in e-commerce- a study of Italy and the United States. *European journal of Information Systems*, *15*(4), 389-402.

Estabrooks, M. (1995). Electronic Technology, Corporate Strategy, and World Transformation. Westport, CT: Greenwood Publishing Group.

Flyverbom, M., Deibert, R., & Matten, D. (2019). The Governance of Digital Technology, Big Data, and the Internet: New Roles and Responsibilities for Business. *Business & Society*, 58(1), 3-19.

Foucault, M. (1977). *Discipline and Punish: The birth of the prison.* London: Allen & Lane. Foucault, M. (1978). La société disciplinaire en crise. In *Dits et écrits*, tome II, 1976-1988. Paris: Gallimard.

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

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

Galetsi, P., Katsaliaki, K., & Kumar, S. (2019). Values, challenges and future directions of big data analytics in healthcare: A systematic review. *Social Science & Medicine*, 112533.

Galic M., Timan T., & Koops B. J. (2016). Bentham, Deleuze and Beyond: an overview of surveillance theories from the panopticon of participation. *Philosophy & Technology*, *30*(1), 9-37.

Haggerty, K. (2006). Tear down the walls: on demolishing the panopticon. In Lyon, D. (Ed.), *Theorising surveillance: The panopticon and beyond* (pp. 23–45). Portland: Willan Publishing.

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

Hassan, N. R., Mingers, J., & Stahl, B. (2018). Philosophy and information systems: where are we and where should we go? *European Journal of Information Systems*, *27*(3), 263-277.

Introna, L.D. (2007). Towards a Post-human Intra-actional Account of Sociomaterial Agency (and Morality). Paper prepared for the Moral Agency and Technical Artefacts Workshop, The Hague: Netherlands Institute for Advanced Study.

Kitchin, R. (2020). Civil liberties or public health, or civil liberties and public health? Using surveillance technologies to tackle the spread of COVID-19. *Space and Polity*, 1-20.

La Boétie, E., (1997). *The Politics of Obedience: The Discourse of Voluntary Servitude.* Montréal/New York/London: Black Rose Books.

Laato, S., Islam, N., Islam, M.N., & Whelan, E. (2020). What drives unverified information sharing and cyberchondria during the COVID-19 pandemic?, *European Journal of Information Systems*, 29(3), 288-305.

Lazzarato, M. (2006). The Concepts of Life and the Living in the Societies of Control. In M. Fuglsand and B. M. Sørensen (Eds.), *Deleuze and the Social* (pp. 171-190). Edinburgh University Press.

Leclercq-Vandelannoitte, A., & Bertin, E. (2018). From sovereign IT governance to liberal IT governmentality? A Foucauldian analogy. *European Journal of Information Systems*, *27*(3), 326-346.

Leclercq-Vandelannoitte, A., Isaac, H., & Kalika, M. (2014). Mobile information systems and organisational control: beyond the panopticon metaphor?. *European Journal of Information Systems*, *23*(5), 543-557.

Leslie, D. (2020). Tackling COVID-19 through responsible AI innovation: Five steps in the right direction. *Harvard Data Science Review*.

Li, Y. (2011). Empirical studies on online information privacy concerns: literature review and an integrative framework. *Communications of the Association for Information Systems*, 28(1).

Lyon, D. (2001). *Surveillance Society: Monitoring Everyday Life.* Buckingham: Open University Press.

Lyon, D. (2003a). *Surveillance after September 11*. Malden, MA: Polity Press in association with Blackwell Publishing.

Lyon, D. (ed.) (2003b). *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*. London: Routledge.

Markus, M. L., & Saunders, C. (2006). Editor's comments, looking for a few good concepts and theories for the information systems field. *MIS Quarterly*, *31*(1), iii–vi.

Martin, K., & Freeman, R. E. (2003). Some problems with employee monitoring. *Journal of Business Ethics*, *43*(4), 353–361.

Martinez, D. E. (2010). Beyond disciplinary enclosures: management control in the society of control. *Critical Perspectives on Accounting*, *22*(2), 200–211.

Marx, G. T. (2003). A Tack in the Shoe: Neutralizing and Resisting the New Surveillance. *Journal of Social Issues*, 59 (2), 369–390.

Mingers, J., & Willcocks, L. (2004). *Social Theory and Philosophy for Information Systems*. Wiley.

Monahan, T. (2006). Counter-Surveillance as Political Intervention? *Social Semiotics*, 16 (4), 515–534.

Munro, I. (2018). An interview with Snowden's lawyer Robert Tibbo on whistleblowing, mass surveillance and human rights activism. *Organization*, *25*(1), 106-122.

Myers, M., & Klein, H. (2011). A set of principles for conducting critical research in information systems. *MIS Quarterly*, *35*(1), 17–36.

Oleinik, A. (2020). The politics behind how governments control coronavirus data. *The Conversation*, June 4th.

Orlikowski, W. J. (2010). The sociomateriality of organisational life: considering technology in management research. *Cambridge Journal of Economics* 34 (1), 125-141.

Packer, J. (2006). Becoming bombs: Mobilizing mobility in the war of terror. *Cultural studies*, *20*(4-5), 378-399.

Parodi, E., Jewkes, S., Cha, S., & Park, J. (2020). Special Report: Italy and South Korea Virus Outbreaks Reveal Disparity in Deaths and Tactics. Reuters, https://www.reuters.com/article/us-health-coronavirus-response-specialre/special-report-italy-and-south-korea-virus-outbreaks-reveal-disparity-in-deaths-and-tactics-idUSKBN20Z27P

Pavlou, P. A. (2011). State of the information privacy literature: where are we now and where should we go? *MIS Quarterly*, *35*(4), 977-988.

Pingeot, M. (2020). Débat: La société de contrôle et le Covid-19. *The Conversation*. https://theconversation.com/debat-la-societe-de-controle-et-le-covid-19-139076

Rowe, F. (2010). Valuing worldwide diversity in a European spirit: Being more critical and open. *European Journal of Information Systems*, *19*(5), 495–500.

Rowe, F. (2012). Toward a richer diversity of genres in information systems research: new categorization and guidelines. *European Journal of Information Systems*, *21*(5), 469-478.

Rowe, F. (2018). Being critical is good, but better with philosophy! From digital transformation and values to the future of MIS research. *European Journal of Information Systems*, *27*(3), 380-393.

Smith, H., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, *35*(4), 989-1015.

Suchman, L.A. (2007). *Human-Machine Reconfigurations: Plans and Situated Actions*. Cambridge, UK: Cambridge University Press.

Swed, O. (2020). Breaking the Order: The Intended and Unintended Consequences of Countersurveillance on the West Bank. *Surveillance & Society*, *18*(1), 48-60

Ting, D. S. W., Carin, L., Dzau, V., & Wong, T. Y. (2020). Digital technology and COVID-19. *Nature medicine*, *26*(4), 459-461.van der Ploeg, I. (2003). Biometrics and the body as information: normative issues of the socio-technical coding of the body. In D. Lyon (Ed.), *Surveillance as social sorting: Privacy, risk and digital discrimination* (pp. 57–73). London: Routledge.

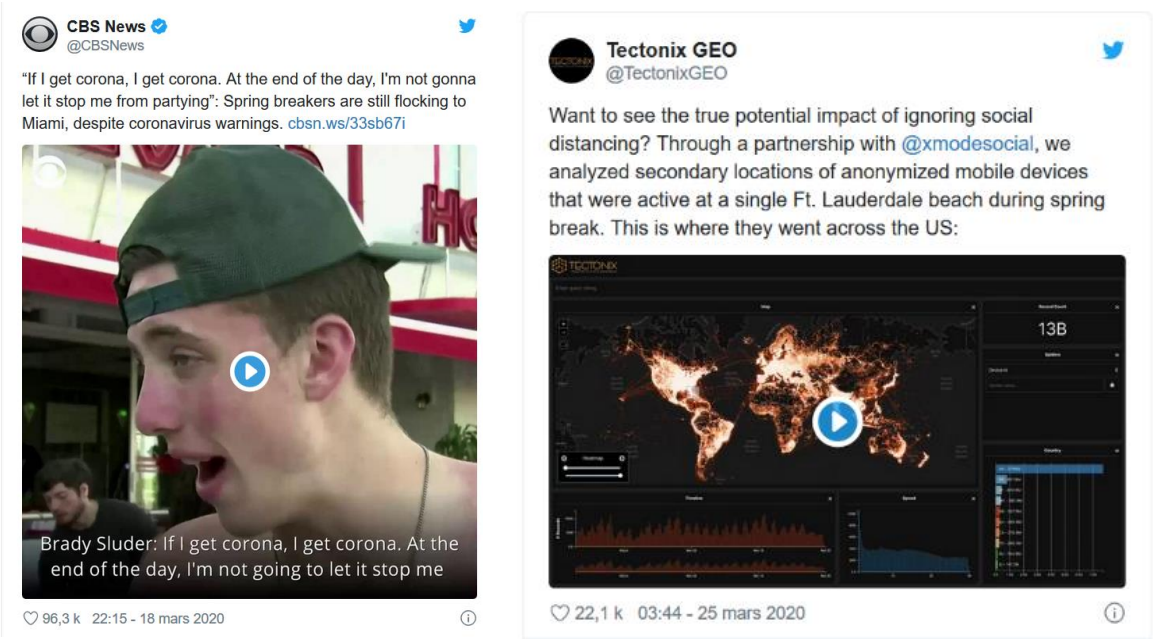
Wang, Y., McKee, M., Torbica, A., & Stuckler, D. (2019). Systematic literature review on the spread of health-related misinformation on social media. *Social Science & Medicine*, 112552.

Webster, F., Rice, K., & Sud, A. (2020). A critical content analysis of media reporting on opioids: The social construction of an epidemic. *Social Science & Medicine*, 244, 112642.

Wong, K. L. X., & Dobson, A. S. (2019). We're just data: Exploring China's social credit system in relation to digital platform ratings cultures in Westernised democracies. *Global Media and China*, *4*(2), 220-232.

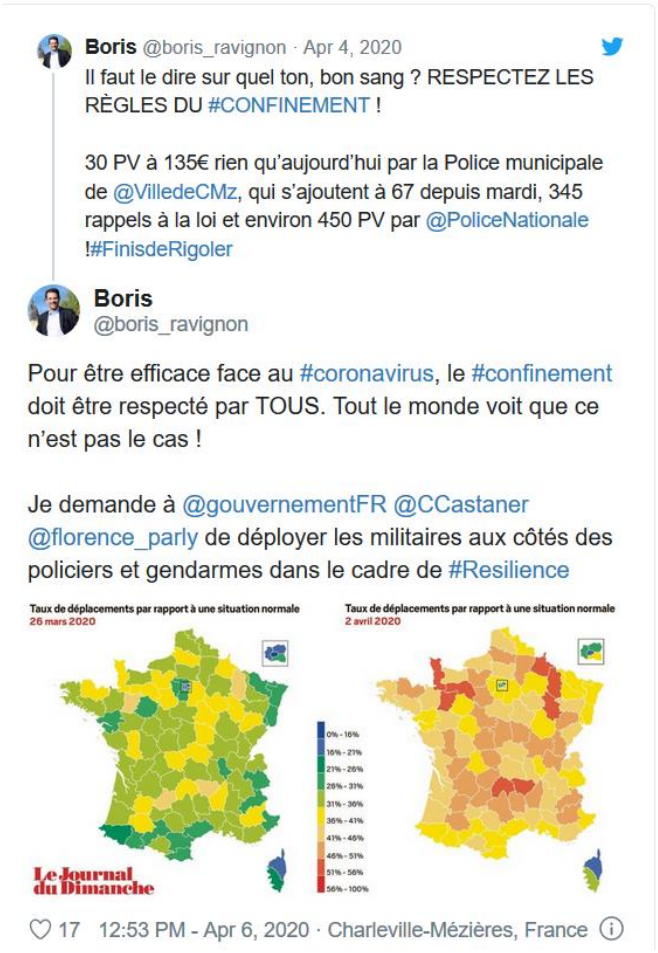
Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books.

Appendix



Screenshots 1 & 2. Use of geolocation data showing the spread of the virus

(Source: https://www.cbsnews.com/news/spring-break-party-coronavirus-pandemic-miami-beaches/)



Screenshot 3. Production of a political discourse based on the French Covimoov application (Source: https://www.lejdd.fr/Societe/exclusif-respect-du-confinement-les-francais-se-relachent-3959914)