University College Cork, Ireland
Coláiste na hOllscoile Corcaigh

SUSPICION, CONTROL AND DESIRE

A criminological analysis of secretive conduct and smart devices'

Thesis presented by

Janos Mark Szakolczai, MA

ORCID: 0000-0003-0535-4994

for the degree of

Doctor of Philosophy

University College Cork

Dept. of Sociology and Criminology

Head of School/Department: Prof. Maggie O' Neill

Supervisors: Dr. Tom Boland & Prof. Maggie O' Neill

External Examiner: Prof. Majid Yar

2022

Table of Contents

This is to certify that the work I am submitting is my own and has not been submitted for another degree, either at University College Cork or elsewhere. All external references and sources are clearly acknowledged and identified within the contents. I have read and understood the regulations of University College Cork concerning plagiarism and intellectual property.

Abstract: The topic of this thesis is the connection between secrecy and the onlife reality, a blurring line between being online and offline. Specifically, it offers a novel criminological perspective on how the smart technological devices integrated in the onlife ecology (with its technologies, features, design, instant online access, and messaging) aid specific instances of 'secretive conduct', involving regular and mundane episodes of suspicion, control and desire towards our kin, partners, co-worker, and perfect strangers.

While most studies on smart technology (phones, pc, homes, watches, cars) concern privacy and security, as well as the elements of isolation and social disintegration - this thesis offers an innovative contribution in the field of criminology. The elements which protect our devices, such as touch ID and face recognition have created an un-accessible wall against other users, both online and offline; the character of such elements and their effects is a central concern of this thesis, revolving around suspicion, control and desire such a condition induces.

Using a cultural criminology perspective, this work will theorize the ecology of onlife reality, the secretive conduct that characterises its environment; interpreting how tools of monitoring and control appear to have taken over any 'space' - from public to private. It

appears that not only is anything observable - but it is done in a covert and discreet manner - the Goffmanian front & back stage result constantly under scrutiny. In this context, the users become increasingly effected by this covert scrutiny. The smartphone functions as a quintessential tool that allows such a blur - leading into the onlife question of crime and cybercrime.

Advancing an experimental 'hybrid' methodology that attempts to unite both digital and 'in-person' ethnographic considerations, the research makes use of informal and incidental 'confessions' of smart technology users, such as their personal or witnessed secretive conducts. The analysis concentrates on specific abusive episodes in which the use of onlife devices allow all sorts of secretive conducts, with direct or indirect elements of harm: these are treated as social 'vignettes', and include parents secretly monitoring their children, partners making assumptions on the other's whereabouts, perpetuating elements of stalking, blackmailing, monitoring, all in a remote and apparently 'secured' environment.

This work contributes to cultural criminology with analysis of the blasé approach to such elements of secretive conduct becoming integral in the onlife habitus of smartphone users. Secrecy is becoming a central element of onlife ecology, taking place unwillingly, and mostly unknowingly. To act in secret, to monitor in secret - wanting to see, control, and observe all become central elements of the onlife.

To Clara and Silvia – and Federica, who stores the secret of life.

"The words are not good for the secret meaning,
everything becomes always a little different,
a little falsified, a little foolish"

'Siddhartha', in the words of H. Hesse, *Journey to the East* (1932)

I'll loosen the knots and slip my bonds. I'll bury *my past, lest it buries me.*
I banish memory.
E. Ionesco, *Hunger and Thirst (1964)*

Wo viel Licht ist, ist auch viel Schatten
'Where there's much light, there shadow's deep.'
J. W. Goethe, *Götz von Berlichingen, (Act I)*

INTRODUCTION

Secrecy has become a key dimension of modern life and an essential feature in our relationship with technology. We attempt to protect our devices, identity and data on a regular basis: while we navigate the net, we incessantly cross security gates with 'personal identification numbers', of greater and greater levels of protection and biometric elements. We consult devices accessible only through highly individualized features of protection, such as face recognition and fingerprints. We access online banking with OK keys, remotely generated pin-codes - double confirmation SMS, 3D Secure technology and app integrated QR codes. Our text messages and chats appear to be protected by cryptographic technologies.

However, these protective features and use of everyday devices affects the habitual interaction of users. They allow a secretive interaction among peers and fellow users. A user may practice sexting with his lover while having dinner with his/her life-long partner; may record a business meeting and sell it to competitors; may track, and observe others whereabouts with the use of a free app; may change, alter, transgress and deviate reality - all at the tip of a finger and behind a screen, in the most apparently "normative" onlife (online+life) existence (Floridi, 2015, Lyon, 2018) that is perpetually altered and deceiving. But this is only part of the culture of secrecy that surrounds us: the criminological aspect relates to the perception of control that permeates, the fear of having secrets discovered, revealed, stolen. One may protect screen usage with touch ID technology, or even encrypt all conversations: yet at the same time, this appears as nothing more than a Maginot line through which defences just as easily leak: one can trivially screenshot the very chats and share them with no alert – thus the breaching of trust and intimacy is perpetually at stake. These aspects appear to promote a specific apparatus of secretive conduct within the onlife ecology that I wish to introduce in the field of cultural criminology - a constant alteration of whom we want to appear to be, with ourselves and

others – and within this alteration the invasive yet easily available tool to enhance control, monitoring, observing, of others around us.

Research Aims

The aim of this study is to generate new insights on the ecology of the *onlife* reality and its correlation with the emergence of secretive conduct from a mainly cultural criminology perspective. We will provide an extensive examination of not only the ecological conditions of being 'seduced' into such conduct, but also the modes in which smart devices, especially smartphones, lead to harm towards subjects. This harm is induced by the features of secrecy; they induce us to 'exist', explore and examine (ourselves and others) in a covert condition, moving constantly between the blurring boundaries of the online-virtual reality and the everyday life experience. Seduction, induction and conduction are all central themes of this work. Specifically, as I will discuss, the very characteristic of such devices is to produce/induce secrets; generating aspects of suspicion, control and desire – a fundamentally intrinsic approach to the onlife ecology – the current and significant zemiology milieu.

The problem posed is pervasive, as the technological developments have spread through the global west unequivocally and at ever increasing rates – smartphone security breaches have skyrocketed even since the pandemic (O'Dea, 2021) –with different variations, but with similar features. This communality is due to the very design of these new technologies which are identical everywhere; they affect and seduce every user by new modes of securing our information and protecting our "privacy". We are increasingly securing ourselves inside a system that promotes abusive ways of living – a constant recurring of the condition of suspicion, control and desire, to which the result of social harm appears as invisible and detached as ever.

Novelty of work

Recent trends in technological developments have led to a proliferation of studies on the usage of smart devices and their social consequences, as they appear to affect most cultures across the globe, which engage increasingly with smart technologies, as well as the ever-growing internet experience. Such devices are becoming cheaper and evermore available to more cultures and younger users. However, while mainstream literature on smart-phone use focuses mainly on topics such as privacy (Zuboff, 2019), security (Solove, 2011), surveillance (Lyon, 2018), data collection (Christl & Spiekermann, 2016) or behavioural studies (Turkle, 2011); (Slepian, et al., 2017), the pivotal connection between secretive device use and users harm has not yet been closely investigated. Though many attempts have been previously introduced regarding intimate surveillance (Gregg, 2013) – or specifics of friendly surveillance (Horst, 2020) domestic alterations (Nelson & Garey, 2009) and digital self-tracking apps (Fors, et al., 2019) and the central analysis on non-intrusive or obvious smart phone uses (Vaidhyanathan, 2018); still a significant paucity of dealing specifically with the subject is palpable within the criminological field. Moreover, the entire culture of securing data from monitoring as

resistance, dealing with forms of cryptocurrency, obfuscation, and internet noise (Brunton & Nissenbaum, 2016), along with analyses on data-harm (Redden, et al., 2020) represents a central and inspiring field. However, this work wishes to approach a different perspective and open a debate over the criminogenic secretive uses of smart devices; – affecting and influencing the over-all dynamics of sociability and producing elusive and hidden aspects of deviance & social harm.

This is central, as any smart device presents itself as the quintessential tool/medium that allows an *onlife* blurring (Lyon, 2018). It acts as a physical antenna to our digital connection: a portal that at the same time guards and spies users and data. Not only the shady and invasive aspects of smart devices, but internet navigation in general must be understood, considering their 'opaque' and 'latent' characteristics: the specific influence of its use, its inclusive aspects of covering and yet producing secrets, that pile-up of data upon data.

Albeit the issue is pertinent across a global scale, in this study we will concentrate mainly on the aspect of smart devices within the global west, which allowed me to use a specific qualitative methodology – making use of in-person participant observation and a novel hybrid-ethnographical approach. Such tool of research, tries to 'catch' the spirit of secretive conduct on its occurrence and specific habitus (Lyon, 2018). Being a digital native, I have personally witnessed the integration and implementation of ever-growing systems of security and bio-credentials inside devices. If early gsm phones, digital cameras, first gen iPods could all be freely accessed, shared, peeked upon – today such a naive condition is no longer permissible. Not only locks and keys seal them – but their novel design hides their actions and functions. The latency – or inconspicuous functioning - of the very devices used becomes central: the modalities in which such devices monitor activities, gather data, are active yet without evidently signalling so, seems to induce a specific 'attitude' or conduct to which the contemporary individual appears seduced– offering a fundamentally dual use technology: both peaceful and predatory.

To this day, little attention has been paid for the actual effect of this environment of secrecy: In a matter of years, we've lost the habit of visible interest or concern for the individuals surrounding us. While on public transport, one could see what fellow passengers were observing, reading, or whoever he or she were talking to. Today, every passenger is instead typically focused on a powerful, multi-tasking tool capable of any search and allowing uncountable functions, at the tip of the finger, and protected by its inconspicuous design – nobody is allowed to see what goes on the screen. And more than that, this very tool can film us, monitor us, observe us – each other, anyone, anytime. The securing functioning again appears perfectly reasonable and necessary. Having become the smartphone so integral with our lives, and containing such an amount of data and indeed, secrets, nobody but us or with our consent should be allowed to access them physically.

In such an ecology, secrecy may no longer be defined as "something one can do alone in a room" (Lane & Wegner, 1995, p. 237), but rather something that may take place in any environment: a total fact that merges within the characteristics of a total institution (Goffman, 1961). Smart devices and the technology they allow are major inducers of this development. Secrecy is in fact no longer private. In the parable of Lyon & Bauman (2013), secrecy has rather become a 'liquid' condition, boundless and leaking uncontrollably in all fields of modernity. Betrayals, distractions, and satellite relationships have always existed, however, if on the one hand these have become much easier to manage, on the other they have become much more difficult to be kept hidden. This becomes ever more significant if we adopt Luciano Floridi's neologism of the *Onlife (2015),* a portmanteau between Online + Life – indicating that we can no longer differentiate our online existence from of 'Away from Keyboard'/Meatspace reality. The ecology of the Onlife, as this thesis wishes to integrate with Lyon's most recent work (2018), is strictly interrelated with this environment that represents the criminogenic elements of such effects, and abuses, of an all-persuasive secretive element of our everyday onlife that follow us *everywhere* and influence us *all the time*.

Smart technologies and secrecy

Locks and gates are a figurative image of the everyday internet user: one cannot navigate freely without being constantly induced to prove one's identity/credentials by opening locks upon locks of biometric data: from the computer to the Wi-Fi, to the email, to the smart-phone, smart-watch and tablets. And locks are the forms of engagement with any screened device: they lock the eyes of the viewer, the hands, the concentration. The same applies the forms of interaction, from a YouTube video through news articles to a chat on WhatsApp. Furthermore, in our everyday interaction, we are locked out from the content of any screen placed as an architectural barrier before us, from the cash counter of the clerk to the monitor of post office or bank managers. We are placed before the back of a screen, and have no sight of the content, even if the information regards 'us'. We, as users, are hardly face to face, and the COVID-19 pandemic has only intensified such conditions: we have curtains before curtains, locking the audience and users out of the 'outside' world. Rhetorically speaking, such a medium is no longer the object of connection, but rather enchainment/enchantment: the locks have thus become central and essential in the production and manifestation of secrets and of secrecy itself. What goes on behind the 'closed' space is protected by the lock; yet, in an ambiguous analogy, it is the very 'portal' for what it reveals: the lock itself is the inevitable peephole into a new reality.

Indeed, this thesis evidences how, in our contemporary society, surveillance and data control systems are not simply in the hands of the NSA or Police enforcement agencies, but invade the everyday life of all digitally, technologically, and socially connected individuals, in a domestic, work and leisure environment. We appear to have become producers and guardians of secrets, ones we are not even aware of, yet we insist on protecting them, and we appear disciplined in doing so.

Indeed, for authors such as Ziccardi, to 'keep' a secret "in a digital and informational world constituted by electronic networks, signals, sensors and impulses (and documents) has become extremely difficult" *(Ziccardi, 2015, p. 18)* The concept of secrecy in the (liquid) digital age has become somewhat genetically unattainable because of its particular development. This is quite evident in the case of the capillary distribution of memory and archives supports, capable of containing millions of different information in little space. They are global and cheap, physical but especially virtual, capable of instant transfer and potentially time-less storage. By this, the 'container of secrets' has become "practical, convenient and easy-to-use" *(Ziccardi, 2015, p. 18)*. Once these secrets exit the original 'container', they can be reached, accessed and shared in a matter of instants by anybody potentially 'connected'.

Within the realm of internet navigation, the individualization, monetization and monitoring of searches, clicks and view counts have become standard feature of the internet, ever since the device has become strictly personal – i.e. deviating from the common use of a single, family-shared computer (usually placed in the sitting room, close to if not substituting the television). The smartphone, specifically, with its capacious storage and its incredibly vast possibilities has since its invention been described as capable of carrying an entire office-worth of functions, from computer but also printers, cameras, cam-recorders, audio-visual processors, fax machines, photocopiers (Gates, 1995). This is headed towards an even greater 'invasion' of all spheres of the everyday with the introduction of 5G technology, that would allow an 'internet of everything' interface, where, with an increased capacity of bandwidth, activity and number of devices connected, anything is potentially linked to the internet and gathering data (Finley & Pearstein, 2020). The chronology of online activities becomes potentially Babel-esque, containing a single pattern of the single user's life in general, movements and interests, as well as one's phobias, paranoias, and various paraphilia. Its importance is twofold: as the use of the internet is so integral and englobing, the patterns of use become precisely targeted and individualized; on the other side, each user wishes to protect and maintain such 'data' from being disclosed or tampered with.

From the right of privacy to the desire of secrets

While Marc Bloch argued that the feudal Age was a truly transparent society (1939), and Sennett studied the shift from public to private life (1974), today we can easily sense the 'soft' enforcement of a secretive existence and our dependence to such. The protection of data contained in our devices, or the information exchanged, has become a standard condition that has entrapped our data 'by interface', and by thiswe ourselves are promoters of such traps. These secrets have apparently overtaken us, are hard to be kept as such. This is evident in how all commercial mobile devices, that we carry in our lives and in our pockets, are protected by cryptography as a standard
security measure. This a protective system that scrambles the data of a device to any other (potentially hazardous) user who do not own a 'decoding key'. Such technologies are

being recently introduced also in China (Lindsey, 2019) and being experimented by major OS tech companies as Apple and
Google with principles of quantum mechanics in order to allow a completely secure modality of information transmission. Such 'obfuscating' measures prove an evident contradiction in our relation between what is promoted as public, what is private and what is secret.

With an introductory analysis of their 'smart' function, I will prove that these have and are increasingly, by design, forcing us into a secretive behaviour, made of pins, passwords, codes and identification, that build walls upon walls in our everyday interactions: we are the only to access such
devices, and the only who are allowed to view and produce its content. Mentioning the work of Foucault, this would produce a particular 'Technology of Hiding the Self', thus the aim of 'taking care of hiding the self': a specific technique of production of content that constitutes a modification of the individual conduct, "not only skills but also attitudes" (Foucault, 1988, p. 18). This aspect becomes even more significant with the current pandemic crisis and the institution of new 'social distancing' measures and subsequent lockdown solutions, that increase the personal space and reduce
the physical environment where to exist within this space.

With technologies such as cameras, CCTV devices and social media monitoring becoming aspects of our everyday lives, the users are not simply victims of such 'data collection', but have become themselves active investigators of the lives of others, using for their very purposes the technologies that have until lately been interpreted as menacing of their private life. It is worth mentioning also that most of our secrets are contained in the very data tech companies store for us outside our reach.

Privacy and personal protection of data are today a mainstream issue to the point of forming a specific privacy-washing agenda of corporations and producers (Fowler, 2020). Nonetheless, this work wishes to tackle the issue from a different perspective. Rather than concentrating research on the topic of our privacy - or the lack of it - this research shifts the attention on the centrality of secrecy itself and how it affects us and our society, to understand the cultural transformation due to such phenomenon.

Such a topic, far from being limited just to ethical or juridical issues, needs to be addressed from a specific criminological outlook because of the development of subtle but ubiquitous deviant and harmful behaviours that we phrase as *secretive conduct*. Indeed, with the expression Suspicion-Control-Desire conduct, I refer to the study and theorizing of these ways of harmful behaviour which are the central key of understanding for my thesis. Thus, these are specific instances where the users take advantage of the secretive functions of their devices - the ways they may monitor each other, observe, search, control. Such conduct occurs within family circles, between partners, lovers, ex-lovers, colleagues, or just perfect strangers. Secretive conduct appears as a constant and somewhat socially accepted condition, or at least under-acknowledged -oftentimes underlying instances of deviance & harm that are not yet critiqued or addressed in the

mainstream academic discussion. The conduct, the way in which individuals 'lead' their impressions and focus their desires is a central Foucauldian perspective. The apparatus/device (Agamben, 2009) that they engage with becomes an integral medium of their ways of interacting (McLuhan, 1964). They induce and partly seduce the user, because of the very design of its features, to 'lead' a specific secretive life – and influence the surrounding environment.

Hence, *Onlife* Secretive conduct affects not only the individual but society itself. With such conditions, Suspicion-Control-Desire conduct is unprecedented and yet vaguely addressed and recognised. The major features that constitute 'social structure', solidarity, trust and integrity (in sociological terms) are being undermined. Especially with the contemporary need to become ever more isolated and detached, to the peak of the current social distancing requirements. We all are surrounded by secrets, seek others' secrets - and are always subject to them. Such condition has a considerable impact on the ability for communication and sense of community, the common ground.

Form data to capta: a methodological dilemma

Much thought has been given in the development of this work in trying to find the 'coherent' approach to analysing and criticising the dynamics of secrecy. Many of these reflections concern the idea of capturing/taking the dynamics of smart technologies and their designers/producers. In these terms, state agencies and corporations act as effective hunters of our information and data, while we users appear as a visible prey. Our data is their gain - turning effectively into *'capta'* something captured and lured. As we are claiming, *'capta'* is becoming a modus operandi of everyday onlife. The *'capta'* becomes the fundamental approach to data collection, monitoring, surveillance - creating dynamics of suspicion, control and desire.

Thus, the recollections of information necessary for this thesis faced, in such conditions, a serious moral dilemma. How to investigate the secretive lives, how to enter the intimate dynamics, especially considering oftentimes controversial, if not plainly deviant conduct? How to record, request, ask, fill consent forms, interview, question and monitor without falling into the trap of doing exactly what this thesis, at the extreme, tries to consider? Such a dilemma found its solutions in the most spontaneous manner, and indeed spontaneity becomes central in its resolutions. As data implies a form of gift-giving - thus a voluntary, un-profitable exchange - this work has found a truly valuable form of 'data' gathering in recollecting these very gifts happening on a daily occurrence. These gifts take place with the utmost triviality: in the everyday onlife. At the bus stop, at a friend's dinner, on Reddit chats, or e-commerce reviews. They are bits of information produced and shared openly - valueless and yet priceless - fundamental in answering the questions of this thesis, such as how do people observe, control, deceive, and monitor others within the onlife ecology?

Privacy, in such aspect, is rather an alienable right (Giglioli, 2019): what instead is addressed is the aspect of 'secrecy' – what goes on 'in the background'; 'quietly'; in our

backs. Through the realm of secrecy - and the concealing characteristic the smart devices offer; everyday users become they themselves promoters and consumers of remote monitoring, surveillance, analysing, observing. We become constantly engaged and induced into engaging in acts of suspicion, control and desire over our data and the data of others, our secrets and the secrets of others. It is exactly these aspects that will be analysed in the perspective of cultural criminology: how unwillingly, uncritically and thoughtlessly in our culture we can become spies and manipulators over the lives our friends, partners, co-worker and children: we may want to see more into their lives, and even, because of the design of such tools, become suspicious of them - desire to see even more - and control such information and the users producing them. Capta, not data, is the core of the smart device.

The secrets we keep thus become a basic form of vulnerability for every user, who nonetheless hardly can ever free him/herself from them. This analysis engages the harmful dichotomy of secrecy as tool to consolidate power: over oneself (as with privacy), over others (with its deceit, control, and desire abuse) and the modes in which we lose the power over both.

The secret stage: the onlife paradox of public and private space

The Suspicion-Control-Desire conduct affects the onlife user in its entirety. Implementing secrecy as a central aspect of daily routine, the result is fragmenting the social structure of the individual. With ever more enclosed personal bubbles of interaction, one-sided screen communication and incessant *capta* gathering, we witness on the one hand an ever-growing enclosure of the Goffmanian backstage – which becomes constantly carried with us in the form of the smart device; - on the other we notice a paradoxical Onlife wiping out that very space, surrounded as we are by tools of perpetual monitoring. In such a scenario, we are all affected. Even when we are fast asleep, or when we leave our smartphone at home while walking the dog, our *onlife* persona is constantly available, searchable on engines and social media - called upon, notified, and contacted any place and any time. Even if this takes place in the background of our lives, it becomes integral and ever exposed regarding our *onlife* within the ecology of recurring secrets.

Other than a smartphone, the milieu of secretive conduct the user must abide to is supported by elements of social pressure: in accordance with the considerations of Sennet (1974) and Yar (2004), we notice how the social and technological apparatuses (Agamben, 2009) are heading towards enclosing of personal boundaries, and individuals breaking down to smaller and smaller personal spaces - inflated only by virtual reality. In such a space - highly individual and single-minded - secretive conduct finds its fertile ground where it can grow and spread. The effect is one wherein there is an overabundance of back stages - opposed to front-stages. Both appear meticulously manipulated and programmed - there is no 'release of pressure' from the public eyes. Yet, this solution is not entirely true: front stages (now allegedly represented by social profiles) have always been meticulously manipulated and programmed, so as to offer a certain Goffmanian

impression (Goffman, 1956, p. 43). Nonetheless, while our lives are evermore isolated and single-minded, our onlife traffic is privatised into a single device: the chasing and monitoring of our existences is evermore targeted and precise. Thus, even the backstage is under scrutiny: no matter how vigilantly we develop our technology to protect the core of its information, something seems always to transpire. Within the domestic space, the distinctive feature of private realms becomes separated and yet perpetually controlled. We have locked up our phones but filled our sitting rooms with cameras (as we shall see in chapter 5/6). The secretive conduct in this prospect opens more and more doors while locking more and more locks behind it.

Such conditions show an evident contradiction in the relation between what is promoted as public, what is private, and what is secret. The protection of the data contained in our devices and the information exchanged, has become a standard condition that has entrapped our data 'by interface', and by this we ourselves are promoters of such trap. Indeed, these secrets have overtaken us, are hard to be kept secret, and are even harder to contain. In such ecology, the secretive conduct formed by elements of suspicion, control and desire appear ever present and indeed invasive. It is a recurring characteristic of the online/offline hybrid: it follows the user in any space and permits the constant conditions of Suspicion, Control and Desire among other users. If privacy has been promoted as a right to be safeguarded in order to protect us from theft and intrusion - regarding concrete components such as credit cards, business credentials and identity - secrecy involves much more intimate and just as delicate valuables. This creates a definite contradiction in the idea of transparency. Moreover, the secrets surrounding us are a cul-de-sac in our forms of communication: by not revealing their content, their protection must be kept at all costs. They cannot be forgotten, nor forgiven.

In accordance with the realm of secrets, which reveals itself as a border between public and private, one requires a technological keychain to be accessed, as an altogether new 'space' is formed: the secret place. Social media is central to this idea; its pretence as an agent of transparency is rather turned into a promoter of masked lives. The information flows among secret peers, controlled and analysed by secret algorithms, sold to unknown third parties, and thus further analysed and processed and then resold. What is public is a shade of reality; what goes on behind the curtain of our walls is secret and hidden - a point that is rendered even more clear with Dave Beer's consideration of algorithms forming a new social power that controls and monitors our web content (Beer, 2017).

Cultural Analysis and the problem *with secrecy*

Secrecy, in this context, has become extremely central and influential in our society: we want more and more of it, and cannot do without it. The cultural effect of such influence, in regard to hidden harms - and the proliferation of Suspicion, Control and Desire - is analysed through the culture of crime within the habitus in which the secretive elements take place and take over: the mundane and 'out-of-the-norm' conduct of online users who interact, engage, deceive and control others 'in secret'. Such a perspective is analysed

within the environmental fabric in which such instances take place. The Chicago School approach is central – just as it is for the Cultural criminologists (Ferrell, et al., 2008) – in trying to grasp "the environment of deviance and crime" (Melossi, 2008, p. 3). The cultural environment becomes even more central, one that "produces a given "knowledge" of the criminal that spans different discursive forms, from scientific tracts to newspapers to fictional accounts." (Ibid, p.10). The cultural context of the actors involved – and the *onlife* subjects engaged – becomes pivotal in defining this new habitus of suspicion, control and desire that becomes, according to this work, the very 'norm' (Lyon, 2018). We will attempt to make sense of the "cultural constructions of deviance, crime, and marginality" (Ferrell, 1999, p. 398).

This research, theoretically and methodologically, knits in the culture of crime perspective of Jeff Ferrell, Jock Young, Keith Hayward, and Majid Yar (2008), and thus tries to target and understand the "cultural meaning" (Ferrell, et al., 2008, p. 32) and the "cultural process" behind such elements of hidden, secret, unperceived forms of deviance and social harm. The internet perspective of this culture is central, as highlighted by Majid Yar (2017), for recognizing "cultural practices and the role in the production and reproduction of transgressive, subaltern or deviant subcultures" (Yar, 2017, p. 123). Fundamental aspect of deviance within secretive behaviour appears to take place online – or better, *onlife*. Yar proposed a fundamental move from an analysis of the 'urban' space towards a more contemporary 'virtual' space, and thus discovering and unveiling the elements of crime online, in forums, social networks, etc. My attempt is to combine cultural criminology – the effects, causes and elements – with a zemiological understanding of these dynamics; describing and theorizing on this novel and oftentimes ignored field of social harms and recurring acts of deviant.

Ultimately, my intention is to integrate a cultural criminological approach to a digital zemiology perspective. I focused on the Internet Crime and its Culture, and specifically the criminogenic harmful effect of the onlife ecology with its secretive conduct elements. Recurring elements represent internet navigation/smart device use, responsible for creating new and worrying grounds of secretive conduct and deviant behaviour in order to produce a cultural criminology of the onlife. This I argue is central to interpreting the background discrepancies and fractures in our societies – with all its aspects of power/knowledge introduced in the work of Foucault (1975) and now as blatant as ever; but also to understand the patterns of deviance and harm: the triviality with which users engage and justify the need to observe, monitor, control remotely their siblings, kin, employees, neighbours and even perfect strangers. This would offer a contribution to Criminology through the analysis and development for a "Cultural Criminology for the Zemiology the Onlife", not only concentrating on the online navigation and consultation but the actual effect of this navigation, the tools used and the people behind it, who have developed and profit from it. Hence the metaphor of an ecology of onlife is a useful framework for analysis.

Framing the issue

This work underlines the cautions given by McLuhan, who, among others, conceived how any use of the medium changes the subsequent society involved (1964). The smartphone in this perspective is more than an idle tool but has a specific effect on the lives of people, and as I will discuss in the case studies, it can be used in a targeted, harmful and deviant manner. Furthermore, my thesis wishes to integrate and contextualize the procedures discussed by Foucault on how our society has embedded into elements of constant control, observation, and identification taking place around us – not simply within the institution's walls – but in all environments (1975). Such perspective not only has been taken up by Deleuze (1992) representing the influence of actual societies of control (1992). And more than that, we now witness how this is apparently happening unknowingly: in the background, endless and integral within our (on)lives. In this perspective, the secretive conduct that is aroused by the uses of these smart devices and their engagement in the onlife need an in-depth analysis, that perhaps may continue beyond this work and most definitely towards a multidisciplinary understanding.

The research questions in this study focus on deviant conduct to lead to harm, specifically aided by smart devices within the onlife ecology. Specifically, the following issues will be addressed:

1. What are the aspects of secretive conduct created by the onlife ecologies?
2. How do smart devices and other technologies generate these forms of secretive conduct?
3. What are the deviant aspects of secretive conduct used to monitor, observe and control others and what is the harm involved?
4. Finally, is the onlife turning into a total institution? And if so, what tools and means do we have to resist?

To engage in a fulfilling manner with these questions, I have proposed a somewhat experimental methodology that will be described in detail in the methodology chapter. Its elements represent an ethnography-based form of qualitative research, essentially by producing true involvement and comprehension of the secretive conduct taking place in the background of our everyday *onlife* experience. Although this work occupies specifically the western, so-called global north perspective and influence of contemporary everyday secrecy, it lacks an in-depth Asian perspective, particularly the Chinese government surveillance-control system which, with its recent technological advances (especially in the pandemic regulation) raises questions enough to require a whole Ph.D. alone.

Through the offlife looking-glass

For this work, I positioned myself as an auto-ethnographer of the onlife - listening and observing its occurrences armed only with my sociological background and interest in cultural criminology & zemiology. I felt the need to distance myself from being a 'hunter

of the 'onlife wildlife', nor even strictly speaking a 'bird watcher' of its 'fauna'- i.e. camouflaging myself and taking notes as expected. Rather, I opted to act in conformance with character of the flâneur, a made famous by Baudelaire (1863) and reanalysed by Walter Benjamin (2002). Such approach is central also to the Chicago School ethnographic analysis of the criminogenic environment, whereas Robert E. Park and Ernest W. Burgess observed and theorised how "socio-cultural environment within which a group finds itself largely determines the type of behavior prevailing within it." (Melossi, 2008. P. 110). Indeed the perfect flâneur, the passionate spectator, is incidentally central in representing the 'spirit' of this doctorate, underling an ambiguous condition of being partly an idle stroller, and partly a curious, non-involved yet shrewd observer who may understand while remaining detached. Such an approach became significant because of my partial disengagement with all social media and smart devices since the end of 2018 - this involved not having a smartphone, but also disconnecting and not engaging on Facebook/Meta or Twitter; nor WhatsApp; avoiding the GPS function; reducing to minimal App usage; - trying, so to speak, to engage in an *offlife* counter-conduct activity within the onlife environment. This perspective places itself not as a luddite or *passéiste* take – but rather a self-limiting and more 'in control' approach to the surrounding environment without requiring becoming strictly 'off-the-grid' (Angwin, 2015) .

Moreover, this approach appeared successful in immediately provoking questions and interest among the 'fully-engaged' users of the onlife reality. For example, using only a mobile GSM device - capable strictly speaking only of SMS, calls and minimal browser consultation - would appear as almost a direct statement of something peculiar, upon which people regularly - from friends to random strangers- would comment on or criticize: This allowed constant and regular opening conversations and debates, to which I participated as an external observant. I would strictly avoid directing any conversations, nor recording any material or data, but instead enjoying and integrating anonymous and 'passing-by' elements of the everyday in my research. An incidental sets of episodes and recollections of Suspicion, Control and Desire began to build up, becoming the core of my research analysis. As the narrative involved was so central, this too has become a major field of my work. Narrative criminology as discussed in the recent conference (Genova, 2022), show how for criminology it is central to engage with the dynamics of what is told what is untold. The interpretation is aways complex, requiring at times elliptical, concise, short considerations and dynamics, referring to what everyone knows and must be simply hinted. This approach is in many ways central in comprehending and discussing the secretive dynamics of crime. It is the concern with the emergence from the "not-said, the not-knowable, anticipating an act which doesn't frequently find words, or taking its place. It follows that, since its inception, narrative criminology has revealed itself to be very interested in the analysis of singular cases ("one is enough")." (Verde, et al., 2022)

The conduct that I perceived appeared in this light surrounding the onlife everywhere, 'spilling out' in countless dynamics. I have theorized upon these, understanding them as socio-cultural criminological vignettes: ones that occur with the utmost triviality, and any reader may relate to them as they appear to take place in any home, any family, any relations - conscious or not. On many occasions, the re-narration of events, witnessed by

me or others offered an effective 'outlining' of the unreflective deviant Secretive conduct taking place in our lives - the modes and modalities through which these take place - the tools used and the harms involved. These vignettes reveal new, unprecedented dynamics that only through indirect involvement the onlife users appear to wish to share, or come to consider as significant, or controversial. They are glimpses of our newly perceived *onlife:* to which our secrets are more than ever valued, and never as today placed under the lens.

Outline of the thesis in three parts

The first part or section offers a canonical commitment to the various directions of the thesis. We will begin by setting down the mythical and anthropological background and discussing the literature that has influenced the development of the thesis. The first part is central in defining the cultural criminology elements this work engages with - and how that approach is central in defining the ground-breaking reality of the onlife realm. The first part includes: analyses of the Roles and Rituals of secrecy from an anthropological and philosophical perspective, defining what were the modes and ways secrecy had been used and interpreted, especially concerning its power structure; the influence it raised, and the system of control and docility – central in the work of Foucault (1974). This excursus appears essential as an opening before finally addressing today's specific dynamics: Its influences, the theoretical framework, and the methodologies that have been chosen and engaged with: from publicness to privacy. From privacy to secrecy, and the modalities through which these changes have occurred. Such aspects will be delineated in the literature review, which will describe and comment on fundamental works of this thesis such as David Lyon, R. Sennett and Z. Bauman, but also Vaidhyanathan, Byoung Chul-Hal, and the work of Frank Pasquale and Geert Lovink, and many others. These authors are included in the literature reviewed because they either specifically address the paradoxical visibility/secrecy and its counter aspects in the online/onlife realm - but they also describe the discrepancies of the social world into a single-lensed, privatised environment, where individualisation and secrets are bound to proliferate. These aspects will be analysed further using the theories of Michel Foucault, Erving Goffman, and Georg Simmel – who are fundamental to the theoretical, conceptual framing of the thesis and who offer, long before the internet and the conceptualisation of an online reality, keys to reinterpret and understand the present. With his work concentrating on the nature of secrets, Simmel offers a still relevant perspective on the dynamics of hiding and exchanging, delivering and capturing. With the interpretation of Foucault, we may understand the modes in which this very secretive conduct may shape the onlife ecology. Goffman offers precise considerations on the everyday practices that define the various instances of publicness, privacy, and secrecy. Within the contemporary scope, such characteristics appear integrated into our social interaction and our technological mediums, forming an even more integrated aspect within everyday life: a collective ecology of secrecy, that appears a fundamental phenomenon that needs study.

Such conditions will be examined through the lenses of cultural criminology to clarify the dynamics of harm with the use of these tools. Also, this work indeed wishes to pick up elements of the 'Art of Listening' to offer a non-invasive method for gathering data about

the nature and use of secrets in everyday onlife. This work, as it will be discussed, insists in the importance of collecting information through the sensibility of a data as given, rather than recurring to what is intended as a *'capta'* - a capture of information; - which is rather the mode of doing 'monitoring' and collecting 'information' by private and state agencies.

In the second part, we engage in documenting and analysing the specifics of secretive conduct relevant to shaping the onlife ecology, involving and recreating conditions of secrecy and secretive conduct. In this study, the essence of the smartphone will become central, as its features appear, controversially, as inducers and promoters of secretive conduct. In such conditions, secrecy becomes not simply a natural element of society, but a specifically induced aspect, ever-recurring and binding of everyday interactions. Such tools (or mediums) become promoters of conditions of permanent exposure and covert concealment of our features, whereabouts and interests. But, as we will discuss in section 2.2, managing our onlife existence such elements of monitoring and exposition are recurring in both our online navigation and city roaming. We try to isolate and yet feel the need to record anything at any given time. Any action nonetheless becomes part of a game of observing and recollecting - fed to the data-hungry grinding machine. We may attempt to hide, as discussed in the section 'What we do in the shadows'; while nonetheless, we find ourselves evermore involved in the Onlife Engagement, where the actual control we still possess over such means, and the ways we use them, is put in question.

In the third and final part, I will use a series of vignettes drawn from the auto ethnographic research to create more concrete examples through which to theorise and further develop analysis. Such vignettes appear interesting as they are glimpses of the everyday onlife witnessed personally or shared in a non-invasive fashion. They are vignettes as they offer caricatures of something any onlife user may witness or relate to. While they risk appearing trivial while out of the context they may (still) raise alarm (to some). These involve, for instance, friends monitoring each other on social media while sharing content on selected instant messaging groups; fathers monitoring daughters through surveillance cameras installed in the sitting room; partners assuming each other's whereabouts and conjecturing on their chatting habits. All these glimpses recollect an everyday onlife engagement with secrets and the conditions they cause, repeated and recurring in a constant spiralling of events. The conclusion does not lead to a technophobic catastrophism of perpetual and entrapping control, suspicion and desire, rather a reconsideration of the directions our technologies have taken in the fog of constant development – and endless gain: a rapid shift we as users may still make of – and perhaps re-think of - differently.

.

Part I: Secrecy and Harm

1.1. Roles and Ritual of Secrecy

In the mythology of ancient Greece, the concept of secrecy and its societal role combined the sacred and the profane (Calasso, 2019). A fitting example is represented in the sacred ceremonies of Athens dedicated to their patron divinity, celebrated during the month of Σκιροφοριών *(June-July)* (Sticotti, 1931). The ceremony, according to Pausanias, consisted in transporting nightly, on the head of two virgins known as arrephorae (ἀρρηφόροι), certain 'sacred' and at the same time 'secret' objects that had been previously delivered by Athena's priestess. These mysterious objects would be placed inside a canister and led through an underground passage to the Acropolis. Some scenes of this sacred procession are apparently observable in the eastern frieze of the Parthenon (Sticotti, 1931). Though never proven, some commentators believe the sacred chest contained cereal paste, representing snakes, phalli, and shapes of men, as to comply with some 'fertility' rite. Yet, the point remains: it was not these chests or canisters that mattered – nor their content; but the mystery of their influence. Probably, they contained nothing: the chests were empty, and the two girls had nothing to hide but the secret itself (Mordini, 2011).

The secrecy thus presents itself with a first and basic connotation: it is what possesses power by the very fact that is not known, but it is nonetheless exposed, in order to maintain its power. It is truly unknown and unspoken, but at the same time much discussed and incited. Here we encounter the evident paradox of its existence: by setting apart something, by secluding it, you inevitably let it stand out. Notorious is the tale of Bluebeard, who would allow his wife to visit any part of his castle, except one anonymous door, becoming an obsession.

This fable recalls *the tale-within-tale* motive of Eros and Psyche, narrated in Apuleius' 'Golden Ass'. Curiosity being necessarily aroused by what one cannot 'see' is a recurrent theme, underlying the powerful influence of desire, suspicion, and indeed the idea of control. In Apuleius, Psyche is married to an invisible figure that offers her comfort and love, in exchange of never having to reveal his own identity: she would nonetheless, tempted by her jealous sisters, try to find out the true identity of her husband at any cost, with quite tragic consequences.

The underlining message of the fable, interpreted in many different ways, is the power of the secret because of it being in itself – in its essence – something secret: by protecting it, it allows an immediate effect of curiosity, and more than that, suspicion. Indeed, the envious sisters tempt so successfully Psyche exactly due to the intrinsic 'fear' that the secret causes. Here we see the basis of transparency: if there is nothing to hide, then there is (apparently) nothing wrong. Conversely, if something is hidden, it must be inevitably 'bad'.

Other than fable, we may find the effects and ambiguous role of secrecy in a Socratic myth, specifically in what is known as the myth of Ring of Gyges: in the 2nd book of The Republic, Plato has Glaucon narrate the rise to power of a shepherd known Gyges, who, after a "thunderstorm and an earthquake" (Plato & Bloom, 1991, p. 359d), saw near his cattle the opening of a crack and chasm in the earth. He decided to wander in, finding

inside a giant bronze horse, and within it a larger-than-human corpse. The skeleton wore a golden ring, which Gyges removed and discovered later it had magical features: when worn, and twisting the collet, he would turn invisible. Here the myth becomes a moral allegory: gained such power, Gyges decides to force his own benefit (fate): he "committed adultery with the king's wife and, along with her, set upon the king and killed him. And so he took over the rule." (ibid, p.360a-b). Glacon thus poses the question: would such ring be given to a just and an unjust man, the effect would be same: secrecy corrupts, as no-none is "so adamant as to stick by justice and bring him/herself to keep away from what belongs to others and not lay hold of it, although he had license to take what he wanted from the market without fear, and to go into houses and have intercourse with whomever he wanted, and to slay or release from bonds whomever he wanted, and to do other things as an equal to a god among humans." (360b-c).
Such argument is strictly connected to the later discussion on smart technology and surveillance: has the all-watchful eye become plainly substituted by sophisticated panoptic control (Strassberg, 2003)? For sure, the myth of divine powers is connected with the one of mortal powers enhanced by divine features, as the means of secrecy and secretive conduct itself.

We may add to the Gyges ring, the device that makes ones invisible, that indeed I have suggested in many ways that can be related to contemporary smart technology. As in the already mentioned Plato's Republic's quote, such tools offers a "license to take what he wanted from the market without fear"- through data mining, cookies and algorithms; and to go into houses - as with Google Home and Alexa, along with smart surveillance technology in general; and have intercourse with whomever he wanted (with the use of Social Media and dating apps), "…and to slayer release from bonds whomever he wanted" - with trolling, as well as hacking, remotely and anonymously; "and to do other things as an equal to a god among humans." - which is, per se, the apparent ambition of GAFA (Google, Apple, Facebook, Amazon) and other corporations. In Platonic philosophy, it is the very omnipresence of god's power that indeed puts a balance to the vice of private man: his all-knowledge that is the definition of divinity itself. As such, mortal hiding is practically useless, the gods are always watching. Such ever watchful theme is recurring in theology, but according to (Mordini, 2008) was first put in practice in the overt totalitarian Calvinist Regime in Reformation Geneva. While this is no place to investigate further this extremely fascinating event, it is worth mentioning how the Calvinist 'residence' in Geneva required all (intrinsically sinful) citizens to check on each other and remove, during daily life, all curtains – physically and metaphorically (Wallace, 1998); (Mordini, 2008). In many ways, this is the beginning of what appears as the birth of technical, active surveillance: not simply implied and 'suggested', or even worse, menaced by divine intervention,

Yet, as we shall see, the secret has quite different connotations, especially concerning the 'nature' of its being 'hidden', as opposed to its need of being 'stored' or even 'guarded'. Also, the connection between secrecy and the sacred is quite evident, sharing both the same roots and somewhat of a common purpose. The connection between the divine and 'holy' figures is secret as long as it requires a certain filter of interpretation: as with the Athenian priestess, the power of the divine only works by not

knowing what is hidden and what is revealed: there stands the mystery, the awe, and the hope of revelation.

Such brief, albeit necessary, excursus on the anthropological and philosophical dynamics of secrecy, will be now followed by a contemporary take on what are the modalities of secrecy in today's everyday onlife: a specific ecology where online and the offline are strictly interrelated, just as secrets and smart devices are.

1.2. Literature Review

In this chapter, I'll attempt to engage clearly in the correlation between 'secrecy' and the cyber 'modernity' of our current times – in a technologically mediated society. In such an approach, it appears essential to make distinctions, first concerning what is the conceived difference between privacy and secrecy – terms that are similar, yet fundamentally different. Such distinction will come hand in hand with the argumentation over online publicness and its counterpart – conceit information. Such concepts nonetheless, as we will see, are closely related. For publicness and secrecy appear the essence of internet use, connected the means of control and surveillance. Such parallel (and paradox), which appears opposite to its ideal of openness and freedom - will be analysed in light to previous studies - as to underline the paradoxical and essentially complex alternation of exposure and control: the fascination and tendency towards it.

The idea of a public entity, as opposed to a private individual, becomes even more 'isolated' with the evident emergence of 'someone acting in secret' – the rise indeed, playing with Sennett's work (1974), implying the rise of a Secret Man: who acts, lives, and conducts a secretive life - though apparently in public. Historically, the political power of the 'secret man' and his influence in society becomes central in the work of Koselleck (1988), with aid of secret societies and states-within-the-state systems of power (that may be paralleled with today's power and influence of Big Tech corporations[1]). Indeed, the life lived by the 'common' private individuals appears today inseparable from its virtual equivalent, as 'real-life'/meat-space and online interaction, but also control and monitoring, appear fundamentally 'merged', as we will see in the discussions of Lyon & Bauman (2013) and Floridi (2015). David Lyon, in particular, is a fundamental recurring figure in this work, having anticipated by almost three decades the current practices of surveillance and monitoring, outlining a condition of 'social sorting' and alimenting the 'ratio of secrecy' among users. The modes and systems, especially connected to algorithms, of control and analysis, is well described in the works of Frank Pasquale (2015) and S. Vaidhyanathan (2018), along with the considerations of Byung-Chul Han (2012) and Geer Lovink (2019). While the theory of desire within (capitalist) society finds its core text in the work of Guattari and Deleuze (1972), desire also finds relevant

[1] Which indeed with the aftermath of the pandemic appear as lucrative and powerful as ever (Klein, 2020)

considerations as related to technology - leading further the argument of McLuhan (1964) and in the considerations of Agamben (2009), who offers a precise Foucauldian perspective on the dispositif/device - translated as 'apparatus'. Finally, among the literature engaged with the nature of secret as a tool of Suspicion, Control and Desire an encompassing author - covering and standing next to all the others - is to be found in the work of professor Ziccardi, who offered such a chirurgical precision in describing the functions of the internet and inspiring clarity in defining the role of secrecy within in, that allowed me to finally take courage, sit down and write.

Roots of Privacy & Questions on Individual liberty

Such apparent and encompassing invasion of secrecy in our everyday lives has been recently brought to media attention in the behavioural research of Michael L. Slepian (2019). His work, specifically concerning psychological distress, argues that the keeping of secrets is a repetitive characteristic of our everyday interaction, and the distress derives not simply from concealing some information, but having "to live with it, and think about it" *(Slepian, et al., 2017)*. Aided indeed by our technological devices but nonetheless already falling victim to a long process of 'hiding' and 'revealing', this is today a global milieu, made of security codes, pins, passwords, 'touch ID' technology, where everything is not simply 'personalized' but hidden and sidelined from consultation from one another, even our closest peers. In the parable of Bauman, secrecy has thus become a 'liquid' condition, boundless and leaking uncontrollably in all fields of modernity.

It is an established notion that the modern conception of privacy comes from the United States, connected to the notorious Warren-Brandeis case of 1890 in Boston. The wife of a well-known layer, Samuel Warren, became targeted by the local news because of her 'mundane life'. She was what we would call today a 'queen of saloons', with the activities of her saloon, being, in the notion of the husband, "enclosed within the private life of his bourgeois fence" (Rodotà, 2005, p. 8). With his friend since law school, Louis Brandis, later part of the US Supreme Court, they wrote ' The Right to Privacy', publishing it on the Harvard Law Review, arguing harshly against "the evil of the invasion of privacy by the newspapers" (Warren & Brandeis , 1880, p. 195)

The argument, in the words of Rodotà, was a lapalissade: one is not allowed to enter the property, just as well one may not enter the private life. The modern bourgeois requires to be protected from invasion in "the sacred precincts of private and domestic life" (Warren & Brandeis, 1880, p. 195). According to this legal standpoint, one thus takes over the 'private space', just as one is guaranteed the 'private property'. This concept already takes its roots from the *is excludendi alias*, the right to exclude the other, a notion already insisted upon by the sixteenth-seventeenth century British enclosures, where owners would restrict the use of land.

Indeed, as already Philippe Aries stated and R. Koselleck intended, "privacy becomes a right in the golden age of the bourgeoisie" (Rodotà, 2005, p. 9): yet the Warren-Brandeis article guaranteed the right "to be let alone" (Warren & Brandeis , 1880, p. 195) not simply to jurists, lawyers and their wealthy wives, but to anyone, leading the

way for "privacy revealing itself more and more clearly an essential component of contemporary liberty". (Rodotà, 2005, p. 10)

Of course the argument of Warren and Brandeis was not particularly novel, referring to themes already popular in the 19th century in both the US and England, as the right of not being photographed or protection from the circulation of unauthorized photographs (Amer. Law Reg. N. S. I (869); what indeed was a novelty was "the 'great refusal' of a privacy as a form of " isolation, abandonment" (Rodotà, 2005, p. 10). Privacy meant choosing "when to exhibit oneself and when to choose to refrain from the eyes of the public" (ibidem). This is another lapalissade regarding our social media use of today: to be let alone does not mean being forgotten, not contacted nor searched: ideally, one may be called, or texted, with a fundamental right and freedom to answer or not – while being searched, monitored, observed in the background: secretly. Here we come to the understanding of the controversial connotation of privacy, as opposed to the privilege of secrecy. For Anita Allen, privacy should be specifically an Aristotelian virtue, not a Machiavellian asset, i.e. enabling strict manipulation and seduction (Allen, 2011) – but of course, it can be. Indeed, for Zuckerberg the protection of privacy is fundamentally an "environmental problem" (Vaidhyanathan, 2018, p. 73): it implies, as stated in a 2010 interview, "a denial of communication, a restriction on movement and gaze" (Johnson, 2010).

We notice here already two things: the idea of exclusion of one for the liberty of another, and the necessity of a private 'wall' to protect from a public 'display', also a very modern concept, connected to the media and newspapers.

Another fundamental proof of privacy being a notion deeply rooted in the 'American way of life' is William Faulkner's 1955 essay entitled 'On Privacy', or, in different editions known as: 'The American dream, what happened to it?". The essay, called also by editors *pamphlet* and/or *libel*, discusses the loss of the American noble principles of individual liberty and indeed the Freedom of Press: Faulkner writes after being repeatedly asked to participate in an article concerning his life as 'author', while instead, his stance towards the editors was as simple as firm: a writers visibility and indeed 'publicity' is compressed and contained into his 'work', that he delivers to the editor and thus becomes 'open' to confrontation, study, praise or criticism. But the author must be left alone. His editors were not convinced: they claimed that the public wanted to know about his private life, and the less he was willing to give them, the more they were going to pay to have it. That he wanted or not, sooner or later, someone will do the article: the more he will resist, the more this someone will insist.

Faulkner's argument is striking and symbolic as most of his work: he parallels the 'loss of the American dream' of 'individual liberty', and thus not being 'harassed by the public', as Adam and Eve realizing suddenly that they were naked and trying to hide from God, once they were 'finally woken'. In the same way, the Americans had awakened from their 'dream', though not from the dream of Eden, but the dream that they are living in Eden. The American dream, for Faulkner, was one of freeing oneself not only as an individual from the "hierarchies of power, Church and class that have imprisoned him in the Old World, but also from the Mass in which those very hierarchies have individually oppressed him" (Faulkner, 2003, p. 75). For Faulkner, such 'mass hierarchy' is the machine of public appetite and the commercialization of the private: there must exist a

form of 'good taste' to be practiced in respect of every individual, a good taste that nonetheless already in the 1950s sounded dramatically anachronistic. This is, as he writes, "terrorizing (not scandalous: we cannot be scandalized as we have watched it grow [the loss of privacy], endorsed it and even used individually, when necessary, for our private gain) (Faulkner, 2003, p. 25)

Just like a private acre, which you can define, fence and limit, the private life becomes an object of possession. Yet, the danger of discrimination arises from another right that came to be: the right of exposure. To be let alone implies the right to make personal choices, from political vote to sexual preference, and also the right to choose how to manifest these choices, requiring nonetheless the right also to manifest such choice without discrimination or social stigma: these need to be protected by the right of privacy, with the necessity at the same time that they can be tolerated 'outside' of it. This, for Rodota' (2005), is fundamentally the reason why the right of privacy has become so popular and important in the everyday life of a citizen.

In the contemporary battle for greater privacy in respect of fair use of content, the idea of multiple selves, as opposed to a specific, public-friendly single profile is a perpetual debate. Nonetheless, the idea of such a 'vignette' of a particular individual results in nothing more than a 'mask', who expresses oneself and behaves in various modalities, depending on its environment. Turning to Canetti, the 'secret' becomes the ideal 'deceiving' method of exerting power within the mass. The profile, the 'personality' has thus evolved into a sort of 'one-way glass', where one can be and at the same time observe and monitor, desiring not to be seen, and indeed obfuscate all the rest. The idea of the person nonetheless is an ambiguous term: already its etymology as studied by (Mauss, 1966) recalls the Etruscan word phersu, meaning mask: in Latin, the 'per-sonare' is translated by Pianigiani as to resonate crosswisely (1907), connected "to a specific stage mask that in the Ancient Greek theatre whose features were exaggerated as to be better noticed from the spectators and the mouth was shaped in a way to be better heard (*ut personaret*). (Pianigiani, 1907) The person is thus a mask: not only it is not who we are but it 'exaggerates' whom we appear to be, and not necessarily desire to be. Its existence stems from a desire to conceal the individual behind the mask: it is a threshold we raise and have found being raised around us, constituting the main for on interaction. As Pizzorno argues, we also 'hide' something 'from someone': it is a participatory act. (Pizzorno, 2008 [1960], p. 51)

Here emerges the controversy concerning the mask: it is something used to expose, not to take cover or hide. Rather, it is a subversive element required to 'pretend' to be on a stage (say, the social media). The theory of desire, developed by Girard and (allegedly) implemented in the social media by his student Peter Thiel (Feloni, 2014), implies the desire to hide, and at the same time perpetually observing and self-promote itself. One's 'identity' is hidden, while the 'personality' is exposed, expressing and endorsing. Within the discussion of privacy, we notice a clear difference. The right to be let alone, where one has indeed a right to pull curtains and not be exposed to public display, is now intended as a need to be hidden. This condition has created a specific 'blasé' attitude to surveillance and monitoring: masks become so integral in our everyday existence, that as long nothing 'unveils' what's beneath, we feel safe. Actually, nothing changed: cameras observe, but in reality, for our everyday life, they do us no harm

(Giglioli, 2019). Just as with cookies and other 'data-gathering' mediums, they watch and gather but only a small fragment of 'us', who we really 'believe' we are is on the profile. With our contemporary use of social media, to be let alone actually means to be free to act without others knowing your actions. The profile design per se permits a front stage (again quoting Goffman) but truly requires invisible manoeuvring in backstage.

An evident example is noted in the work of Woodcork & Graham (2020), who in pre-pandemic times researched gig-economy delivery workers. These claimed to be perfectly 'ok' with their workhours being under surveillance, geo-localized, and monitored, as long as they felt safe to 'talk shit' among themselves of their employers and clients in general during duty. This creates a whole new idea of 'uniforms': they represent a condition, a service, and an institution: but it is simply a mask. Behind it, the person feels perfectly free to think and act as one wishes, unmonitored, though observed. The watchful gaze is ever-present, yet apparently harmless.

However, as we will now discuss, it is not harmless: very far from it. Elements of cyberstalking, doxing, trolling as well as malicious social surveillance are repetitive elements representing Internet and beyond since its institution and commercialisation. As noted already in the mid 90s by researchers such as Marx (1998) the ethical implication surrounding the web and its content are difficult to pinpoint down. What we engage with regularly is some sort of 'dystopic' un-balance between what the consumers use the Internet for and what the producers engage and use the data for (Marx, 1998). Episodes of abuse are replete and form the recurring consideration over control and censorship, becoming a growing topic within governments and families. As we will discuss, this is mainly because the Internet apparently offers some sort of a secretive environment in which users can use all sorts of remote systems of observation and control. They can make use and abuse of the animosity patterns. However, this animosity is controversial and it's not unilateral. Corporations and (ab)users may control and practice all sorts of harmful, criminal, and deviant, behaviour on the backs of fellow users. The violation of privacy in this perspective it's an endless and repetitively situation. While I will briefly mention the balance of privacy within this on life scenario it is not the main core of interest of the thesis.

To a certain extent, one may claim that from this perspective the secretive approach to internet use resembles the quintessential utopia of freedom. Online privacy is intended as a tool to protect the means of navigation - and indeed this very notion of protection will be central in the later discussion. Nonetheless, surrounded by secrets, and not allowed to access them in a reciprocal manner, we are bound to misunderstanding, falling into anxiety traps and excessive preoccupation - all symptoms of what I tried to synthesise in the terms 'suspicion, control and desire'.

Indeed, in his 'Cultural Imaginary of the Internet', (Yar, 2014) recognised how "our collective hopes, fears and fantasies about the future are now increasingly centred upon the virtual world". The virtual world indeed is per se designed around a secretive environment - made of passwords, hyper-personalised device and browsing experience - to which there is no solid ground for citizens to relate to. If for Yar the virtual reality

allowed an ideal space where to create utopias of other worlds, where to take shelter and proliferate in his own terms, the secretive space (often times imaginary or over-protected) creates itself a fantasising of what is hidden - what to hides and protect, what to scheme about, what to betray.

This thesis will thus unpack the fundamental ecology of the onlife - made of secretive conducts (passwords and individual user experience) combined with constant abuse and advantage of its environments, a specific 'secretive conduct'.
The internet has become the quintessential tool to seclude oneself - a point preceded, as noted by (Yar, 2014), by a century-long process of social 'fragmentation' as studied by Jane Jacobs' *The Death and Life of Great American Cities* (1961), followed by Richard Sennett's *Fall of Public Man* - reaching a clear media-based connection in the influential 'Bowling Alone' (Putnam, 2001), which indeed underlines that by now "engagement and interaction with our neighbours have now been substituted by a kind of pseudo-interaction and fantasy relationship with characters on the screen." (Yar, 2014, p. 63)

In our contemporary society obsessed with security and the protection of ourselves (Lyon & Bauman, 2013), what remains 'unsheltered' is our option of sheltering: the possibility of using masks not to distract, but to 'tone-down'. This is the ultimate feature of 'protection', not only from hazards, but actually from the 'ever-enhancing' and 'mimetic-desire' (Girard, 2017) features of our both online and offline everyday life features. The mask becomes an apotropaic object: one that scares away the 'evil spirits' (as intended in Ancient Greece), or indeed the 'overwhelming of noise' in the contemporary connotation. Its feature is one of actually 'logging-off', rather than be perpetually connected, so as to be constantly in control. The mask, in this perspective, becomes rather a necessary option to 'let go': the social profile in this perspective rather than a 'mask' could become a portrait, something like a 'themed' mailbox that we may consult for pleasure, rather than a 'pre-formatted' platform constantly filled with content. An example is given by the perfectly coherent homepage of tech-guru Jaron Lanier (www.jaronlanier.com): it is not a blog nor a social media profile: it is a non-default nor pre-designed website that offers basic and minimal information of the person, offering contacts and info.

This of course, as (Rodotà, 2005) notices, may lead (or better, collapse) into what Sennett already called in the conclusion of his *Fall of Public Man*: a 'Tyranny of Intimacy'. It is not (simply), as Sennett specifies, a sort of tyranny of the intimate life, as described in Flaubert's' Madame Bovary, intimate oppression characterized by a "catalogue of domestic routine" (Sennett, 1974, p. 337) that leads to claustrophobia. Nor is it (only) the result of fascist oppression, with the aid of the secret police, where the intimate life of an individual is taken in permanent scrutiny, and so one lives in constant fear of unwillingly committing some crime. Instead, the Tyranny of Intimacy implies a slow erosion of "the delicate balance which maintained society in the first flush of its secular and capitalist existence" (Sennett, 1974, p. 338), forming a "mysterious, dangerous force which was the self [coming] to define social relations" (ibid, p.339). Here, the human becomes an atomised individual, "unstable and self-absorbed" (ibidem): obsessed by the despotism of his own self, his needs, his space, his insecurities, his inadequacies, his obsessions, and

mistakes. Thus, the contemporary is not characterized by a public individual who shares everything surrounding him, quite the opposite: one has the tools to potentially share 'reality', the public, yet it is still, to use McLuhan's definition, a medium: in other words, a perfectly controlled filter. It is the power and right to control such a filter as the basis behind privacy: it is the agency to produce and share information to a public platform, while all the rest is kept hidden. The tyranny described by Sennett is indeed the need to become public, to keep eyes away from what is hidden, and thus secret: the secret behind the make-up/filter tricks of a beautiful face published regularly by an influencer on his/her account. Indeed, the concept of filter itself is quite strikingly referred to the medieval 'philtre' – a magical potion or mix of sorts.

What is evident is that while up to recently intimacy was a privilege of a few, secrecy today becomes the necessity for all: a fundamental right and form of protection, from abuse and control of the Orwellian (and apparently inevitable) Big Brother. But what indeed are the dangers of our own abuses of secrecy and protection from one another?

Today, following an argument by *(Rodotà, 2005)*, we are facing in a way the same issue as with the historical Magna Charta. If in 1215 the Magna Charta edicted the Habeas Corpus, implying that the ruler may no longer in-punitively 'lay hands over the body', since the turn of the century we strive for the necessity of a Habemus Datum, in other words, the creation and protection of our virtual identity, as to "fossilize its unicity" *(Rodotà, 2005, p. 122)*. As we mentioned above, Rodotà notices how the original right of privacy was part of a bourgeois priority, a space where to say 'no', thus one excluding the others from any sort of invasion into the private sphere. Today instead such space is perceived as a 'right to allow in': the right has evolved into the necessary safeguard of every 'user's control' over his data, wherever they are. Yet, such rights are opposed to the perpetual schemes in which such data are constantly handed over, while a simple technique of 'refuting' to hand away such data would reject to the user the growing number of actual social processes, supply of goods and services. This passage, that can be interpreted as a shift from an original notion of privacy to a principle of data protection, especially in the European context, corresponds to a deep mutation in the invasion of the private sphere. Rodotà notices how though it is dangerous and even excessive today to claim 'we are our data', it is nonetheless undeniable that our social representation is increasingly assigned to sparse information in different databases, 'profiles' forming what Lyon calls a 'social sorting' *(Lyon, 2003)*, that affects equality, the freedom of communication, expression, circulation, right to health, work conditions, access to credit and insurance. Here, Rodotà discusses how our freedom from a specific "genetic discrimination" *(Rodotà, 2005, p. 128)* is still possible as long as the large databases – police archives, healthcare, penal, taxes, credit, consumption – "are not connected with each other" *(Rodotà, 2005, p. 134)*. Indeed, such connection would produce a genuine Big Brother condition, against which the Italian author suggests the building of a specific 'ethic of surveillance', that would somewhat protect us from what, quoting McLuhan, could be a 'Global Village Control' – a sad reality the current pandemic has only unleashed its true meaning. This protection, for Rodotà, is the notion of Damnatio Memoriae, as it will be explored later in the thesis.

At the end of this section on privacy and the public we arrived at the core of the problem of privacy: that beyond the quality or condition of being secluded from the presence or view of others there is always hidden the desire to expose to others.

Desire to hide vs. to desire to expose

The concept of desire is essential to understand not only our technologies but the social effects they arouse, especially in a consumeristic and marketed society like ours. This can be analysed in a wide range of fields, which I will briefly introduce through the culture behind the justification and incitement of secretive conduct, in order to discuss how desire is connected to secrecy and how this desire is per se a form of control.

According to the magnum opus of Guattari and Deleuze, the Anti-Oedipus (1972), the notion of desire is central for modern life, capable of forming and influencing us into what Foucault intends as a fascist mentality of everyday life (Foucault, 1983). For the two French authors, it means that "the social field is immediately invested by desire, that it is the historically determined product of desire, and that libido has no need of any mediation or sublimation, any psychic operation, any transformation, in order to invade and invest the productive forces and the relations of production. There is only desire and the social, and nothing else." (Guattari & Deleuze, 1972, p. 28). In modern society, human beings became desiring 'machines', whereas "desire produces reality, or stated another way, desiring-production is one and the same thing as social production." (Guattari & Deleuze, 1972, p. 30). These desiring-machines exist as a group fantasy: the two authors mention Reich's argument, according to which the masses had desired fascism, just as today it is the gregarious mass that perversely desire their potlatches to be controlled, but desire that their desire for desire is preserved. But if the desiring machines may be intended figuratively, the persuasive technologies that surround us today perfectly embrace the consumeristic idea of both 'seduction', in their design, features and status, and the desire their technological potential opens up. Each of these machines, especially the desire machines for Guattari and Deleuze create a 'cut' (1972, p. 36), a separation: what is desired creates an isolation and a distinction. It is a "system of interruptions or breaks (coupures)" (Guattari & Deleuze, 1972, p. 36). The desiring machine allows a cut that nonetheless never halts the "material flow" (Guattari & Deleuze, 1972, p. 36), nor indeed what we may intend as the digital flow, that indeed is the internet.

Secretive conduct as a fundamental feature of modern society:

While we have already mentioned Simmel's interpretation of Secret Societies as integral within decaying social structures, in the work of Koselleck we understand the role of Secret Societies as a foundation of the modern state and fundamental character of men. In his Critique and Crisis, (Koselleck, 1988) famously discussed the nature of secret societies in the birth of a specific secret space where to criticize authority. These began to be formed in the shadow of coffee-houses, widely considered as the cradle of the public sphere and "people's public use of their reason" (Habermas, 1989, p. 27).

According to Koselleck, the most controversial members of such houses were Whig émigrés, forced to leave in 1685 France after the revocation of the Edict of Nantes (Koselleck, 1988, p. 65). They became the strongest supporters of the parliamentary constitution. Foreign intellectuals lacking a pure "political power", though socially recognized as a form of 'new nobility', had formed a new "stratum", with often different interests, though brought together by the lack of a satisfying "space" in the existing institutions of the Absolute state (Koselleck, 1988, p. 64). They were all subjects of the State yet were the antonomasia of the modern bourgeois: studied and learned gentlemen, with monetary possibilities and contracts, "though completely excluded from politics." They would meet in cafés such as the Rain Bow Coffee house, which would become a place for "masonic rendezvous" (Koselleck, 1988, p. 64); where they could not administer, but criticize the administration. This became for Koselleck the starting point of political admiration by indirect ways, a form of power that will not pass unnoticed, both to the authority and those influenced by it desiring finally to influence.

As Koselleck explains, these were times of a great debate on the philosophy of Hobbes and Locke. Individual moral conscience and political conscience faced a split between the public and private halves: one's actions are totally subject to the law of land, while the mind remains free, at least in secret. "From here on the individual is free to migrate into his state of mind without being responsible for it" (Koselleck, 1988, p. 37). As long as the subject does his duty and obeys, "his private life is of no concern to the sovereign" (ibid. 38). This nonetheless also implied that if an individual would assume to him/herself a role which is not compelled to him, especially in a subversive attitude, he must "mystify" or mask it, "lest he be called to account" (ibidem). This for Koselleck, and indeed for this thesis, is "an essential point for a genesis of secrecy" (Koselleck, 1988, p. 38). From this point, the individual will gain a personal space of his own, for which the State had to be "politically neutral". But also, Locke will open a new value of power: not simply one of State Law, to which the citizen must abide to, but also the law of public opinion, which will "come to prevail since 1688, with the rise of the Economically determinate Whig bourgeoisie" (Koselleck, 1988, p. 59) The Absolutist State had thus created a new order, and would soon "fell prey of that order" (ibid, p.39).

In this turn of power structure, "it is no longer the sovereign who decides; it is the citizens who constitute the moral laws by their judgments, just as merchants determine a trade value" (ibid, p.56). It is the citizens who decide the circumstances of what they find good and what evil: their private views "rise to a level of laws purely on the strength on an inherent censure." (ibidem) The public realm thus rises from the private one, expanding into the public one, "and it is only in the public sphere that personal opinions prove to have the force of law." (Koselleck, 1988, p. 56)

While to direct political power is reserved to the State, moral legislation acts indirectly through the pressure of public opinion, "not equipped with the State's mean of coercion" (Koselleck, 1988, p. 59) Nonetheless, it is only apparently lacking authority: though it "exists and works only through praise and blame alone" (ibidem), it is more effective in its repercussions, "for from this verdict no man can escape" (Koselleck, 1988, p. 59). Out of ten thousand individuals, not one may be spared from the "moral judgments of his fellow" (ibidem). Bourgeois morality thus becomes effectively a public

power that obliges all citizens to adapt their actions not only to "the state law, but simultaneously, and principally, to the law of public opinion" (Koselleck, 1988, p. 60).

Interest in such bourgeois morality, and a systematic change of conduct, both public and private, is fundamental Richard Sennett's work, who offered the initial insights in developing this thesis. In his Fall of Public Man (1974), Sennett notices how the notion of public is closely knit with the concept of audience, connecting visibility with theatricalization. The audience for Sennett has since the 18th century spread out of theatres and reproduced its 'fantastical' realms in everyday interaction, imitating the styles, fashions, and performances of the actors. The historical period is paramount: the cities Sennett is mainly concerned with, London and Paris, were indeed the largest and ever-growing capitals of Europe. They were 'overtaken' by strangers and 'cosmopolitans', who would now need a new mode of expression and interaction to build their characters, be noticed, interact with other strangers: this would happen in public but between personalities. The 19th century becomes fundamentally an age of spectacle, where windows of the giant, newly conceived department stores allowed being out in public "at once a personal and passive experience" (ibid, p 145). Buying clothes by the 19th century would express 'who you were', forming a new idea of 'private', one where "secrecy is the price for continuous human contact" (ibid, p.148). Secrecy becomes a requirement in order to bear all the various stimuli and interaction that the new cities offered: here we see the wandering of the flaneur and his 'blasé' attitude, the desire to withdraw into our personal, private and silent spaces, instead of interacting, discussing, conversing. Clothes, again returning to Sennett's arguments, helped as a shield: not expressive as in the 18th century but concealing, covering; they would offer a secret language, with no clear rule of interpretation if not to the 'initiated' to a particular fashion. The public actor, as Sennett calls it, is ultimately to be perfected: we analyse it and is analysed by everyone, giving out nothing of himself if not precisely chosen, selected. All impulses are suppressed, the expressions are sophisticated and almost impossible, if not with the use of expert psychoanalysis, to be interpreted.

Yet, this also is just a façade. The shield around us only forms a tesseract around fears, paranoias, and sicknesses that characterize the modern citizens, with a constant "fear of involuntarily, erratically expressing oneself, from one's bodily needs to one's feeling in the family circle" (Sennett, 1974, p. 182). Secrecy becomes the fundamental cause of psychic distress, caused by the fear of a "superimposition of public and private imagery, defensive withdrawal from feeling, and increasing passivity" (ibid, p.194). The 19th-century theatre audiences in Paris and London would observe plays in silence, as the 18th-century habit of expressing disdain during the show was now considered as vulgar. The theatre had become a narcotic engagement, of silent awe, where only particular, specifically entitled and charismatic personalities could express themselves, inspiring and commanding. This has, for Sennett, fundamentally changed our relation not only with leading figures (from the public actor to the politician) but also has formed an 'ideology of intimacy', where the "belief in closeness between persons as a moral good is, in fact, a profound dislocation which capitalism and secular belief produced in the [second] last century" (Sennett, 1974, p. 259). This fear of public exposure indeed would have altered our approach to friendship and intimate companions, being overly concerned with 'binding' and creating trust, an approach that nonetheless only leads to relations

constantly testing each other, leading either to conflict or to becoming soon bored of each other.

The rethinking of our intimate spaces is best understood by Sennett in pointing towards the problems, rather than the solutions: the tyranny of intimacy, as Sennett points out and indeed concludes, lies in trying to find a public meaning maintaining its private form, refuge, shelter: one nonetheless cannot live, nor do without, the other, as we will see in the following.

Surveillance towards a crumbled intimacy (backstage) within the home

On a similar line, the work of Philippe Aries is ground-breaking in describing the fundamental intimacy shift in the everyday life, especially in the domestic (back) stage (1960). There, up to the end of the seventeenth century 'nobody could be alone', and rooms had no distinction in their roles or specific furniture, instead "in the same rooms […] they ate, people slept, danced and worked and received visitors" (Aries, 1960, p. 381), often all in contemporaneity. "Social isolation was virtually impossible" (ibid, p.385); independence was exceptional. Only by the eighteenth century "family began to hold society at distance', with the first example of domestic life: privacy and isolation as a common feature not simply for nobility but middle class as well. Beds would be confined into bedrooms, as well as toilets and hygienic equipment to their appropriate rooms. It is here that we learn the essential distinction between a chambre (room), as opposed to the word salle (salon): a specific 'decent' distinction between where visitors may enter, and where there must stay out.[2]

Such argument comes in strict relation to the 'liquid' state of our contemporary times, and the perpetual shifting of spaces and spacing of roles and spaces. Shifting toward the analysis of the contemporary issue of surveillance, control and perception of control, the conversation between Lyon and Bauman in 'Liquid Surveillance' (2013) is extremely enlightening on several issues, twirling with profound knowledge of the various tinges of the subject. Specifically, Bauman's contribution unites his notorious concept of adiaphorization to the topic of surveillance, defining it as a 'disabling moral resistance against the committing of immoral deeds and the sole use of criteria of instrumental efficiency in the choice of ways to proceed" (Lyon & Bauman, 2013, p. 82). For Bauman, what this means is the risk of forming a system of control leading towards an 'automatization' of authority, lacking any "consideration of morality" (ibid. p.13). The discussion is aided by the views of David Lyon, who with a sociological, anthropological and criminological approach discusses the risk not only of total surveillance but how this surveillance forms a system of complete control for the worse reasons: it monitors and judges indiscriminately, loosing nonetheless at the same time the capacity of actually 'discriminating' what is supposed to be monitored.

Their work has been connected to the key notion of 'liquidity', coined by Bauman, that regarding surveillance underlines a condition "without a fixed container, but jolted

[2] Such considerations become ever-more impressive with the COVID-19 outbreak, a work which I feel entitled in engaging in the near future.

by 'security' demands and tipped by technology companies' insistent marketing, surveillance spills out all over" (Lyon & Bauman, 2013, p. 9).

Within their conversation, the Foucaldian panopticon is compared to the contemporary marketing monitoring, studying the patterns of consumption, showing the repercussions in the everyday life of the privacy techniques inside our technologies. Specifically, for Lyon the idea of privacy has died, especially because of this online 'data analysis' aided by 'invisible eyes' such as drones and indeed, a truly 'social control', made by common observance and monitoring through social media. In this condition, surveillance is truly liquid: one cannot simply 'spot' a CCTV device and walk away from it: the whole system and modern society with it are 'dipped' into its influence and schemes, creating what Lyon calls a 'social sorting'. Bauman and Lyon notice how there is never 'enough' security: over a certain limit, we may never do without it (Lyon & Bauman, 2013, p. 90). Fear generates further fear, forming a sort of paradox, where "on the one hand, we are more protected from insecurity than any past generation; on the other hand, though, no previous, pre-electronic generation found the feelings of insecurity such a daily (and nightly) experience" (Lyon & Bauman, 2013, pp. 91-92).

This is the way how the controversy between the public and the private was dissolved, preparing the suitable devices for managing both.

Ever-accessible tools to control and be controlled

The device thus - especially the smart ones - has become a central object of everyday life. To understand yet what is meant by devices, a word important also for Foucault's *dispositif*, as we mentioned before (Foucault, 1978), a central definition is found in the short text by Giorgio Agamben, "What is an Apparatus?", published in 2008, right when the smart devices were becoming objects of mass consumption (in that year iPhone 3G was launched, selling 1 million devices over the first weekend (Apple Inc., 2008)). In the English edition, the word *dispositif* is used and translated variously: apparatus, device, dispositive (closer translation to French and Italian) and also machinery. For Agamben, the apparatus is "literally anything that has in some way the capacity to capture, orient, determine, intercept, model, control, or secure the gestures, behaviours, opinions, or discourses of living beings" (Agamben, 2009, p. 14). It is thus a recollecting tool, but also influencing and subjugating, which 'incessantly' models, controls and contaminates the life of individuals. Indeed, "the nature of an apparatus is essentially strategic, which means that we are speaking about a certain manipulation of relations of forces, of a rational and concrete intervention in the relations of forces, either so as to develop them in a particular direction, or to block them, to stabilize them, and to utilize them." (Agamben, 2009, p. 2) Their existence is one of constant strategy: offering and producing grounds for allows schemes over the subjectivities (subjects – subjugates?) of fellow citizens - a pure deviating device (de-vice?).

On this note, a final fundamental mention must be given to the instructive work of Ziccardi which has been essential in the development of this thesis. Professor of Legal Informatics at the State University in Milan and lecturer in cybercrime in Bologna,

Ziccardi's 'Internet, Control and Freedom" (Internet, Controllo e Libertà, 2015) argues that the four fundamental elements connecting the society of information are:

1) the secret in the digital age,

2) digital transparency,

3) electronic surveillance, and

4) the technologically-produced control,

Such a framework, Ziccardi notices the secretive activities of a Government, "to the operations of the organizations and the centres of power more or less secret and the managing procedures of the flux of documents in the public sector" (ibid. p.19), but also of the existence and activities of espionage and counter-espionage, the notion of secrecy in the digital era becomes an essential and most arduous factor to be maintained and, at the same time, sought with ever greater intensity. As shown by the Datagate scandals and the Wikileaks phenomena, the notion of secrecy can cease to be a vantage in the hands in power, and rather turn into a sort of vulnerable point.[3]

Ziccardi mentions the emergence of an actual "power over the secret" *(Ziccardi, 2015, p. 19)* on behalf of the citizen, which indeed becomes a somewhat accessible and 'open' process of 'unveiling' other's secrets 'for a public interest', in particular regarding the private sector (as in the example of large multinational corporations), to the point of 'disclosing' "certain aspects of an admiration reaching the State secrets and the occult actions of the intelligence agencies" *(Ziccardi, 2015, p. 20)*. Within this context, the secret becomes an essential tool in the hands of a whistle-blower, through the practice of leaking. The secret, in this context, also raises the question of actual animosity online, and how for example this can protect the liberty of expression.

According to Ziccardi, Julian Assange's distributing of 'secrets' have opened the debate on what can be defined as 'radical transparency', with its pros and cons, especially regarding national security and sovereignty: an issue that criticizes and yet at the same time, controversially, promotes the spreading of surveillance in the everyday activity of online users. Especially in the case of 'secret surveillance', we can easily notice how never before have there been so much data referring specifically to people: "never so precise, never so intimate, never so linked and controllable, so useful and focalized for those who decide to surveille" *(Ziccardi, 2015, p. 23)*. These tools of surveillance and control, because of the invasive qualities of the contemporary technologies and their "constant presence in the everyday life" (ibid. p.25) have transformed into "a sort of dependence on the technologies (oftentimes, incorporating tools of control) that facilitate, through human behaviour, control itself" *(Ziccardi, 2015, p. 25)*. Indeed, in this very context Ziccardi helps to pose the question whether the citizen has today "margins to resist" *(Ziccardi, 2015, p. 26)*, in other words if he may use the very technologies used to control his data, or indeed if he can somewhat oppose to the diffused surveillance, reconquering the right over his lost privacy.

[3] More will be said regarding the even more recent Cambridge Analytica issue.

Seemingly the problem of privacy and the public takes place on governmental and juridical level, although it very likely that such things are already removed from their control and function in complete secrecy, as we illustrate it in the next session of literature review.

Secret as power

Secrecy, for Canetti, "lies at the very core of power" *(Canetti, 1984, p. 290)*. In his Crowds and Power, he understands the secret as indeed those stealthily means to lie down and hide in the crowd, camouflaging the self and thus embracing the invisible; in this condition, those who behave in secret can observe without being seen, wearing its 'cloaking' essence as a "second skin" (ibidem). Patience is the core of its power: never revealing itself, even if the desire is strong. Here we stump upon the central force of the secret itself, the power of its influence and moreover its 'potential' that is idle but perpetually released: the secret is something that waits: it is hidden but its concealing place always in danger of being discovered thus must always be protected. The secret is powerful as long as it is hidden, thus it must never be too obvious, or all efforts will do done to have its location revealed. This is the basic principle of its power, by never fully revealing nor its core nor its concealing place: "The power of remaining silent is always highly valued. It means be able to resist the innumerable provocations to speech, treating questions as though they had never been put and never letting it be seen whether what others say has caused pleasure or the reverse. It is voluntary dumbness; and it is not deaf. The stoic virtue of imperturbability, if carried to the extreme, would lead to silence." *(Canetti, 1984, p. 294)*

By remaining silent, the secret never shows its potential fully, because once it is shown it releases thus expires its power: it must remain in a form latent object: the potential is in 'sleep' mode: always present, always reachable, but never revealed. Everybody must know it is hidden somewhere: it must never be forgotten, because forgetting is also a means of losing power: it must be part of the collective memory constantly. "The secret concealed in silence should never be forgotten. Its possessor is respected for not surrendering it, even though it grows him and bums him more and more fiercely." *(Canetti, 1984, p. 294)* The secret is there, perpetually, somewhere: "Everyone who knows something is watched by a second person who, however, is never told precisely what he is watching for. He has to record each word and movement, and by full and frequent reports, enable the ruler to assess the loyalty of the suspect. But this watcher is himself watched and his report corrected by that of yet another." *(Canetti, 1984, p. 292)*

The items of interest (our data) are protected and stored only to be further analysed, distributed, sold: protecting data only to further control it. The very 'power' of such a system lies in creating a condition where one feels safe to expose, only to be – softly – placed under the attention of what he was interested in. A feel-safe factor is a definite tool of the secretive conduct: by rendering the user safe to gather information, such data is stored privately in private devices, but private within a private enterprise and sold privately.

We can understand its similarities with the predatory state of latency. A condition of dormant 'suppression', where the subject, the force, the 'secret' awaits: As we have seen, it is a masking technique, used through history for means of divinization (shamanic and sacrificial) and obscure secret societies, becoming yet today so common and essential to social relations, almost the required feature of interaction, to the point of becoming a required status for wellbeing: "Let us define the concentration of a secret as the ratio between the number of those it concerns and the number of those who possess it. From this definition, it can easily be seen that mode technical secrets are the most concentrated and dangerous that have ever existed. They concern everyone, but only a tiny number of people have real know- ledge of them and their actual use depends on a handful of men. " *(Canetti, 1984, p. 296)*. So is the nature and potential of the capta regarding us, stored in hidden servers – to which we might never find out the purpose; until it is too late.

Suspicion and deceit:

The secret implies something hidden: something that is covered and is in 'perpetual' liminal state. It is not forgotten, as if so it would no longer be a secret: secret is something kept well in memory of those who hide, and custody it. The subversive element of secrecy relies in a particular, ambiguous word- understood in the notion of latency. In Pizzorno, covering up the essence of who we are, we lose the sense of what is real. The mask also allows the crowd to camouflage into the one. It becomes the very weapon of concealing and deceit: it mutates the body and covers it features (pain, sickness, fear, joy, euphoria) that are otherwise 'manifest' and thus 'evident'. The concept of latency further empowers this subversive attitude. It is the very environment that allows one to hide and safely hide again, without being noticed.

Latency thus holds (hides) in se the riddle with the 'problem' of secrecy, and clue to unlock it, manifested in the ambiguousness of its etymology: lethe, source of forgetfulness and oblivion. Latency, central word of this argument, originated from latere, "lie hidden, lurk, be concealed," a concept implying the idea of something actively hidden yet potentially dormant and thus passively exposed and exposable, fascinatingly connected with the Hellenic mythology of the river Lethe. Indeed, in the Orphic eschatology, once the deceased reaches the underworld, he is expected to confront obstacles: he must take care not to drink from the infernal river Lethe ("Forgetfulness"), but instead reach the pool of Mnemosyne ("Memory"). He is provided with formulaic expressions with which to present himself to the guardians of the afterlife, where the divine fragment of the self would reconnect with the immortal destiny (Carratelli, 2001). For the Hellenic cults with proper instructions forgetting could truly "purify" (catharsis) one's soul, instead of constantly "reincarnating" the secret and thus carrying the burden. But these where nonetheless hidden practices, shared only with the few adepts of mystery initiations, as magical medicine (pharmakon) to the few who believe. It was also a deviation from what was, possibly, a more natural solution: a-letheia, the Heideggerian truth, the opposite of what is hidden, and that cannot be forgotten. Thus, possibly, a confession is curative force, so that the community and the victim may understand, forgive, and finally truly forget, without being afraid of surviving traces. The etymology of Lethe, as mentioned before, becomes an ever central: what is the connection between concealing and forgetting? Possibly, if one risks forgetting the very source of his 'persona', it is the one has a better 'memory' (another evident technique) that is advantaged in manipulating both oneself and the others. It is a mask

we forgot that we are wearing, until one notices that everyone is wearing it, and he can change (itself without evident manifestation. There is nothing wrong with desire, except when this desire is used as a trap, which then indeed becomes a self-perpetuating trap: wanting to know, and eventually wanting to perpetually hide. Latency appears to become the central word to which the suspicion, control and desire formula abides. Latency is the possibility never to forget, and rather, remain idly active and act (read strike) when no-else is aware.

Ecology of 'opaque' harm and control

A specific Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy (2016) and, offering precise and fulfilling consideration on the systems of control and data collection, can be found in the 160 pages long research of Wolfie Christl and Sarah Spiekermann. There, the two Austrian social scientists underline the various tools and functions available online to Corporations to monitor, recognize and analyse individuals in many life situations, creating digital tracking and profiling ecosystems. Such a report becomes even more significant by combining it with the elements of social harm reproduced in the gathering and collecting of data, as reported in the Data Justice Lab (Redden, et al., 2020) – where a precise recollection of the elements of data-harm are regularly updated by Joanna Redden, Jessica Brand and Vanesa Terzieva (2020), involving loss of privacy, inequality, discrimination, identity theft, social sorting and even physical injury.

Such elements contribute in the connection to the onlife ecology we are defining, as these conditions appear fundamentally opaque- meaning not fully transparent and mysterious in their nature and functions. We can engage in this concept in many of our fundamental theorists: in Floridi (2015), we find the consideration whereas Algorithmic systems, acting as new epistemic membranes, seem to increase the opacity of many social phenomena. They are also changing the ways individuals are (automatically) identified, tracked, profiled or evaluated, often in real time, adding opacity (invisibility) to traditional systems of identification, evaluation and, thus, of "government" (Floridi, 2015). In Lyon (2003) we engage in the argument of social sorting through opaque forms of 'discriminations'- whereas users would be denied access, funding, financing, based on the result of the data recollected on their behalf- returning to the dangers of discrimination. Offering specific and well-researched examples, (Spiekermann & Christl, 2016) prove how such opaque systems are "still poorly understood by the majority of users" (ibidem, p.10), nor do users own effective options to resist the power of such data ecosystems. Also, Christl noticed, in an updated report, how instead users rely on apparent 'open' data-software-downloading and using content for free, while offering precious information's to 'data brokers' such as Oracle, quietly handing out users' consented data to eco-systems with real-time persuasive tools such as "digital tracking and profiling, in combination with personalization and testing, […] not only used to monitor, but also to systematically influence people's behaviour." (Christl, 2017, p. 84).

Framing the Zemiology of Secrets

This thesis engages with the elements of harm that go beyond the basic notion of 'cybercrime' - thus attempts to engage with the novel conceptualization of a digital zemiology of secretive conduct. This is central as to immerse in a scholarly fashion in the various conducts that users engage within the onlife scenario. While privacy is well predisposed as a feature protecting users, secrecy is here approached as the consequential detrimental effect. This is not to say that secrecy per se is dangerous, - indeed as mentioned in the above chapter it is a central and recurring aspect of society- but the current and overall technological tools that replicate the elements of secrecy in the onlife ecology allow a series of harmful conducts. Secrecy becomes the unwary and incidental cyber-tool for spying, controlling, manipulating - and doing so, and wanting to do so with endless means.

As with Hillyard and Tombs(2004), much of the consideration of this doctorate lies in the idea that the harm caused by secretive conduct is a product of 'Neo-liberal' globalisation. This involves the reckless advancement of technologies in the name of highly sectarian profit, with very limited concern for the social implication of these very advancements. The Neo-liberal paradigm is evident in the way in which smart devices were launched (shoved) in the market and flooded the everyday interaction, though platforms that just as well were shoved in the lives of people - along with its implications, technologies, tools, instances. For the large part, we stood watching, trying to understand how to use these, and pretend we enjoy them. Many others took great advantage of these features, of whom I tried to define only a small, hidden portion, under the conditions of S.C.D. Such conditions replicate the criminogenic theories of the General Theory of Crime, the imitative elements of Social Learning and even the implications of Routine activity theory. All of these theories recognise the elements in which users take advantage of the secretive elements of the onlife and engage in harmful and cybercriminal activities such as cyberstalking, trolling, doxing, interpersonal electronic surveillance (IES) as well as more 'traditional' (but enhanced) cheating or simply controlling partners, siblings, kin. However, while this is a very broad perspective on a very central aspect, my approach in this work is to engage with the unexpected elements of harm that take place in the everyday onlife of globalised users. By unexpected, my work implies understanding how users replicate these elements of suspicion, control and desire take place without being aware of the harm involved. And the victims of these harms are oftentimes claiming neutrality to the very harms. Such conditions create a potential replication of the very nonpunitive elements: Instead, as for the General Theory of Crime forwarded by (Gottfredson & Hirschi, 1990), the low-self control conditions are favourable for the replication of criminal activity. Yet, as we will see, the smartphone per se is the haven of disinhibiting any concept of self-control. It allows instant access, produces immediate, high-quality graphic content - allows hidden and covert elements of surveillance and control. It renders the above-mentioned elements of harm in the onlife scenario trivial and perpetually replicable and imitated. How to tackle and create awareness of the dangers of cyberstalking when Apple itself, one of the leading tech companies in the world, places in the market a relatively cheap yet fancy GPS tracking device, ideal for cyberstalking? (Matei, 2022)

In such a scenario of moral indifference, even the analysis of social learning (Akers, 1998) becomes almost trivial: the actions of harm endlessly interact among private and/or public groups; the imitation of the very behaviour is endlessly accessed; the covert elements allow a basic area of reward and also unpunishment. This goes further within elements of interpersonal crime, within a specific ecology and topology of cyberspace (Yar, 2005:414). In particular, the Routine Activity Theory becomes yet another ecological approach to crime causations and as such is dependent on the ability to look at offenders and targets in space and time - criminogenic when no capable guardian is present. Indeed, in this work I've engaged the episodes of 'shadowing' the very guardians, and recollecting how they would become 'cyberstalkers' of the assets they wished to protect, be it their partners, lovers, siblings, or children.

As a follow up to the Beyond Criminology (2004) zemiological perspective, the criminological approach of this work is thus one of "labelling and sanctioning these extensive forms of harm" (p.4). Crime appears a limited output, as it is too focused on time and place of specific instances. Instead, the harm perspective allows In the current scenario, the technological able, the parental and hegemonic 'strong' is evidently in power over the technologically, economically, subjugated weak. Yes, the harm involved is very digital and extracorporeal: oftentimes hidden and unperceived. The episodes of monitoring and controlling are well 'obfuscated' if not justified within the liminal boundaries of 'care'. But it is indeed in this 'secret' aspect of what is involved, and the effect of this involvement that this thesis is important for criminology. Secrecy of the Onlife becomes an ideal and unique way to engage with the elements of crime that are otherwise vaguely perceived as problematic, such as monitoring children remotely, observing partners' online activity, distributing harmful content, and overall replicating trivially elements of suspicion, control and desire that are growingly entangled in the (secret) habitus of the onlife.

This work proposes itself a novel approach to dealing with the issue of crime and harm focusing on the novel conceptualisations of the onlife. If other scholars, such as Jaishankar (2007), defined Cyber Criminology as "the study of causation of crimes that occur in the cyberspace and its impact in the physical space" - this work offers promising research observing not only the criminal elements that characterise the onlife scenario, where the cyber impacts the physical, but approaches these in a zemiology perspective, proposing a specific scenario for the study of digital or onlife zemiology. Digital harm has been theorised in an evident parallel of this thesis in the work, among others, of Gordon, Faith; McGovern, Alyce; Thompson, Chrissy; Wood, Mark A. (2022), recognising indeed a 'Beyond Cybercrime' necessity, a prospect previously forwarded by Yar (2015). This work wishes to combine the elements of cyber harm with a novel conceptualisation of the culture surrounding the causation of harm. In this, the effort of these years recollects the cultural criminology inspiration with an ongoing conceptualization of what our internet experience is turning in and the tools involved.

Secrecy is the core interest of this approach, and it is criminological significant and relevant for a number of reasons.

First, secrecy is the hidden dimension that alters our transparent existences. It does so knowingly and unknowingly, with covert and ambiguous dynamics. Secondly, secrecy involves hegemonic implications, and unaware elements of power, prestige and invisibility. Thirdly, secrecy is a shade of privacy, though one with enormous influence and serious implications that are marginally engaged in the social sciences. Fourthly, secrecy involves unheard, hidden and oftentimes unaware elements of both harm and victimisation.

My contribution to the field of criminology in this perspective is combining the elements of secrecy with technology, especially the smart devices at our disposal. As I will discuss, the smart features replicate the elements of secrecy and secretive conduct that enable a series of harmful results. By approaching the secretive elements of smart devices and onlife technologies in general, I believe a novel understanding and direct tackling of its harmful effects is not only achievable but necessary. For too long we have mindlessly made use of tools that harm us and do harm around us. I wish with this work for this to be no longer a secret.

Secret-recollection and surveillance

A leading literature related to such theme, that have become basic texts in understanding, denouncing, and criticising the opaque, backstage manoeuvres of Big Tech, finance and state organizations is to be found in F. Pasquale's "Black Box Society" (2015) - central in defining the workings of data recollection and algorithms taking place 'at the back' of consumers. Such study may also be connected to the 'Anti-Social Media' (2018) discussion by Vaidhyanathan on Social Networks and everyday crypto surveillance.

In the first, Frank Pasquale underlines how our equivalent of secretive conduct is part of the Big Tech apparatus, the storing and protecting data ecology that characterizes contemporary life: The Black Box thus – a device once limited on airplanes for recollecting and storing flight data in a secured and shock-proof retrievable manner – is today a recurring and essential feature for storing and analysing characterisation of our online – and practically everyday-activity: influencing our lives in innumerable ways, from finance credit, advertisement and work opportunity. Indeed, through an ever-growing and sophisticated system of algorithms, Pasquale's main argument relates to the "Internet and finance companies that accumulate vast amounts of digital data, and with it intimate details of their customers'—our—lives" (Pasquale, 2015, p. 4). For Pasquale, there is a specific infrastructure whose purpose is to personalize as much as possible the online user and digital experience, with its searches, tastes and preferences, as such data would become exponentially valuable. While there is a palpable users-secrecy apparatus from the public - as related to the bank balance of a user - it is a 'one-way mirror: Indeed, of the actual actors 'behind' the 'front stage', the 'invisible hand' that has access to such information, and we do not know 'their' workings. The Black Box Society thus recollects everything, more or less indiscriminately - only later re-proposing content, reanalysing it - thus defining fundamentally indiscreetly our wants, needs, and thoughts, with the ultimate capability of influencing it; - a pure latent *capta* manner. The Black Box Society thus embraces the "paradox of the so-called information age" (p.19); indeed, it is a system

within the System, surrounded by an aura of secrecy: it is a secret what the corporations know, how they act, what do they presume, what do they prepare for (such argument is led forward by Beer (2016)).

Pasquale's concluding effects are not only regarding a white-collar crime perspective: according to Pasquale, the "companies that control these processes are some of the most dynamic, profitable, and important parts of the information economy": the information obtained, along with the secret algorithms they use, rely on the ever-longing quest of predicting the future that nonetheless, "however profitable […] is dangerous to society as a whole" (Pasquale, 2015, p. 217). The list of dangerous outcomes - corporate and individual - of such a system is majestic: not only through social sorting of innocent individuals as indiscriminate and hurt, "branded as security threats or goldbrickers or credit risks by inaccuracies that they can't contest and may not even know about" (p.217), but also create an "unfair or inappropriate considerations combined with the power of algorithms to create the failures they claim to merely predict." Moreover, Pasquale notices, the failures in predictions (as in the 2008 housing crash) are hard to be recognized and their causes revealed - not to mention being called to question and incriminated.

If Shoshana Zuboff has defined the market workings and profit over our data with her Surveillance Capitalism (2018), in Siva Vaidhyanathan's *Anti-Social Media* (2018), we see the variation of this control theme in understanding the uses social networks and media not only in being controlled, but controlling each other (this was also discussed by David Trottier as early as 2012, with the idea of actual everyday life being monitored 'without [anybody] even being aware of it'. If everyone is potentially watching, they will also be 'hungry' to see also what is not 'shown'.[4]) Vaidhyanathan notices the everyday life dangers of surveillance: not simply being observed by a remotely controlled CCTV camera, but filmed, recorded and observed through high definition lenses of smartphones, available virtually everywhere and always at hand, whereas "anyone of us who carries a camera attached to a mobile phone in an agent of surveillance" (Vaidhyanathan, 2018, p. 53). Again, the implication is one that secretive conduct is a central tool of the very Big Tech, whereas, without such mediums, the entire system would not operate. The harm is embedded in their design.

In addition to potentially being constantly filmed at any given time, breaching our privacy, one may be targeted and used for revenge, especially in specific social networks groups and circles. According to the North-American author, Social Networks, with particular emphasis on Facebook/Meta, offer practically uncontrolled platforms for not only revenge porn, but also "incidents of humiliation, harassment, and unwanted exposure" (Vaidhyanathan, 2018, p. 54). Vaidhyanathan implies that public profiles and 'newsfeed' is simply the tip of the iceberg of the real manoeuvres of this social network allows and permits. In reality, what surrounds us is a "cryptopticon", "an inscrutable information ecosystem of massive corporate and state surveillance" (Vaidhyanathan, 2018, p. 67). The Social Media thus ultimately produce a Surveillance Machine, to which

[4] We have examples of this public shaming of highly popular 'influencers', but also through the global COVID-19 lockdown, with cases of filming and monitoring, and subsequent commenting and shaming, of other citizens not 'conforming' to the norms and putting others 'at risk' of contagion (Hess, 2020).

the smart device is the ultimate tool, which "have enlisted us in a massive, global, surveillance effort run for the benefit of both commercial powers and states", to which we appear to have willingly abided (more or less globally) as users, without clearly knowing the consequences and effects. Moreover, "Facebook is also an anxiety machine, an anger machine, and a resentment machine." (Vaidhyanathan, 2018, p. 51) Striking is Vaidhyanathan's comparison with Aristotle's ethics of friendship - divided into mutual, pleasure-based and brotherly -, as opposed to Facebook/Meta's generic and universal category of Friends, implying that even the corporations themselves were somewhat clueless of the sociological, political and criminological devastating effects of such platforms, promoting instead, in the name of undisputable profit, what they "believed" to be was system of generic freedom and openness. One that, as we shall further analyse, resulted in quite the opposite.

Such perspective is, as we will see, well explained in David Lyon's lifework, discussing the invisible burdens that perpetually threaten us and have found recent confirmation in the 'Facebookgate' scandal of Cambridge Analytica. Along with the previous ones of Snowden, Manning, and other whistle-blowers, contribute to an ever-increasing the milieu paranoia and insecurity over our information (Lyon, 2018): requiring unendingly to protect ourselves, but also to increase our secrets and to hide our actions: the creating of a shady and opaque eco-system that surrounds technology, algorithms and its users/producers. This is connected to a further 'tuning' of the 'opticon' type analysis, one coined by Siva Vaidhyanathan as 'cryptopticon' in 2011, that calls attention to a "cryptic, hidden, scrambled and mysterious" monitoring reality, where "one can never be sure who is watching who and for what purpose" (Vaidhyanathan, 2018, p. 67). Such argument is led forward by Byoung Chul-Hal in considerations on the *aperspectival* panopticon, underlining its "omnipotence of the despotic gaze […] of everyone from everywhere, which anyone can perform." (Han, 2015, p. 45) of its surveillance features. This today even more significant with the contemporary discussion on using citizen's data and biometrics in order to track and prevent the spreading of the coronavirus *(OECD, 2020)*, with the somewhat ambiguous discussion on how to use citizens' private data, monitoring their whereabouts, without actually creating some sort of liberty breach. The state becomes a watchful eye as long as the citizen acts on its behalf: a perpetual spiral of observing and hiding.

The Malicious normality of cybercriminality

Without the smartphones that we use today and their functionalities, the criminality that we're discussing would not be possible. Most of this secretive conduct would not exist. Smartphones replicate all the elements of cyber harm from stalking to doxing and to doing surveillance which are the core aspect of this thesis. Cyber criminality has become a traditional form of doing crime and criminality. Smartphones have become a traditional tool of our everyday life. In this additional section, I will try to pinpoint the literature surrounding cyber criminality, especially regarding harm that may leak within the onlife scenario.

While this is no place to describe the history of the internet or cyberspace in general, it is interesting how these systems have diffused unabated despite important concerns about the impact on individuals and society. No matter the concerns over the use of data and the formation of surveillance; the destruction of social strata and cultural apparel, the technology has advanced rapidly and entangled into the onlife scenario this thesis borrows from Floridi. Cyberspace, born from a military environment and echoing the horrors of a dystopic uber-controlling brutal realm has instead become, aside from trivial concerns, a central aspect of our lives. It is undeniable and unavoidable. And with it, the crimes and harms that seem also integral to our civilization.

The connection between some sort of malicious nature within the cyber realm has been conceptualised from the very beginning of its formation. The word cyberspace was used in a dystopic scenario of William Gibson's, 'Necromancer' fittingly published in 1984. The book describes an 'consensual hallucination' formed by the hegemonic power of multinational corporations. The panoptic/Orwellian elements of this scenario, that characterize Foucault's conceptualisation, render indeed Bentham's "private, profit making institution" (Melossi, 2008, p. 18) as fitting as one can get. As we will discuss in part 2, in opposition to the utopistic agenda of Barlow's vision of a free cyber community, Gibson saw only abuse and "a constant subliminal hum, and death the accepted punishment for laziness, carelessness, lack of grace, the failure to heed the demands of an intricate protocol." (1984). In this perspective, cyberspace per se represents some sort of replete environment of deviance and harm: limitless and unregulated. In the hands of few and in control of all. Indeed, if *cyber air makes us free*, when looking at the element of secretive conduct this is it is interesting to notice how secrecy is a particular aspect to be imitated.

This is because secrecy is something that per se would imply that it's taking place in so sort of privacy, and thus not evidently visible. Elements of imitation or modelling engage with those of people observed and how are imitated to observation. However we address it, the cybercrime theories offer an understanding of the cyberspace and the users within it recollecting the armed elements of harm and unease that are well integrated in our everyday use. Again, the recognition that defined criminals and the actors in this cyber realm is extremely difficult. As mentioned above, the routine activity theory helps with our ecological and topological understanding of cyberspace (Yar, 2005:414) for understanding crime causations. This is central in the thesis for the ability to look at offenders and targets in the time in place. But more than the simple implications and the motives of defenders, other theories on how crime and criminality endure online, and in our onlife scenario, can be used. Central among these is the Social Learning Theory, that based on the differential Association theory that proves how crime is a learned behaviour (Sutherland, 1939) and has specific connections with the idea of imitation (Dearden & Parti, 2021). Further developments of this understanding are evident when looking at the conceptualizations of Akers (1998, 2009), and the Chicago School interactionist general theories of crime and deviance that were developed over Sutherland's attempt to criminalise corporate malicious activities. Crime is learned through intimate interactions (Sutherland, 1995)- deviant peer associations.

Self-control is a recurring object of consideration when looking at crime prevention. However, as pointed out by Dearden & Parti (2021), in the cyber-space cyber offending is caused and influenced by the dynamics of recidivism and communication. Observation - used throughout this thesis as a method -does become a mother reference when engaging in social or antisocial behaviour. This smartphone secretive conduct essential in this because the elements of deviance taking place through the smartphone become noticeable thanks to the separative of aspects that the smartphones allow. The smartphone does allow to be antisocial within a social environment. The smart device has long offered itself as an object to fill the gap of perpetual connection with mobility, and thus 'cut' any possible 'physical' distancing from users. This feature was first introduced by the end of the twentieth century with wi-fi technology, allowing namely a wireless internet connection to users, still somewhat limited to the use of laptops and bulky mobile gadgets. The mobility of 'data' connection allowed devices to perform any form of navigation in any space and environment that allowed signal. Such technological evolution reached an initial prestigious peak with the popularization of the first-generation iPhone (2007). As we will discuss more in detail later on, such device could allow users to consult email, web, pictures and practically manage and entertain life at a tip of a finger. Suddenly, social isolation became an entertaining matter: as one can consider watching the original Apple Corp ads of the first iPhone, the fun of screen interaction would be interrupted by actually someone calling you: interacting with others appears to be the last and least desirable feature of a mobile device. This is an integral aspect of the onlife.

Smartphones thus, in the general realm of onlife secrecy, creates the very setting in which favourable condition to deviance are expressed and reinforced. As discussed in the recent and insightful work of (Herrero, et al., 2021), it appears that smartphones addiction replicates the elements of the General theory of crime (Gottfredson & Hirshi, 1990). According to the theory, individuals with low self-esteem are attracted to behaviours that are impulsive and risky. This is interesting when we look at the dynamics of smartphone that will try to show and indeed its way of trying to lure users into specific conduct that with the status we show as evidence of harm. As we will see, as a side consideration to the scope of this thesis, one needs not being an addict to replicate this conduct: simple, basic everyday users seem to suffice.

Indeed, central in this work is the specific use of the devices that are engaged with and the criminogenic effects it has. If the elements of interpersonal crime lie in criminogenic situations motivated offenders, suitable targets, absence of capable guardians (Leukfeldt & Yar, 2016) – the smartphone strikes here as a guardian (with all its controlling and surveillance tools that we will discuss later), and yet representing the complete absenteeism of a capable guardian. It creates a covert environment where all criminality, deviance and harm may endure – in secret and only 'revealed' through 'leaks'.

Such an approach helps to identify the central elements of crime and criminality within the onlife scenario, especially the criminogenic situation (motivated offenders, suitable targets, absence of capable guardians) (Leukfeldt & Yar, 2016). Other theories

nonetheless help to understand and explain the shifts in everyday life patterns in creating offenders and finding targets and promoting ideal situations of crime. The Routine Activity Theory (RAT) well describes this phenomenon. Used by Cohen and Felson in 1979 to describe and explain the rise of criminality in the US during the 1960s, it was introduced by among others Majid Yar in conceptualising the elements of cybercriminality (Yar, 2005). The theory can be successfully used to define and understand elements of criminality such as phishing (Ghazi-Tehrani & Pontell, 2021) cyberbullying and cyber harassment (Kumar, et al., 2021). Some scholars argue that Routine Activity does not fully explain cybercrime activity (Vakhitova, et al., 2022), to the extent of developing further theories such as the Cyber-lifestyle-Routine Activities Theory, to criminological theories and converging the facets of the routine activity theory with the risks of victimisation (Guerra & Ingram, 2022).

When we look at the details of what cyber criminality means inside the onlife realm that this thesis tries to describe, recurring are the faucets of harming and damaging scenarios. Interpersonal forms of electronic surveillance & cover monitoring, cybercreeping, cyber stalking, bullying, revenge porn, and cyberassaults are all recurring elements that form the basis of a growing controversial reality. What is permitted, and to what we have 'given' permission loses its grasp in a virtual scenario. So much takes place without us knowing, at our backs (Forssell, 2016). Yet, it has a specific, enduring effect on us, both children and adults (Shariff, 2014). A wide range of harming and criminal scenarios unfold in an immense variety of situations, from technology, law, art, and finance. These develop through mainly the social-engineering practices of e-scamming, frauds and specific data attacks, as well as growing engagement with cryptocurrencies, deepfake and NFT & blockchain scams. However, this thesis is particularly concerned with the elements of interpersonal use and abuses of cyber-based systems. In particular, the elements of cyberstalking are significant, an "invasive form of partner monitoring" (Marcum, et al., 2017, p. 375) can take in apparent 'friendly' social environments, particularly aided by social networking platforms that become per se social surveillance websites (Tokunaga, 2011). While no longer talking in 'real life', users remain virtually and formally 'friends' and are thus observed and controlled, oftentimes unknowingly. Secrecy again appears a central aspect of both harm and proliferation. Such episodes take place on university campuses (Marcum, et al., 2017) as well as within internal communications of co-workers (Lowry, et al., 2016). It takes place globally and in an all-aged (Horst, 2020) and pluri-gendered reality (Burke Winkelman, et al., 2015). It also replicates on a multiplatform level, with shifting rules and regimes across devices and various apps offering both instant messaging as well as picture sharing (Srinivasan & IlamParithi, 2018). Stalking and bullying are particularly connected in this scenario, particularly for the insistence of offences. Such dynamics show evidence of "more psychosocial and emotional damage than traditional offline physical bullying because of the increased volume, scale, scope, and number of witnesses"(Gillespie 2009, cited in Lowry, et al. 2016:963)

Especially harmful and well-reported elements of this phenomenon is the public enduring of the data involved. This is particularly relevant in cases of revenge porn, which can be recognised as a recurring and "systemic violence" (Eikren & Ingram-

Waters, 2016). Such elements of technological-facilitated sexual violence and harassment take place jeopardising in many ways the de-facto intimacy that devices offer – HD filming and instant messaging combined with secretive and protective features. Such a scenario, alimented both by angry ex-partners and hackers, replicate elements of harm within a virtually infinite scenario where images may be released, shared and stored endlessly. This point, already raised by Ziccardi (2013) proves how there is no easy way out of any of these situations, and the difficulty is evident in forming some sort law of Revenge Porn (Eikren & Ingram-Waters, 2016) or cyber gender harassment (Citron, 2009).

Breaching of intimacy is indeed a recurring aspect of the onlife criminal scenario. Anything recorded in any onlife situation is perpetually at risk of being taken, raptured. Intimacy has in this perspective become deeply jeopardised. Such aspect becomes even more central when looking at the domestic spaces, and the surveillance and control they involve.

Surveillance in the intimate environment

Surveillance per se is an object of intimacy. It involves some sort of hidden space that allows listeners to hear, and observers to watch. Dynamics of surveillance as specific culture has been forwarded by Foucault end and recently discussed by David Lyon (2018). In their arguments, discussed elsewhere in this thesis, what is seen and controlled replicates elements social engineering, that, derived from military dynamics, replicate in the biopolical structure of modernity (Foucault, 1978); (Melossi, 2008). In this scenario, such military and hegemonistic dynamics replicate very well in the parental role over children and siblings (Livingstone, 2002). In families, the intimate lives of its members are very frequently, and very easily, under scrutiny (Nelson & Garey, 2009); (Steeves & Jones, 2010). However, the modern technologies and onlife scenario have rendered surveillance not only possible on a whole different level, but have increased its features, as well as its strategies of covert control/observation, as well as negotiation and resistance.

This central theme is very well discussed in the work of Caron Margareth Barron (2014), who shows the dynamics where the tools of surveillance, such as smart phones, become themselves tools to 'scramble' parental control. Children not only gain and earn devices with the 'excuse' of safety and 'emergency', but develop specific languages and elements of secret coding through texting as forms of 'escaping' surveillance (Kaufmann, 2021). This perspective of an alternative language is not limited to the smartphone, but has been related to SMS texting (Livingstone, 2002), and can be easily related much before that. Children, returning to Barron, are not "passive, powerless recipients of surveillance, rather they tell us of the forms of negotiation and resistance to monitoring after play spaces." (Barron, 2013, p. 411). But these instances nonetheless seem only marginal, considering the tools, both free and purchasable, digital and analogical tools, that parents can use to aliment their means of Suspicion, Control and Desire. Again, the remote aspect of these device is central: they can observe, control, "record, store, collate, relay and replay data' about their child indefinitely and with

practically infinite means (Rooney, 2010). Indeed, Rooney discusses the central point of trust and the lack of it, alimented by the indeed replete scenario of consumeristic tools available on the market. One that, as discussed the same year by Steeves and Marx (2010), creates a gold mine market of gadgets, baby monitoring tools, kits, and devices, out of a 'crisis of trust' within society. Indeed, this mistrust is not only limited to parents not trusting their own children, or the children of others– but is embedded into a specific culture of suspicion and fear (Furedi, 2019). This extends to other's parents, teachers, institutions, politicians, strangers, in fact, *any* 'other'. To track, monitor, and control appears as the only solution for a growingly mediated and scandal-seeking reality, another apparent feature of the online scenario. Also, a central aspect is that this form of control and surveillance, especially through the COVID-19 dynamics, is becoming ever more 'biological' in its scope and aim. It attempts to 'catch' under its gaze all aspects of those observed, again, especially within the intimate/domestic sphere – not only his or her whereabouts but the interaction, the contacts, the moods, and dynamics. Thanks to the normalisations of parental spyware apps (such as the much promoted Google Family Link), covert domestic CCTV installation and invasive testing, all this has become a recurring element of the onlife reality. The actual elements of surveillance and cybersurveillance within the home have common practices: both individuals, pets and appliances. Indeed, also rapidly common is the use and interaction with 'smart sensors' of all sorts, offering "smart thermostats, wireless smoke detectors, or home security systems" (Choe, et al., 2011). In this particular study, the concept of privacy proves itself already faltering (more than 10 years ago). The need for being 'away' from some gaze fundamentally are limited trivial and mostly innocent (or at least understandable) deviant behaviour to the eyes of others/strangers. Farts, nakedness, masturbation, or other more or less gross (but somewhat natural) conducts are all somewhat despicable outside an intimate scenario. However, this is what makes the intimate space so significant: its boundaries are set within the scope of the intimacy, and within the safety of its walls.

Another interesting experiment on this theme was based in Helsinki (2012). A combined study of researchers from Max Plank and Helsinki Institute of Technology analysed the intimacy dynamics as to actually understand the limits and boundaries of intimacy within a truly, Big Brother scenario(while this is a 10 years old project, the outcomes appear still very relevant). The survey was conducted by installing into willing citizens a series of anonymously controlled cameras with integrated microphones (Oulasvirta, et al., 2012). The results are particularly interesting for us for a number of reasons. It shows the dynamics and limits of surveillance acceptance within the home. In many ways, that particular study dismantles the sacrosanct idea that intimacy and privacy are related and unbreachable. In reality, while some of the respondents felt 'weird' and 'annoyance', and refused either to participate or dropped out after a short time, most of the participants, in exchange for a guarantee of anonymity (and a fee), went through with the project. The results show how indeed, though some friction is evident and has been reported, the surveillance did lead, in the long term, to acceptance and accustom. It represents the disinhibitions this thesis is thoroughly concerned with.

The tools, once again, prove their very strong effect in shaping society, and not vice versa.

From care to control

When we look at the dynamics of surveillance and monitoring in the intimate environment, the idea of Care connected to elements of surveillance is a recurring theme of this work and in criminology (Barron, 2013). David Lyon and Zygmunt Bauman approached the concept repeatedly in their 'dialogue' (2013), arguing of its features within a liquid environment. Lyon notes how "key problem with contemporary surveillance is its myopic focus on control, which quickly excludes any concern with care." (Bauman & Lyon, 2013, p. 37), to which Bauman does not unfortunately directly engage, though offering a plain definition of what can be in a word described as the onlife, as coined by Luciano Floridi (2015), whereas "Our life is split between two universes, 'online' and 'offline', and irreparably bicentred." (Bauman & Lyon, 2013, p. 37). In this scenario, children and parenting are indeed the primal concern of creating a blurring line within what is abusive and what in necessary within the elements of care and control. Within this apparently normative milieu of new technologies, our private space becoming normatively entrenched with smart solutions, that allow powerful means of control by and over users (see an insightful explicatory advice from Google on helping healthy digital families: (Google Inc, 2022).). We must come to terms with the hidden features and covert design these have now cheaply, if not freely, achieved through toys and smart-home devices (Steeves, 2020). The scholarly importance of these tools goes beyond the simple 'security' factor: they create completely new dynamics of control and observation over the domestic space and its members. The new values set by the Sars-COV-19 dynamics of family isolation and parental burden shed new light for the use and abuse of these devices (Gasser, et al., 2020). If we have accepted unthinkable conditions in a pre-pandemic mindset, to control and halt the coronavirus we can come across an acerbated set of new surveillance tools and dynamics. This has become the focus of David Lyon's last work (2022), as well as a series of articles and scholarly contributions that not only address the new forms of surveillance but modes and tools that allow so with hidden measures, covert analysis (New York Times, 2021), police authority abuse (dw.com, 2022) and a wide range of unconsented monitoring reports (Gasser, et al., 2020).

Today, as the 'remoteness' aspect of our lives seems to lighten, we are nevertheless facing the continuity of many abusive dynamics. Again, this seems to be particularly relevant to our youngest members of society. While students are returning to school for face-to-face, the surveillance dynamics that contributed to and were promoted with the smart-teaching apparatus seem to stay. This theme has come, ever and ever again, to some limited public attention, as on the Guardian (Mahdawi, 2022) and on Wired (Ceres, 2022). Student monitoring, covert recollection of data, viewing and hiding appear as a returning, recurring and yet inevitable aspect of our onlife reality.

In praise of the Medium

It would be certainly limiting, and strictly demagogical, to express concerns over the secretive use of instant mediums, without counter-arguing its most fundamental qualities. Central in this perspective is Michel Serres's definition of the Thumbelina figure, somewhat representative of the millennial aspect of society - recognizable within " a student, a patient, a worker, an employee, an administrator, a traveller, a voter, a senior, or an adolescent, or a whatever, a child, a consumer, in short, that anonymous person of the public arena that we sometimes call a "citizen"." (Serres, 2012, p. 61). The society Thumbelina lives in (addressed a decade ago already), is all in all compatible with Floridi's *onlife* reality: one where at the tip of a finger all members have infinite access to infinite information - on anyone and anything, "Whenever she wants it. In her hands. It is accessible, from any portal, via the web, from Wikipedia. It is explained, documented, and illustrated, with no errors that those found in the best encyclopaedias." (ibid, p.29). If this element is one of the core potentials of secretive conduct, Serres makes a convincing argument that indeed it is the cradle of a new form of knowledge, as revolutionary as writing and printing itself. Such revolution will be capable to rearrange social organisation, distribution of communication - forming a new human, fresh and dynamic compared to the crippled dinosaurs it preceded.

Serres's words are giving warning of danger, attracting attention to secrecy and potentially secretive conduct, but as we will see in the Theory chapter the final words are not yet spoken, alias the public and the social reality were found to be dislocated. Such injury received the most alarming treatment by various theorists, but it will be believed that, after so many alarming words, an ineradicable conviction had taken possession of people' minds that, however, we might try manipulating our surroundings, reality still endures.

1.1. Theoretical Framework

Research Thread

Culture is an aspect of cultivation (cultus- colere, Lat.): it grows and spreads though it requires a significant sense of civility and erudition to offer or propose a direction. Therefore 'conduct' is also essential, as a means to lead or transport towards a 'compromise' in society. As noted by Stephanie Kane "one need not always go places that obviously signify criminality to find crime [courts, jails, prisons]. One can find instead find crime suspended in or juxtaposed with relatively neutral occasions for social interactions" (2004:312). The culture surrounding such social interactions is central to this work, recognizing the hidden elements by noticing the trivial occurrence. What are

the criminal elements taking place in the background of our existences, and what is the culture surrounding it that allows it? With these perspectives in mind, I have attempted to pinpoint the elements of deviant conduct and the harmful effect that is embedded in our onlife culture. For such an approach, a new distinction between what is public and what is private was needed. Also, a clarification of the very dynamics that have become a habitus condition of our everyday interactions. The culture of crime becomes strictly embedded with the effect of this culture, and the harm it causes to users. Interestingly, being the golden thread of the two involves 'secrecy', most of its causes and effects, though very powerful and enduring, are yet to the most invisible. When sitting on a public bench, enjoying a lunch out with friends, going for a run, a walk, or a swim, we all – constantly connected to our smart devices – not only are observed, controlled, and monitored, but also locked in, out, and all over our existence. Thus, I have concentrated this analysis away from the social impulse for private, toward the impulse for the secret. A secretive realm is where 'cutting and splitting' among individuals and lives appears evident in everyday interaction: no wonder the word secret allegedly connects with the etymology of crime itself (lat. *secernere*) – meaning a 'spit, a separation', and ultimately, as Koselleck notices, a crisis *(Koselleck, 1988)*

So far, we have highlighted the principal theories recurring in the thesis. We will now indulge in analysing in detail the essential contributions they have offered in interpreting what could be defined as cultural criminology of the onlife secretive conduct,[5] starting again by Simmel and his main categories, which has special importance for our topic.

I. G. Simmel and the Perception of Boundaries:

Reciprocity

The fundamental contribution of Simmel in the thesis lies in his perception of the importance of secrecy in the everyday life manoeuvres and interaction, yet the evident fall-out into forms of abuse. Secrecy is per se an element of 'balance' in society, yet fundamentally implying conflict. It is integral and yet covert. Balance is meant in the case of reciprocity, where layers of intimacy and exposure take place regularly: friends share information or data in a reciprocal manner - any interruption, border, limit to the exchange is commonly recognised and respected. Again, this is central and healthy - just as, we will see, the blasé attitude is central in bearing the conflicts within the metropolis. Conflict indeed takes place when the unbalance becomes evident - secrets have been leaked, intimacies breached. More than that, as we will discuss in the vignettes, the secrets are breached, leaked, manipulated secretly: the conflict is subtler, or one-sided. If we are

[5] Consideration with use of Rene Girard and Marcell Mauss did not make the final version of the thesis, though their work is fundamentally fitting and recurring in various aspects – and at times incidentally referred to.

listing the concepts before their examination, maybe we are in a better position to bringing out their meaning, in order to integrate them into the thesis.

In his article on the 'Sociology of Secrecy and Secret Societies", published in 1906, Simmel begins with considering the interrelating aspects in the exchange of two or more interlocutors. For Simmel, right in the front page, a "customary reciprocal representation" (Simmel, 1906, p. 441) is essential, as well as citing in a sentence two words dear to both Mauss (reciprocity) and Goffman (representation). It is such a condition that sets the base of the distinction of what is known and what instead is veiled between two (or more) specific "pictures" (ibid, 443) in the mind of another, "of reciprocal relationships with that personal relationship" (ibidem). Also, we are required to conform to a specific "reciprocal knowledge of each other" (Simmel, 1906, p. 444), on which we must base our conduct, either revealing or dissimulating certain information. Modern man, according to Simmel, is particularly prone to this conduct, especially regarding lies: this is because of the economic-credit conditions of our civilizations, without which, Simmel goes as far as claiming: "modern life would be simply impossible". (ibid, p.446).

Lies

To take advantage of a lie and to differentiate the liar is fundamental to the role of secrecy dynamics, that oppose an ideal of "complete reciprocal transparency" (ibid, p.448), leading towards a fundamental dualism: "that is concord, harmony, mutuality, which count as the socializing forces proper, must be interrupted by distance, competition, repulsion, in order to produce the actual configuration of society" (ibidem). Such consideration, that would be in agreement with Girard's approach to mimetic rivalry, would lead towards a society "continually disturbed, unbalanced and detached by individualistic and irregular forces" (ibidem). In such conditions, reciprocal knowledge would nonetheless require necessarily a form of nescience, "a ratio, that is immensurable variable to be sure, of reciprocal concealment" (Simmel, 1906, p. 448).

Discretion

In such a reality, the two-exchanging information must define the dynamics of how far the information exchanged may go. Acquaintances, for example, become entities who agree to share in accordance with a specific "discretion" (ibid, p.452). They would set down specific social rules outside which "what is not forbidden is permitted, and what is not permitted is forbidden" (ibid, p.453). The distance between strangers itself is shaped in what may be intended as 'comfort zones', that mark the space which may not be penetrated or crossed without "disturbing the personal value of the individual" (ibidem). Simmel discusses here a concept very similar to the contemporary understanding of privacy, being the body intended as "our first property" (ibid, p.454). Its invasion and possession appear as a direct violation of the personality: the discretion would appear the "sense of justice with respect to the sphere of the intimate content of life" (ibidem).

Boundaries

The space between what is shared and what stored would be recurring aspect in the article of attaining and promoting "discretion of the other (ibid, p.455), defined as the "refraining from knowledge of everything which the other party does not voluntarily reveal to us" (ibidem). But our realities are characterized by a quite opposite aspect, where indeed "each knows something more about the other than the latter voluntarily reveals to him" (ibidem). Such condition, intended as indiscretion, may be exercised in modes that would result quite violent and morally unjustifiable, "as listening at keyholes or prying into the letters of strangers" (Simmel, 1906, p. 456). As obvious, two categories for Simmel appear particularly sensible in this matter: friendship and marriage. These two offer the most personal interpretations of what is an accepted discretion, especially because what binds the subject with the above-mentioned categories is the alternations of self-revelations opposed to a well-calibrated self-concealment, in respect and reserve of one another. It is instead in the absence of such reciprocal discretion that not only marriages and friendships become failures, but we can understand secrecy in real sense: that is, when a purposeful concealment and aggressive defence takes place, without respect of private property, nor an actual "right of secrecy" (ibid, p.462). In this perspective, the secret rather appears as a form of strategic anti-reciprocity tool: it underlines the means to secretive conduct, transforming the vantages of secrecy (mainly privacy) into a form of 'acting in the shadows'. Reciprocity is constantly required by the service (as when accepting cookies), yet by accepting it, reciprocity is breached. This is evident in the configuration of social networks as well: there we witness the user's need to share information in order to fully use the service, implying a specific 'informal' duty to share, and thus offering more and more information to the algorithms working in the background.

Indiscretion

Secrecy in the sense of indiscretion would allow and secure a "second world" (ibidem). The unbalanced ratio of secrecy would modify the nature of the relationship and specifically the attitude of the concealer. Such point appears extremely striking for this thesis, especially when we combine such 'second world' to the actual digital 'second world' that we may experience online, and more specifically, in the onlife existence. Simmel underlines that while there is a quantum of secrecy that may turn into abuse, "obstinacy and cynicism" (ibid, p.463), we must not "allow ourselves to be deceived by the manifold ethical negativeness of secrecy" (ibidem). Indeed, "secrecy is a universal sociological form[6], which, as such, has nothing to do with the moral valuations of its content" (ibidem).

Charm

The various instances where performers and performances (conductors and conducts) may aid and be aided by secrecy will be later noted also by Goffman, whereas everything

[6] A statement that appears perfectly compatible with Mauss's definition of a *Total Social Fact.*

secret gains a particular charm, becoming or appearing essential and significant. Moreover, this particular charm reaches its highest pitch at the moment a particular object disappears and thus reveals "the feeling of its value in its most intense degree" [7] (Simmel, 1906, p. 465). Its very "presence sets barriers between men" (ibid, p.466), but at the same time offers a "seductive temptation to break through the barrier by gossip or confession" (ibidem).

Concealment & Revelation

Such aspects, as Simmel underlines, are part of the individualistic nature of men, and appear based on their two primary interests: concealment and revelation. This contrast presents itself as the front (stage) and back (stage) intertwining, fostered by the above-mentioned secretive charm. These two are characterized by a "permanent in- and out-flow of content, in which what is originally open becomes secret, and what originally concealed throws off its mystery" (ibid, p.467). This idea, though apparently paradoxical, is not only perfectly compatible with our contemporary on- and off- existences[8], but underlines the requirement in human associations for a definite "ratio of secrecy" (ibidem), whereas the publicity of one is in strict correlation with his becoming more and more secretive.[9] We see here how the arguments of Simmel are extremely contemporary, by comparing the characteristics of the transparent democracy with the inevitable secretiveness of their offices, whereas "politics, administration, Justice, have lost their secrecy and inaccessibility in precisely the degree in which the individual has gained the possibility of a more complete privacy" (Simmel, 1906, p. 469). Such complete privacy would have been promoted by the "crowded conditions of great cities" whereas modern life would have "elaborated a technique for the affairs of the individuals" (ibidem).

Privacy and Mental Life

This mental condition is a key theme in another central work of Simmel, the earlier article The Metropolis and Mental Life (1903). There, Simmel recollects the duality (yet another recurring word of this thesis) of internal and external stimuli created by the very metropolitan life, that come to tackle the very " sensory foundations of mental life" (Simmel, 1971, p. 325): against the domination of the metropolis, a protection is needed, a specific barrier: Simmel calls it the blasé attitude, a sort of indifference [10] to all the "rapidly shifting stimulations" (ibid, p.325), that may form a 'protective shell'- protecting the most sensible aspect of personality, the emotional inner [secret] life. It is a response, an adjustment of sorts to prevent the otherwise "inevitable dragging the personality downward into a feeling of its own valuelessness" (ibid, p.330). The blasé attitude would appear thus as a specific "social conduct" (ibid, p.331): a mental attitude towards people requiring a necessary 'reserve'. Suspicion towards the other - too common, tempting and devastating in the everyday metropolitan life to resist from - finds thus release in "mutual

[7] A point that becomes, other than in Goffman, even more significant later discussing the desiring triangle of Girard and the notion of rivalry.
[8] Just as in Bauman's *Liquidity* concept discussed in the literary review.
[9] An argument that will be central and further analysed regarding social media.
[10] Using Foucault's later definition.

strangeness and repulsion" (ibidem). Without this conduct, Simmel considered that hatred and conflict would be inevitable: dullness is necessary, and indeed central in the modern mentality: it is the 'padding the bunker' attitude to for discretion and autonomy in controlling the 'ratio of secrecy', between the public (front-stage) and the private (back-stage). Such dullness appears essential in explaining the basic condition of this thesis's secretive conduct, where too much available information about ourselves becomes contraposed with the refrain, concealment, sheltering and protection of one's self. Also, such dullness we may also interpret as a form of resignation (as every time we 'accept' cookies or the browsers saving of our passwords - thus underlying also the harvesting of our data) not to be entirely taken over by the very anxiety onlife media produces. The secretive-blasé attitude is specific of the secretive conduct, as discussed more in detail later. Its condition would appear as an indifference to the secrets of others (as the protection of smart devices and private life), but also the mental attitude of developing secrets and reserve on a regular basis, both online and offline.

Masks

Central also, in Simmel's final note, is the role of the mask in "drawing lines of separation" (ibid, p.485) between certain orders and the natures of peoples: specific disguises become necessary, either to promote oneself (as in the case of profile pictures) or to actually obscure (obfuscate) the whole person. Again, the centrality of the issue lies in a duality, characterized by the masking 'inclusion' and 'exclusion' of its members and 'users', who may be integrated in the masking ritual and its influence. Social media, again, is an evident Simmelian parallel, in its pretence, through its public and thus visible material, to "include all man, and thus representing humanity as a whole" (ibid. p.491). Yet, the masking and protecting nature would appear to prevail, especially in the risk, and evident collision/rivalry in the case of suspicion of betrayal, as in the case of participating simultaneously to different secret societies/social media (groups or services). Conspiracy and suspicion become thus Simmel's final remarks on the matter, as whatever is hidden is a direct competitor of what is open, even if only perceived as such: especially the suspicion that secrecy conceals danger.

Society of secrets

We have seen that the concern of Simmel, outstandingly contemporary today, is one of the central influence of secrecy in the everyday: it is a tool to hide as to protect one's life (a form of mental barrier) for security and well-being, but also a malicious tool of abuse-from protection to subjugation. Secrecy is a tempting approach and medium (indeed medium is the next theme discussed): it is also a form of power to create and yet sub-due power structures, as noticed in the structure of the secret societies. We have noticed some parallels with social media, whereas the creation of identity of the user, display of his activities and his interests - is produced with a pretence of publicness, yet pursuing schemes and working rather in the background. Such approach is further alimented and promoted by the platform structure itself, where the social media itself allows the users to express themselves private and publicly, collecting all material either way for third party

purposes[11] (a condition that is reconcilable both with John Wilkes testimony to the authorities of his Hell Fire Club meetings (Lord, 2008) than to Cambridge Analytica's scandal (Ziccardi, 2015)). We see how secrecy is a double-coiled sword: it allows freedom and protection but at the same time implies control and surveillance. Moreover, often times such control and surveillance is taking place with the same conditions that they protect from: freedom and protection in secret to control and surveille *freely* and in *secret*.

We have concentrated on some of Simmel's concepts that occurred in various writings, like mask, society of secrets, privacy and mental life, and integrated them with the onlife experience. Simmel came to the conclusion that there had been some sort of a dual action of the mind, which might lead to a catastrophe or a discovery of secret plans; which is not exactly my point. The blurring line between secrecy and publicness is rather central: The ecology described by Simmel integrated with secrecy- dinamics are part of a human interaction – though the abuse of the ratio of secrecy is, in this thesis, underlines as a fundamental elements of the onlife scenario.

II. M. Foucault's Discourse on Conduct.

So far, we have seen how various modalities of interaction may arouse, promote and increase Suspicion, Control and Desire through technology and a secretive social conduct. In this section the focus will be on the central figure of this discussion, Michel Foucault (1926-1984). Foucault is widely known for his genealogical analyses of Madness (1961), Crime (1975) and Sexuality (1976-1984), but also for his lectures on power-knowledge relations, the nature of theodicy and the care of the self.
The centrality of his work lies in his 'perception' of the panoptic reality surrounding our modern environment – the elements of the *onlife* ecology and the instances in which smart device related social harm takes place. To see, observe and control – with particular focus on the idea of power – is central in this work. However, Foucault has offered also other central interpretations, that are also highly influential in understanding and theorizing the elements of secretive conduct – and in general the secrets surrounding the *onlife* environment. This includes novel considerations over elements of discipline & docility, but also the nature of confession and control – which will now be analysed.

Confession/avowal mechanism

According to the complex analysis of Foucault, control may be related to a form of secretive conduct finding genealogical roots in the recollection of what is confessed, thus forming an evident dichotomy between what is public and what is stored away. In the

[11] Elements of such 'surveillance' is noticeable also in the spying schemes the London Clubs, as with the figure of John Wilkes (see (Sennett, 1974), (Lord, 2008))

History of Sexuality, he emphasises how the obligation to confess is deeply integrated into us. Truth 'demands' to grow out of ourselves, the core of secret truths cannot be held back. He defines confession in the Christian West as "the first technique for producing the truth" (Foucault, 1978, p. 68), specifically concerning the truth about sex. According to Foucault, confession would have a history in many respects similar to that of disciplinary techniques: like the disciplines, it would have been born in the religious sphere, would have reached its maximum moment of development during the Middle Ages and would have spread to other fields of society, establishing itself "as one of the main rituals we rely on for the production of truth". (Foucault, 1978, p. 54)
Nonetheless, "Confession frees, but power reduces one to silence; truth does not belong to the order of power" (Foucault, 1978, p. 60). The ritual of confession was a cathartic and clerical establishment, with an "effacement of the thing said by the its very utterance" (Foucault, 1979, p. 84). Since the end of the seventeenth century, such institution was later overtaken by a "recording mechanism" (ibidem), replacing the one of pardoning: such antique and vicarious procedure would thus be localized, registered, forming and gathering "into dossiers and archives" (ibidem). Elements of such constant demand of speaking about the self are 'self'-evident on contemporary social platforms, with the peculiar 'twist' of being also these systems designed to register, promote and gather all the information/data produced- without allowing an 'easy-way-out' to have these disappear as securely deleted from all servers.

Panoptic power

This appears as the beginning of what Foucault would come to define a Panoptic power-system. If the recording of confessions would constitute, "through time, a sort of constantly growing record of all the world's woes" (Foucault, 1979, p. 84), the perpetual watching becomes necessary not only to extrapolate what is committed and later confessed, but to monitor and prevent what is about to happen – or might be committed.

Such an all-watchful metaphor derives, as stated by Foucault himself, from the rational and strictly utilitarian architectural model of Jeremy Bentham: a perfect structure for channelling power and observation over individuals. Indeed, such model has ultimately become the prison model by antonomasia: the perfect controlling device over the condemned. Central in this concept is connecting Foucault's automatism of power: the prisoners behave and convince the others to behave accordingly; anybody, actually, may render the mechanism functioning. The ultimate aim is just the same: mould bodies, lead them to constant transformation and manipulation, towards an idea of constant and functioning 'docility'. By constant observation, or rather the threat of this very observation, the conduct of the watched would be controlled, and ultimately rendered, according to the perspective of Foucault, 'disciplined' (Foucault, 1975). It does not matter if there isn't actually anybody watching: the effect is just the same. The object of control is in being both visible and yet unverifiable. This concept is helpful for describing the 'fishy'/elusive/latent functioning of smart devices, from smartphones design to Smart Home products, even surveillance devices themselves: offering services while at the same time being constantly 'on alert', thus collection information/data and the automation of surveillance (Melossi, 2008) with a datatification ecology involving data gathering and

mining devices as the home assistant Google Nest (Google.Support, 2020), Alexa or even Amazon Ring (Redden, et al., 2020).

Discipline and docility

For Foucault, such a system has become integral in our society, leaking out of the walls of the Benthamian architectural 'prison'. The model has generalized its functioning, is "a way of defining power relations in terms of the everyday life of men" (Foucault, 1975, p.205). Its scheme may be represented and "implemented in hospitals, workshops, schools, prisons" (ibid, p.205). But, whatever its application, the significance is in its efficacy and efficiency is "to perfect the exercise of power" (Ibid, 206). Discipline thus becomes the mechanism that penetrates and observes (and absorbs) all fields: power must become formed by a "permanent, exhaustive, omnipresent surveillance, capable of making all visible, as long as it could itself remain invisible." (ibid, p.214) Even more impressive regarding the contemporary is the later consideration of a "thousands of eyes posted everywhere, mobile attentions ever on the alert, a long, hierarchized network" (p.214) that seem, again, to underline the ever-present surrounding of smart devices in our everyday life, especially with their filming and recording functions - with ever greater quality and precision: a system, as we shall see in Part 2, that promotes a 'Harriet the Spy' (1964) condition of constant watch and surveillance, as described in the children tale. This condition, though used as a democratising and trust-oriented pretext in the conception of Synopticon (Mathiesen, 1997) – on other words a transparent environment/ecology of constant exchange - appears today rather dubious (a point picked up also in (Han, 2012)): instead, using Foucault, such reality has not only pervaded in all of society, but appears to underline the users 'docility' to these panoptic onlife ecology: we know we are watched but (for the most part) appear blasé to its functions. Moreover, we are actually blasé in filming ourselves and others, producing and consuming incessantly material - sharing, viewing, commenting- being shared, viewed and commented- just as in Bentham's panoptic guardians withing a total institution.

On a more technical analysis of the tools and machines that allow this very control, we may notice the discussions different variations of the Foucaldian power structure, with various highly relevant variations of the 'watchful structure' inside the modern environment. There are many lists to be consulted: one significant for Lyon mentions Dieder Bigo's considerations on the Ban-Opticon in controlling and influencing migration trends (Bigo, 2008); Loic Wacquant's Social Panopticism (Wacquant, 2001) analysing the policing functions of welfare services. But for a more up-to-date consideration, we may find striking answers in the analysis of Siva Vaidhyanathan and his Cryptopticon (first used in 2011), that underlines the "cryptic, hidden, scrambled and mysterious" (Vaidhyanathan, 2018, p. 67) workings of social media, ultimately linked with Big Tech companies and state surveillance, managing and recollecting users' data. Even the magazine The Economist offered recently a pandemic-concerned take on the Coronopticon (The Economist, 2020), considering the effect and influence of contact-tracing apps and citizens' health monitoring.

Panta-opticons

The All-Seeing-Place becomes an actual 'space', where everything is watched, judged, contained and controlled: as an update to Foucault's and Bentham's considerations, the contemporary Eye is not only electronic and recently 'Artificially Intelligent', but also, remote, never forgetting, invisible and ever-growing: owned and controlled by corporations as well as government. This is evident, as shown, with the online and offline consumption of surveillance, the use of satellites, drones, but also marketing algorithms, GPS tracking, and consumer triangulation. In addition to this, the technology today easily allows the citizen to himself control and personalize his information, and to control, with a basic IT knowledge, the information of others. Such approach understood as an 'opaque technology' *(Lyon, 2020)*- that recollects and accesses information with "people barely understanding the opaque systems surrounding them". In this environment, the effects of a liquid state of permanent secrecy become evident: a specific system where the more visibility is achieved, the more secrecy is required. Such is the current ecology of a panoptic environmental complete control (Lyon, 2018).

Sexuality as discourse

Foucault's theoretical centrality to the keeping secrets/protecting data can be found interpreting his 'History of Sexuality, Vol.1', where Foucault focuses once more his considerations on the seventeenth century. There, he argues against the idea that secrecy and secretive conduct regarding 'sex' was a Victorian bourgeois imposition and repression, with the aid of a "simple imposition of silence" (Foucault, 1978, p.27). While indeed apparently silence, taboo and nonexistence filled the vocabulary of what was perhaps once blatant, visible and obviously natural, such restriction over sexual discourse had lead towards a "mechanism of increasing incitement" (ibid, p.12).

Rather than saying less about it, Foucault notices the different ways in which sex was formulated, with specific ways of "not saying such things" (ibid, p.27), though apparently implying them, with strategies and gestures "that underlie and permeate the discourse" (ibidem). Sexuality thus became more secret, and its discourse and conduct secretive, though as effective and popular as ever. It became a central theme of discourse, always at the mouth but never specifically mentioned. Its content taboo yet its 'act' obvious: because of this is it deeply rooted, it appears, with secrecy.

This argument can find striking similarities with today's requirement and reminder to protect our passwords and changing them regularly, with ever more sophisticated formulas, codes and technologies. Visiting any website incites to the duty in corporation' respecting of privacy- underlying the users also exchange of such respect. The argument of our secrets/data and their value is constantly incited yet underlid: the effect constantly promoting the respect and protection of one's space (from hackers and dangers), though undermining the constant breaching of that very space (for marking purposes and 'improvement' of service), though with 'consent' and 'awareness'. Moreover, Foucault noticed since the Age of Reason a "regulated and polymorphous incitement to discourse" (ibid, p.34) of sex, with a "wide dispersion of devices that were invented for speaking about it, for having it spoken about, for inducing it to speak for

itself, for listening, for recording, transcribing, and redistributing what it is said about it." (ibidem). Such a quote reckons an astonishing resemblance not only the basic data collection bits of websites, but the very functionality of smartphones. Also, striking parallels may be drawn with the discourse of privacy and secrecy around the use, and the very nature, of such smart devices. This aspect for Foucault is peculiar to modern societies, having exploited, similarly to sex, the discourse of secret "ad infinitum, while exploiting it as the secret" (ibid, p35).

Sex-excitement

Indeed, regarding sex, working of the smartphone, that will be discussed in detail in Part 2, show the sexual-incitement powerful structure that the smartphones allow and produce. Sexual content is potentially perpetually 'looked up', viewed, and consumed-through websites, apps, sex-work services and chats. But it is also perpetually producible, shared and promoted and incited through apps. Sex thus, fundamental theme sidelined-censored 'apparently' from public discourse, is rather through smart mediums always at hand. Owning the chronology of the porn sites consultation, searches, views; the recollection of images potentially taken and shared among lovers and friends; the record of calls list and messages- the smartphone becomes the always at hand producer of 'secrets' (personal, private, intimate, and even 'deviant' as ones of paraphilia's and infidelity). Such content becomes the principal object of 'locking up' functions of our devices- rendering ever personal, private- single used and always at hand- yet being always promoted as tools in need of updates and new technologies as to avoid being breached, stole and hacked. The secret-producing tool becomes an object of constant incitement and perennial sense of danger underlying the servo-mechanical requirement of their function.

Secretive conduct

The conduct of secrecy appears thus perpetually promoted and at the same time constantly questioned: such aspect becomes central for our thesis regarding the understanding of governmentality, or the biopolitics of control over conduct (conducting conduct) as discussed in Foucault's lectures at the College de France (1978). Such governmentality (or the conduct of one-self) would allow forms of social control in disciplinary institutions, a term also dear to Goffman relating to Total Institutions (Goffman, 1961), thus englobing systems that would involve the individualization, classification, ordering and control – without possibility to step-out. The conduct is thus a complex 'action' for Foucault, something that is yet governed, but at the same time may lead (conduct) towards or influence the conduct of others. It involves a power, as opposed to a form of resistance, and at the same time a secretive conduct, that is not simply a disobedience, but rather a "sense of struggle against the process implemented for conducting others" (Foucault, 1978, p. 201).

In this work, central is the concept of a seduction to a certain conduct – to induce, seduce and thus conduce the elements of secretiveness, refrain, convert behaviour. The smartphone is the central medium that 'leads' such way of being – it is a conduit to this

specific secretive conduct: it aids and promotes its conditions. Such are the variations of the onlife ecology, to which the discourse of privacy seems pervasive, yet undermining the true secretive elements that constitute its conditions. How privacy is raved about – by users, governments and corporation – while undermining the evident effect of all this discourse, represents partly how secretive conduct is becoming itself pervasive.

III. E. Goffman and the Management of Impressions

Turning to Goffman, the sociologist contribution to the relation of everyday interactions is - though more than 60 years old - exemplary. The interaction between individuals, his/her roles and 'performances' are essential aspects to understanding what indeed do we express, what do we refrain from, in other words how we conduct secretive behaviour. Nevertheless, as it is evident, Goffman was surrounded by very few of today's technologies - least of all the internet - or the onlife reality for that matter, yet it is important to engage with his interpretation of everyday life. We will thus engage in his most fundamental consideration, trying to interpret his thought with the modern ecology - indeed, with the onlife ecology.

The works of the Canadian author are milestones in the post-war sociology and ethnography, concentrated on the aspect of Interaction and Representation (1959, 1961, 1963, 1967, 1982); Institutionalization (1961) and Stigma (1963). Of these arguments, I will fundamentally base my theory on the presentation of the subject, and his alternation between front and backstage: such area or region is central for Goffman in the formation and performance of roles. The social control that will be analyses lies in the necessity of controlling such stage/region. Such section will be entitled and referred to as 'impressions', as its the influence of such impressions towards others that the subject may control or be controlled by his very impressions.

In Goffman's interpretation, our everyday life is characterized by a performance, just as in theatre: of such performance, its "principles derived are dramaturgical ones (Goffman, 1959, p.9). Specific "boundaries" (ibid. p.109) are respected by the individual (also a performer), in respect of two fundamentally different environments where to present and expose oneself: the 'frontstage' and the 'backstage.'

The Front stage is central for the observation of one's performances and presentations of self by others, it is the "setting" (ibid, p.32) which supplies "the scenery and stage props for the spate of human action played out before, within, or upon it" (ibid, p.32-33). The setting is particularly important for presenting oneself in a favourable light, and thus a central aspect of concepts of manipulations and self-interest (ibid, p.18). Concealment appears as the medium and boundary that connects yet separates the two: a question of hiding what we do not show in the front region. Because of this, Goffman shows how the individual tends to control behaviour and communication to offer an information game of a "potentially infinite cycle of concealment, discovery, false revelation and rediscovery" (ibid. p.20).

When the performer nonetheless is particularly insincere in his revealing the nature of performance (an argument I will later discuss using the reciprocity triangle) he is defined by Goffman as a "cynical performer" (ibid, p.21): a (sadly) universal example of this are politicians, who during political campaigns publicly profess to be sincerely interested in addressing some social issue, while, in strict cynical terms, not really caring about the issue. We see in such a position (that one can see in a fantastic performance in the third and fourth season of the Wire) with the frontstage performance to the public for electoral purposes and the backstage actions behind the scene that are carefully hidden. A more specific example is evident in the frontstage declarations of Zuckerberg while testifying to the Congress during the Data Gate scandal, addressing concern about the problem of fake news, toxic web and hate speech, guaranteeing he's taking measures to limit it. Nonetheless, it has been revealed that in the 'backstage' of such declarations Zuckerberg himself, along with Peter Theil have met in different occasions with Trump, even recently (Smith, 2020). In all of these controversial situations, whenever the polito-economy 'tricks' are questioned, cynical performers may always change the game, even at his defense, assuming the mask of being nevertheless the champion of 'free expression', against censorship and bias. (Paul, 2019)

But returning to Goffman, cynicism may also become a means of isolation of real intention and "insulating their inner selves from contact with audience" (ibid, p. 31). Performers would then tend to "conceal or underplay those activities, facts, and motives which are incompatible with an idealized version of himself and his products (p.56). He may also change parts he plays depending on the very setting he is performing in, giving practically a definition of mask use and interchange, a point that will be brought up by Alessandro Pizzorno and discussed in the literary review.

Returning to performance: Goffman notices a clear distinction between concealment used and performed in the form of a simple "white lie" (p.69) (as in the case of the doctor prescribing placebo), as opposed to creating "intentionally also any king of false impression without putting himself in the indefensible position of having told a clear-cut lie" (ibidem). The mass media communication technique became for Goffman a central tool for disguising or profiting from lies (as it will be discussed in the later argument of influencers falsifying influence). In this light, Goffman notices that the audience themselves may find awe in concealment of the performer himself, sensing "secret mysteries and power behind the performance, and the performer sense that his chief secrets are petty ones" (p.76).

As discussed in the introduction, also Goffman underlines how often "the real secret behind the mystery is that there is no mystery (p.76)- as long as the audience does not know as such (or pretends to do so[12]). The front thus for Goffman appears as a space for stage acting. Though it is too simplistic (or rather poetic) to claim 'All Worlds a Stage',

[12] example can be given by the weak shamanic performance witnessed among the Inuit (1921-1924) by Knud Rasmussen: though the unsuccessful specific ritual (a 'rapture' by the spirit of a bear) appeared to the Danish explorer evident, the audience of the shaman's tribe were nevertheless transported and convinced: they dare not to question the authenticity of the magic: rather, it is the Gods not in mood to participate.

"the ways in which it isn't are not easy to specify" (p.78) The connection with Foucault appears evident in the role of such performances and dramatic dimensions, that are a strategically cultivated conduct: the impressions are for Goffman specifically managed, acted and performed. For Foucault instead, the centrality lies in the specific 'conducting of conduct', especially in the condition of what is visible and what invisible. People, in other words, are bound to become into being secretive - to the extent, as we will see, of being disciplined into it. The theatricality, central also in the work of Sennett, is fundamental in the formula of Suspicion, Control and Desire: one may pretend, wearing a mask, to act somehow, while demanding else. One may act as friend, while being cynically manipulative and requiring control over the other. Also, the Desire factor becomes central in the 'want' that hiding generates, especially returning to Mike Davis' idea of 'padding the bunker' (Davis, 1990) – in specific the condition of sheltering oneself ever more in locked, secured and protected environments. Indeed, the requirement for more secrecy is apparently addictive: it demands to increase and requires so just as well. We will see in the case studies how thanks to the contemporary mediums, and in particular smartphones, individuals can 'play' roles of being a loving and faithful companion, while contemporary having their lover constantly reachable on chats, and always at hand: even while having their companion present. On this note, we may continue our analysis by observing the influence of the backstage over the frontstage.

The backstage (or region) may be the essential aspect to justify this condition: it is there that the "impression fostered by the performance is knowingly contradicted as a matter of course (p.114): In the backstage, the performance is "cut off" (p.115), offering an interruption and "brief periods of relaxation"[13]. The audience has no access to the backstage: there, "vital secrets of a show are visible [and] performers behave out of character" (116). It appears as the 'safe place', where workers in a factory may take a rest, bad elements from a mental hospital may be restricted during visits, or mechanics may get 'dirty' while customers wait in the shop. The backstage is thus the region where to store 'secrets', not to be shared with the audience, but may also allow, or become conducted, towards 'discrepant roles'. Goffman separates four types of secrets that may be presented and witnessed in the everyday life, interpreted by the candidate as:

a. strategic, as in armies or businesses or sorts
b. 'inside' secrets, as in societies of sorts- secrets societies in particular
c. entrusted secrets, where they are kept, among others, for others.
d. free secrets, where everyone has the object of information shared, but not the subject.

While a&b result in personal secrets, c&d regard others, with performance being central as much as the action of pretence: the discrepancy lies in the secretive performance that may access/invade the backstage, how such action affects the various roles of performer and audience. These invaders are represented by:

i. the informer, that may be interpreted as the equivalent of a whistle-blower;

[13] it will be elsewhere proposed by the candidate that this is no longer the case: the backstage follows us everywhere, may be accessed always, and just as such always invaded

ii. the shill, mainly a hypocrite figure, who may be witnessed is the equivalent of a social media group sharing and even trolling others by "provid[ing] a visible model for the audience of the kind of response the performers are seeking" (p.145-146)
iii. the shopper, described as the person having "technical right to see the show but ought to have the decency [...] to stay in his own back region" (p.148)
iv. finally the go-between, who knows the secret and shares it with the team: he is a mediator, yet a chosen one, at least apparently.

We realise how all these roles indeed appear part of the individuals/subject's agency, a voluntary, if not necessary role to whom disclose backstage secrets, in exchange of a certain utility, advice, help of sorts. Not so clear instead is the more extreme role described finally by Goffman as the "non-person" (p.150): these can be recognized as subjects and, potentially, objects. In the case of subjects, the non-person appears evident in the creation of social media and networking profiles: there, through the developing, building and forging of an ideal-fake personality (Turkle, 2010). This, as we shall see, is true both in more friend-based platforms, such as Tik Tok or Facebook/Meta - or work-related profile managers as LinkedIn (Boland & Griffin, 2015). While it can be argued that indeed all social media are based on self-promotion and impression management, (amazingly anachronistic beware of this can be found online (Peters, 2008)) the result appears indeed in creating a form a 'non-person subject': one that conducts both a public existence and a secretive alternative (both digital and IRL) that he must control and keep separated. Yet, the constant access and exit of the backstage, along with the unrevealing and discovery of other 'backstages' creates a condition that already in Turkle's case studies of the early social networking use of Myspace resulted in creating 'high anxiety' (Turkle, 2010, p. 241) among young user. We will see more of this later in illustrating this point.

As we have seen, the performance factor is a central element of secretive conduct today: on the one hand, we see the cynical performer who makes the most use of his 'public' and 'private' powers to apply the formula of 'Suspicion, Control and Desire', on the other, it relies in the form of impression management, where unrequired characteristic may be 'hidden' to the 'public', and indeed covered in the backstage. This condition is one of 'releasing the pressure' of the public, thus owning a precious space where to 'take the mask off' and be 'yourself'. Yet, an evident condition arises where, for the common user-citizen, there appears to be no specific 'safe place' to store this 'hidden' information- and put away the mask. While the online public profile may promote an idyllic image of you, both carrier-wise and to friends (and followers), the danger of constantly having information 'leaked' is permanent. Not only, the potential of creating false profiles/identities (non-person subjects) creates, as we will see in the case studies, episodes of constant suspicion, anxiety, uncertainty about our surroundings. The smart devices central in alimenting such condition, being the quintessential non-person object who may enter our 'backstage' while present in the 'frontstage': also, it is fundamentally the tool with which the front is recorded and the same tool that stores it in the back. Its various functions, potentials and dangers will be analysed in Part 3.

Total institutions

We may consider another fundamental theory of the Canadian author, represented in his recollected essays 'Asylums' (1961). Here, Goffman described in detail the differentiation and characteristics of what he describes as total or encompassing social arrangements, whereas their "character is symbolized by the barrier to social intercourse with the outside" (Goffman, 1961, p. 16): these barriers appear as physical, as in the case of actual places of encounter, or social and digital in the case of online interaction. In such light, while Goffman concentrated on the role, dynamics and involvement of mental patients in asylum and the members of staff, we may see fundamental parallels in the encompassing characteristics of smart devices, and the very platforms that they allow access to.

Such argument will be further analysed in the social vignettes, and the specific role of smartphones and smart-surveillance technology in altering and yet influencing our conduct in the everyday life in a total or encompassing manner. Even the medium as proposed by McLuhan becomes central in defining the non-person and yet the power to not only enter and exit the front and backstage, but monitor and record it, proving what goes on back and forth, constantly at hand and perpetually in memory. The go-between, as we will later see, becomes the essential action of the tool but also the condition of counter-conduct of the performer.

Theorizing the criminological ecology of the Onlife

With the aid of these core authors, we have tried to underline the theoretical baseline that characterizes the ecology of onlife and the question of secrecy in the everyday life: though all from the past century and living an age 'all in all' different from ours, especially for the absolute lack of internet, their impressions and considerations may find fundamental parallels in the contemporary condition.

The contribution of these three principal authors (Foucault, Goffman and Simmel) is essential for outlining the means in which secrecy emerges: is stored, manipulated, and controlled in the contemporary society. Secrecy is indeed a central element: not only for the everyday life interactions (as a first read of Goffman and Simmel implies), but for the modes in which it promotes, entitles and propagates panoptic means (Will to know) and the docility that it implies. While the modalities of this panoptic reality and the docile conformity are central themes across the following chapters, I will offer now a brief recollection. For panopticism in Foucauldian terms, related to secretive conduct, this work recognized the modes in which the society we live in is constantly under watch - with our secret conduct in its central scrutiny. In the modern conception of the panoptic gaze (Lyon, 2018) we have witnessed the evolution of visual-sensory surveillance and digital-algorithmic analysis, with not a simple observation of the 'public' life - what is done, so to say - under the eyes (form organic to the technical)- with specific elements of

recording, recollecting, analysing. In this perspective, the panopticon has entered all realms – any space. The empowerment of the data control has lost its value: even the concept of data in being today overwhelmed by even more silent, secret, and hidden elements of 'raw data' analysis within our phones.
Instead, by using such phones, by delivering such data out in the open, we witness new and endless elements of confession, distribution, and proliferation: either willingly or unknowingly. These elements leak into and out the stages of our onlife existence: front and back.

Such prospect of ever-observation seems paradoxically opposite to the 'protecting' conditions promoted by corporations and state agencies over consumer and citizens 'privacy': codes, locks, pins, all apparently are developed (and enforced) to protect 'data' - but, as this thesis claims - fundamentally promote evermore conditions of creating further and further raw analysing-worth material- data-hungry systems. The docility in these terms becomes the fundamental discourse over secrets - protecting secrets, harvesting and consolidating them - only to further generate and promote their use and condition.

This conduct, another Foucauldian term, becomes essential in understanding the ways to not simply 'perform' - as Goffman intended - terms of engagement with one and another despite his/her secrets - but leading parallel lives, engaging in public though producing in private - being 'here' while being 'there'. All these elements, as we will see, become integral with the use of mediums, specifically 'smart-medium'- come to represent the quintessential tool to promote and conduce with the very secretive conduct this thesis is outlining. Smart devices, as we will describe in part 2, offer endless prospects of entering and exiting those boundaries that for Goffman represented somewhat of a threshold between public and private lives - the curtain behind which the audience could not access, and the actors could - ideally- rest. Of course, this is a reduction in his analysis, nonetheless today, especially in the smartphone induced reality - such distinction is no longer attainable. It does not stand. Rather, this work had to come to terms with a different interpretation, that found a founding interpretation in Floridi's concept of the onlife (2015) - thus a blurring threshold between the online and offline existence - no longer divisible nor (easily) evadable. The smartphone appears as essential tool of the onlife existence: fully functioning and necessary tool both while 'connected' or in 'airplane mode' - capable of filming, recording inconspicuously- chatting, engaging and searching without drawing attention, rather, becoming a normative element of all instances of secretive conduct: producing data and constantly storing it, hiding it - only to shared it, publish it, leak it perpetually on platforms and other media.

It is in recollecting these considerations that such normative aspect became under scrutiny and lead to the 'deviant' perspective of this work, whereas the normative aspect of filming, monitoring and storing appeared a somewhat hazardous to the essential aspect of conviviality within society. And truly, while witnessing and considering various forms of engagement a further level of 'conduct' appeared worth considering, becoming central in part 3 of this work, the secretive conduct related to secret production, monitoring and

promotion. It is in this analysis that we come across the suspicion, control and desire elements of deviants that emerge within such a milieu of secrecy - somewhat hinted in the works of these authors- and now appearing as central and entrapping as ever. The specifics of harm become a central question that this thesis will engage with. How such a condition is pervasive, and the effect is difficult to recognize, is a central enquiry that perhaps is still open to answers.

1.2. Methodology

Epistemological dilemma

A central dilemma is posed by the nature of this work is the standard method in which generally data is gathered – and indeed any reader to this point would read the word 'data' with a certain hesitance – being how the word 'data' has become, in accordance to this work, almost a hyperbole of something else – i.e. not given, but taken. Data thus is a central element of criticism within this work: the influence of this data on use, the manoeuvres and conditions, and the social harm involved in gathering, monitoring, filming and recording users, especially when there is no awareness nor consent taking place. Such consideration required an alternative 'tool' to study indeed the 'tools' surrounding us.

Many variations have been personally attempted to deliver a study on contemporary secrecy, from a plain (whist overly complex) genealogy of secrecy in society and the harm involved – to an ever polished and focused (and eventually final) analysis of the characteristics of secrecy in the contemporary environment, focused on the technological variations and criminological implications. My approach was one of making use of regular first-hand eyewitness accounts and observations. That offers advantages such as revealing certain mood of the onlife I was trying to understand, and secretive conditions that characterise it. Also, my approach uncovered some interesting details and rendered conditions that were apparently obvious and trivial at time critically observed by the viewer and the viewed. The method finally arrived at and delivered is perceived in no way infallible: it is, as all qualitative analysis, open to interpretation, reflections and debate. It is, nonetheless, possibly a unique attempt in trying to grasp, with minimal 'pollution' and manipulation, the hidden lives surrounding us, and the glimpses of so-called invisible deviances variating behind the soft curtains of our daily stages.

From genealogy to an interactionist "hybrid" socio-ethnography

Strong aficionado while researching the theme of this thesis was perceived in attempting a form of a genealogy of secrecy to contemporary times. Such an approach proved worthwhile for a lifelong work, though a few elements of this quest has remained in the

thesis. This is perceivable in the rites and mythologies section, and the literature reviewed in the form of a genealogy of studies on secrecy until today. Indeed, the genealogical method – inspired by the writings of (Nietzsche, 1887) - attempts to find patterns, and indeed doubt of the 'truths' that in time have become granted, central as to understand the true meaning of things: their development and change. With part 2 and part 3, nonetheless, this work has engaged in the interactionist approach of qualitative research methods, involving participant observation and direct study of social interaction, individuals and the tools surrounding them. This involved also the integration of cultural mediums, such as cinema, music and television, offering instances that enforce, and describe the secretive milieu within the onlife.

Indeed, the attempt was not only to represent the various elements of the onlife – and the criminological ecology of its environment – but to enumerate the development of various instances of its secretive induction: the 'means' in which privacy changed its connotation, secrecy became a fundamental aspect to interact with technologies. Also, the rapid disintegration of the private space – from an initial public one – into an ever more secret institution – with totalitarian connotations.
The research focus/questions required a socio-ethnographical approach; in part 2 this is explained and related to theoretical / epistemological considerations, and in part 3 by a specific recollection of case studies, gathered in what it is here conceived as 'offlife' counter-conduct ethnography. This is significant as the approach underlines not simply the onlife theorization of Floridi (2015), central in the criminogenic implications of this work – but also as a researcher to (partially) step out of its ecology – the specific environmental elements that define the crime and criminality this thesis tries to identify. This means not only look 'over the shoulder' of certain actors, but side by side – and yet again at a distance. With such an approach, combining genealogy and ethnography, the candidate feels confident he has found a means to understand the current condition – recognizing effectively "how we got here"; at the same time observing and critiquing by being engaged yet managing to 'stay out'. More details on the approach will be offered below.

Receiving data, not collecting capta

While the basic definition of 'data' relates to some sort of information, or an action recorded through observation, in aid of facts and statistics, such word nonetheless derives from Latin implying something given (datum). In the digital equivalent of such datum, such information becomes source of and from the user, such as age, gender and address – at least in minimalistic terms. We may already sense a net difference in the 'purpose' of collecting data: instead of being something 'given' by the user, digital recollections would thus appear usually compulsory and sometimes un-noticed. They are latent operations, produced in the background of our device use and internet navigation. In this light, such information appears formally as 'taken', rather than given, or handed over. Such argument, offered already in Lanigan (1994), are thus coined as capta, from the Latin

capere (to catch). Such idea has been picked up, indirectly, by other academics such as Drucker (2011) in the field of digital visualization tools and psychology by Russo (1957).

The data/capta distinction, to which I will later offer a greater theoretical analysis, offers nonetheless an important sensibility to the nature of this thesis, whereas some information stored by a user, and un-noticeably (not incidentally) taken and sold by corporations (GAFA/Big Tech, in particular), would appear not simply a harmless use of 'data', but a forced *capta* of what could have been hidden and a secret. Our role as citizens appears as one of requirement to 'give out' information and at the same time protect, obfuscate and secure ourselves. This incoherent condition, as I will show, contributes in the circumstances of suspicion, control and desire that this thesis engages.

Capturing Data

The exploitative dynamics in which information extraction (capta) take place on a normative basis during normal of internet navigation, smartphone use and general - characterised by an alternation from voluntary public exposure (in social media and networks) to a rather 'background' recollection. The implication is that the secretive conduct derived by such onlife ecology is a response to the overexposure, nonetheless the 'hiding' behind passcode, touch ID- and privacy policies in general - only increment and enhance the role of secrecy in our everyday life: it enhances its meaning and function.

So, what do we really talk about when we talk about 'giving away' information? Let's consider this. Words matter in coding: with the wrong spelling or usage the entire page fails: the same thing happens in society. When we talk about "data" we imply giving something: it is an exchange, a basic anthropological reciprocity. When someone asks me a lighter on the street, and I kindly hand it over, one presumes the stranger's interest is in lighting a cigarette. And if that is case, it is fine - and one assumes that all there's to it. But what is not ok is if the person along with the lighter takes note of the brand, measures the quantity of gas in it, asks me my name - and now that he's at it analyses my fingerprint – and stares me as long as he can. When this happens, we are talking not of giving and receiving: we talk, to be mild, of taking and keeping.

The taking and keeping appear to have become a central element of internet navigation: 'data' are taken and kept from users - analysed and monitored, on a regular and spiralling basis. This is nothing new - and it is beginning to become a known fashion. Nonetheless, the wording is central, because it gives a different light in what takes place, how and why. The word 'data' is indeed perhaps too kind, if not simply misleading. What rather takes place - what is involved - is not a giving of our information - but a taking. In this perspective, the datum (given) is to be redressed as 'capta' - something taken. Such approach is not novel, and indeed the 'capta' conceptualisation has been used before, in particular by Lanigan (1994) who uses a methodological analysis related to information 'taken', opposed to one that is 'given'. It is nonetheless a somewhat anachronistic

reckoning, that today need to be directly considered. Capta, arguably, are the currency, and the abusive power of the systems that are built around us.

Observing and 'overhearing'

As mentioned above, there is an evident methodological difficulty in producing a thesis and thus collecting 'data' describing the hidden ecology of a surrounding, and entrapping, secretive onlife existence. Hence this is the direct involvement of anyone and everyone to its features. In many ways, this work wishes to analyse the hidden dynamics of deviance – but as Becker already noted in his Outsiders, the secret deviance is practically impossible to analyse: "no-one notices [it] or reacts to" (Becker, 1962 [1997]) – with particular emphasis on the social harm involved.

If Surveillance is characterized by an 'at a distance' approach, aided by the secretive/covert mediums (Szakolczai, 2021)- the analysis of its features required on the researcher's side a pure Chicago school "ethnographic approach that involved the need for talking to, living with ("participant observation"), and getting to know the people they were writing about, seems self-evident enough"((Melossi, 2008, p. 106)
The approach of the Chicago School was one of not being afraid of the crowd, less than ever to expose its features – such perception was felt significant – more than ever with the Covid-19 restrictions: elements that through-out the thesis I have suggested must have increased evermore the dynamics of secretive conduct.

In such perspective, this work required an approach that would find itself in tune with the condition of 'gathering' information – and not disclosing secrets. Allowing the incidental 'exchange' of instances – rather than the specific 'confession' of incidents. In this mode, a new form of 'hybrid' methodology was conceived – or allowed to form freely – whereas the data and case studies were 'gathered' as a form of gift – ad not a specific 'capta', seeked out and hunt down only for the purpose of 'research'. If the smartphone and the onlife reality specifically 'induce' such forms of conduct, as my thesis was trying to prove – I need to either conduct myself similarly (whist nevertheless falling possibly in a muddy water). Instead, as already mentioned, it appeared essential for this research that I would not be fully engaged, but as much as possible detached – a citizen of the onlife existence but at the same time an *offlife* participant. With this approach, I found myself as an incidental observer of the surrounding ecology – to which participants are fully integrated and, often times very marginally critical (Giglioli, 2019). As the onlife existence involving smartphones, social media, networks, online maps, interactive apps, freemium games are surrounding the everyday in a regular and complimentary fashion, even a simple glimpse of the surroundings proved a significant source of study. But here the research would open further possibilities: as most of my generation, being digital natives, I was enthusiast and totally integrated in the social media milieu. I have used and committed, for at least half a year or so in all major social networks, from Twitter to MySpace, Flicker, Google+, Snapchat, Instagram, only to grow ever more tired, sickened

and even scared of them, and finally closing each account one by one, until deciding of getting rid of all of all my social network profiles, sometime in 2018. Since then I have attempted to live – and continue my research – in what I call a (partial) *offlife* existence. I've *disconnected* myself of all Social Media – including WhatsApp and Telegram – and ultimately getting rid of smartphone altogether. Ever since I use only a basic GSM phone for calls and texts, having a computer as my sole access to internet – allowing me to conclude this work.[14] Such fundamental 'disconnection' from social media and networks has offered me what I perceive as a detached, objective and free, highly critical consideration of the various aspects of its manoeuvres. Also, I have personally witnessed the difficulties in effectively continue a healthy social life (COVID-19 notwithstanding) and communicating without chats, nor messengers – avoiding emoji and voice messages – depriving myself of instant searches, GPS positioning, fitness measuring's, all those everyday routine signals, notifications and pop–ups that fill the *onlife* of fellow students and colleagues.

Nonetheless, I have insistently attempted to keep myself up–to–date, constantly enquiring friends and consulting tech–sites to inform myself of new software or hardware updates – new features, technologies, dynamics – becoming in certain occasions more 'aware' of the features of some devices than the very users surrounding me.
as stated before, I have sidelined myself from using a smartphone since 2018 and during the entire duration of my research – along with unsubscribing to all social media and network. This fact seems to stand out in any social context, in every occasion.[15]

As seduction, induction and manipulation are central elements of the smartphone use – because of their very design- the research of 'getting data' of this thesis attempted to side-line itself from such system: commenting incidental encounter to which any user – academic or read, or simply interested or 'woke' citizen, may relate to.

Data as Method

To collect 'data' is an intrinsic feature of modern science. Data is interpreted as proof, acknowledged as 'hard data' – strong evidence of what is been researched. The more 'data' is collected, the better a theory appears grounded. The more this data may be analysed by others, the more the conclusions share, the better the scientific process is accepted. Yet, when we collect data in the general sense, we acts as hunters who pick samples in the fauna and the flora. We thus remove the sample and analyse it in our personal labs for our personal research and, eventually, gain. The same takes place when we process interviews, collect information, select material: we take and use. The capta dynamics, though exaggerating, appear integral in the research: either we realize or not. Nonetheless this approach is important to analyse, even from a criminological perspective, because it is exactly the 'blurring' lines of these dynamics that allow all sorts

[14] This is a point to be noted, as I doubt not only this thesis, but any thesis, would be almost impossible today to be finalized without an internet connection– not to mention the COVID–19 lockdown difficulties.

[15] Such aspect appears more and more worth noticing, as time passes and I find myself more and more treated as an (inconvenient) 'fish out of the [onlife] water'

of abusive data gathering, that while owning a form of scientific value – and making the internet 'work' – it is not the only data gathering may be done. Both in doing research and online navigation a more coherent approach to the original meaning of 'data'.

The data as given implies another forms of research, that is in no way novel, and indeed indirectly it is pursued by most researchers, nonetheless it is worthwhile to underline its dynamics. Such distinction is not purely over qualitative or quantitate analysis, ideally, both can engage in elements of capta, as well as elements of data-as-give. This short article will use as a case study my personal attempt to produce a PhD thesis that gathered material for a case study, only relying on the 'data-as-given': such approach implies the possibility to produce knowledge without 'capturing' information.

Onlife listening and reading:

This thesis tries to combine the online data gathering with the epistemological misinterpretation of what 'data gathering' is. We have distinguished what is, effectively, a capta dynamic, where the information is 'taken' – oftentimes not only without consent, but actual knowledge of the actors/users involved.

For the ethnographic analysis in producing this PhD, I've engaged a narrative criminological perspective of shadowing the onlife ecology. If the idea of shadowing implies some sort of questioning and active involvement over a length of time(McDonald, 2005; Quinlan, 2008), my interpretation and use of the method involved a spontaneous 'uniformity' to the surrounding ecology. My approach was to use my digitally native expertise and natural social involvement to witness and observe the elements of suspicion, control and desire on a spontaneous basis.
My approach was not one of recording, filming, interviewing or intervening, but listening to the spontaneous environments and the actors/users involved. The word listening is ambivalent in the onlife reality we are experiencing. The onlife underlines the blurring line between online and the 'offline' word: the two are part of the same existence, the same 'life'. To listen to what goes out in the streets and 'read' what happens in blogs and forums appear as equivalent – and I will compare such an approach with the condition of the flaneur. Nonetheless, it is important to underline the connection between street listening and online/onlife reading. As we mentioned above, the hunter-gathered aspect of collecting things and storing them – ripping roots, picking berries and fetching eggs – is a strictly capta dynamic. It is a well-established action, that carries with it all sorts of meanings and rituals. Nonetheless, while pursuing his or her hunts, the hunter-gathered enjoys all sorts of nature gifts that are offered. The chipping of birds, the warming sun rays, the refreshing breeze. These are all indirect 'sensations' the hunter-gatherer may experience and enjoy. They are priceless, and uncollectable, at least in quantifiable manner. These are, in other words, qualitative 'gift' experiences – opposed to the quantitative analysis. But in a quantitative perspective, when engaging in nature in such perspective, the sudden 'discovery' of an unknown raspberry field, or a family of excellent mushroom, appears per se also a quantitative gift.

In a modern-day analysis – such condition becomes evident when seeking inspiration. A writer, a researcher or an enamoured may be wondering in the city streets and discover all sorts of glimpses of life that may offer qualitative joys – that may produce a mood ideal for further work &/or love, or effective, concrete quantitative forms of inspirations – producing a poem, a concluding chapter, a love letter. The messages that cities produces, the outer world, are indeed uncountable, for anyone who may or wants to see and listen.

This choice of going 'offlife' has opened a quite astonishingly incidental set of valuable considerations: not only reflecting on – and indeed arguing about – our entrapping relationship with our mediums, and thus our being fundamentally servomechanical to their functions. But also, by presenting my offlife existence in the everyday life (to do so I just needed to place my *gsm* phone on a table; admit that I was not part of any WhatsApp group; not even willing to access maps or GPS tracking), those completely involved would question such liminal position, and quite naturally – again, to my astonishment – open up to their worries and concerns about not only the onlife existence, but rather the ecology of secretive conduct it permeates. But observation was not enough to grasp the conditions and occurrence of the instances I tried to recollect: essential was also the perception, the feeling, and in this, the 'overhearing'. Much of the auto-ethnography in this work indeed took place picking up indirectly instances, conversations, dynamics: and when commenting them, nonchalantly, accidentally or trivially, such approach would arouse a number of responses, agreements, nods. As if the secretive world surrounding us is just waiting to be leaked: released and discussed. It is in this perspective that this work found fertile ground: in the recognition that almost anyone in the onlife dimension, and subsequently owning and being surrounded by smartphones, has stories to share, discuss, comment, on secretive conducts and its counters – personal or indirect, regarding colleagues, partners, friends, kin, neighbours – or simply oneself. It appears as something anyone may relate to. Anyone may contribute ad add relevant features of Suspicion, control and desire to the thesis: from phone conversations, photo bombing, group crashing. To these, we must consider other insights that, with minimal reckoning, offer instances of secretive conduct with the arts – cinema, music, literature – a central contribution to the cultural influence of secrecy in the everyday life, underlying the global scale of its features.

These materials gathered and commented, that would result in specific sociological vignettes, formed from two specific instance, both quite peripheral and non–conducted (directed or manipulated)

1. elements of secretive conduct taking place, with the most naturalness – in front of the observer, and the general 'acceptance' of all surrounding peers.
2. Subjects approaching and revealing their doubts in the secretive conduct of a kin, friends, colleague, lover, partner, stating – oftentimes without remorse – the conditions of a secretive conduct.

The ethnographic analysis of this thesis 'plays' with the vague distinction in what is perceived as deviance and harm in the onlife existence: what is allowed, what is labelled, and what is stigmatized: what is tolerated, what dangerous, what harmful. These appear as an unclear, ever-changing and generational set of rules which we are constantly put to question and scrutiny. Indeed, as opposed to my MA dissertation, where studying the parkour culture I participated in the action, trained with the subjects and 'asked' questions, for this thesis I insisted on *listening* to the surroundings. Such an approach, if it must be labelled, appears aligned with Simmel's form of sociology, as defined by David Frisby, Simmel being "a 'wanderer' through the everyday world, […] able to adopt 'a distinctly "objective" attitude' to social reality since he possesses that lack of attachment and the necessary distance of the wanderer" (Frisby, 1985, p. 65). Frisby underlines Simmel's poetic "search for 'the transitory, fleeting beauty of our present life" (ibid, p.70). Indeed, this thesis maybe lacks such poetical qualities, yet is inspired by the very sociological qualities of the *flaneur*: it wishes to underline the sociologically *flaneur* considerations on secretive conduct witnessed, produced and considered here.

By *listening* to anecdotes and testimonies, directly and indirectly, innumerable vignettes have been collected as instances of the intricacies of secretive conduct happening in all surroundings. These have been recollected, noted and jotted in everyday occasions, from parties, to dinners – waiting for the bus or standing in line. Some have just required view and observation, others a slight comment, a vague question: and in those occasion, not always but consistently, the 'confessions' of everyday secretive conducts simply 'spilled out'. In these terms this work side-lines with the growing field of narrative criminology. Indeed, in the specific circumstance when the narrative of the events is focused on, the indirect/peripheral interviewer transpires his 'sensation', 'perception' and 'interpretation' that 'something is not quite right', that 'he or she must be hiding something' or even a simple 'why is he or she doing that'? The social vignettes offer, through fragments of everyday life, a valuable insight as the total social fact of a phenomena. The 'vignettes' appear as a decorative feature, with their very etymology deriving from the vines drawn on the side of book pages, and ornamentation in general (OED). Such were depicted either as shoot or vine leaves (*pampino*). These 'fragments' or "social vignette" are evident in the work of Simmel, and for Frisby offer an "outline of a sociology of the senses" (Frisby, 1985, p. 70).

Again, such approach is not new or unique: forerunning academics such as Ferrell (1996) and Wacquant (2004) managed to engage with the 'out there', integrating it, joining it and 'living it' with their theory in a much more chirurgical fashion: their approach underlines the importance of tackling everyday life, where "every event, how–ever restricted to this superficial level it may appear, comes immediately into contact with the depths of the soul, and that the most banal externalities are, in the last analysis, bound up with the final decisions concerning the meaning and the style of life" (Simmel, 1971, p. 13)

The vignette type analysis of this work is occupied with the vague distinction in what is perceived as transgressive and deviant in the onlife existence: what instead is allowed, what labelled, and what stigmatized. In the use of certain devices – such as

surveillance cameras within the domestic space – privacy appears breached by anyone who enters the home, even the inhabitant himself: the privacy appears to be in the hands of those who may consult the recordings in private. These appear as an unclear, ever-changing and generational set of rules to whom we are constantly put to question and scrutiny.

In perspective, my work forwards the considerations of Fromm and Les Back's pieces on the 'Art of Listening', to which the two works offer different, yet valuable perspectives. Fromm embraced the psychoanalytic "technique", to which he states 'rules' and 'norms': by replacing 'analyst' with 'researcher', significant to my work is Fromm's insistence on the researcher's imagination expressed and perceived freely, as well as his empathy, not only in living the vignettes as his own, but love its conditions. Opposite to Fromm, who perceived such requirement as necessary to perceive and comprehend the other without fear, I admit my approach differs in recognizing evident problem of 'loving' the onlife reality and its technologies: rather, the objective was not being tainted by the onlife comfort zone our society is accustomed to – and thus incite for an unconditioned love to the devices surrounding us.

By comfort zone I intend the technological fatalism, described in many instances in my work, our society appears conforming to. The widely shared perception is that onlife secretive conduct is an inevitable result of the use of our devices, something that simply is – we have evolved to it – we need it. Not only it is perceived inevitable, but handy, pleasurable, efficient, necessary, perfectly fulfilling our desires and offering shelter and creativity to our (ever–lonely) existences. By posing myself as counter–current/counter–conduct (many of my interlocutors admittedly accused me of being a mere hipster) to this onlife technique, my listening would thus appear not tainted, nor hypocritical, to its use. External yet native: perfectly aware and integrated.

In Back, we find a more in–tune' "global sociological imagination" (Back, 2007, p. 23), – winking to C. Wright Mill's – "grounded in the contested encounters of the everyday multiculture" (Sharma, 2008, p. 587). Back invites the researcher to paying attention to the "fragments, the voices and the stories that are otherwise passed over or ignored" (Back, 2007, p. 1). We must underline here that what is passed over or ignored in secretive conduct is the fact that the issue has hardly been openly addressed, because it has become a regular, yet damaging, aspect of society. Its schemes become revealed and evident only when spot–lighted, as this thesis wishes to do: they are, in other words, in the mouth of everyone, but with no–one to tell it so. Very few are out there to listen.[16]

The approach of listening as a form of methodology appeared central just as it was conceived: incidentally. Indeed, the recollection of the ecology of secretive behaviour appeared while writing this thesis visible in any environment, occurring with naturality and regularity– or in the words of Les Back (2007) at the local bus stop of any onlife society. As a researcher, I never had to ask for data, it was constantly delivered or given: showed, exposed, or simply 'conducted'.

Further research

[16] In this remark, listening also opposes the idea of perpetual "reading"(data, thus analysing)

Such method, that can be indeed recognized as a form of 'offlife ethno-methodology', would thus implicate a mode of doing research that avoids the occurrence of capta, but accepts and 'takes in' elements of pure 'data' – intended as *given*. In practice, such method is valuable as is offers a way not to induce the interviewed/interlocutor towards a certain consideration of the onlife reality (which is inevitably any westerner's reality); but rather remains open to personal interpretation on behalf of the speaker. He or she, in other words, confesses the elements – without being forced to do so: the approach welcomes by this the complete spontaneity of information exchange. Such modality is in no way novel – especially related to internet use. Digital ethnography researchers (Pink, et al., 2015) or even more recent hybrid ethnographers (Przybylski, 2020) have use of 'open' and 'unrestricted' comments and reviews posted on various platforms and online – whist respecting their privacy. In this work, I have attempted to respect their privacy *and* their secrecy. This is because it is not simply that names have been changed – but the instances shared are easily reproposed in different context and cultures: the secrets are shared but there are everybody's secrets- they are 'pulcinella secrets' (Mordini, 2011): something everyone is aware of, and which anyone may talk about – without needing to refer to directly. This is because everyone knows what is being implied, and who is involved: again, everyone. Moreover, the deviant element is also not universally perceived, but nonetheless clearly appearing as a relief once finally addressed. Is it alright to monitor one's sibling on a nannycam? Is it fair to check your sons or daughter's text? Are all these instances of intimate surveillance normative only because they are unspoken, or because they are invisibly popular? Such question, though addressed in this work – need further study and more data. What their addressing nonetheless implies is that such pulcinella secrets – meaning secretive conducts that everyone knows take place but nobody addresses; are perfectly compatible across cultures and ages – thus merging in a non-discriminatory and non-binary recollection of valuable case studies and onlife recollection of the secretive conduct. Any researcher, seeking similar instances, may find other, albeit similar, considerations – through genders, cultures and generations.

Ethical considerations

Already in 1998, Gary T. Marx recognized that data collection implies some form surveillance, arguing for a fixed set of etiquettes, thus preventing 'immoral' or harmful conditions. In scholarly considerations, this translates with a sort of necessary 'prudence' on behalf of the collector, and the need of 'consent' from the collected. When we look at what is commonly known as Big Data, we refer to the 'information' "aggregation, analytics, and predictive modelling" (Brunton & Nissenbaum, 2015, p. 51). The way in which collecting of data implies the 'taking' of information "we have willingly shared, or have been compelled to provide, and produce knowledge from inferences" (ibidem). This takes place through virtual and digital means within (but not limited to) a web-based/online interface, the concepts of consent, morality and harm, change perspective.

Indeed, a great deal of concern was given in avoiding the replication of capta – and instead make the greatest scientific advantage of the 'datum' received and perceived across the

thesis. My intention was to avoid the hegemonistic approach of wanting to prove a theory and using subjects as my experiments and 'lab-rats'. Instead, I opted out of the research equation becoming myself the object of the experiment. The people are not the data this thesis is based on, rather the glimpse and food for thought. Rather, I became in many ways the interest of study for others. With this approach, I recollected and observed reactions as well and discussions. The use of vignettes in this context is rather a philosophical escamotage. This approach is very common in Socratic dialogues, narrating episodes as an element of explication of concepts. Names, locations, timetables are not significant, what they do is conceptualise around an issue. They are not mythical (such as in the Cave analogy), as they recollect elements of reality – however the true participants of this reality are not significant. This approach is philosophical but also anthropological. The vignettes indeed are not 'case studies' per se, nor they effectively 'prove anything', nor sustain my theory as 'mere facts'. Rather, they offer a qualitative starting point for the secondary analysis. They are glimpses what is happening is an everyday phenomenon – precisely within the ecology of the onlife. However, rather than using this 'data' as to prove when certain episodes happened and where, they are used to replicate and conceptualise over the milieu that allowed these conditions narrated in the 'vignettes'. They are something that I have witnessed and that anyone may relate to, as well as finding further proof online. With this work (that has been approved by an ethics commission), the ethical consideration has gone beyond the simple keeping animosity of the people and the conditions involved. In fact, the people involved are anonymous per se, as their existences are submerged in an overflow of onlife information. They give meaning and a palpable 'concreteness' to what otherwise are digitally formed perceptions, social media recollection, new-media mediation. The episodes and vignettes that I describe are easily recollected and replicated on blogs, vlogs social media, and all sorts of personal and voluntary public exchanges. My intention was not to make a testimony of 'intriguing' scenarios or conditions but recollect the spontaneity and triviality of their occurrence. Any reader feels involved, any user is a participant: we all perpetually replicate the elements of suspicion, control and desire while being involved in the onlife scenario. For this reason, the vignettes represent trivial matters of central importance. Not as single episodes, but recurring glimpses of a milieu, experienced within their habitus.

When applying and discussing experimental elements of this research approved by the University College Cork ethics board, central was the implication that no specific 'data gathering' was involved in producing this thesis – confidentiality was in no way tackled, nor the vulnerability of subjects engaged with. The confidence in this stance lies in the fact that not only there has been made no use of recording, rehearsals, or filming – but the social vignettes described, and the people involved, are of informed yet anonymous individuals who share nothing in common but significant and explicatory experienced glimpses of the onlife ecology – to whom any global north user may easily relate to and identify, while in no way discriminate or break any confidence. The people involved who shared personal experiences did so with the awareness of my work and confidence of having nothing to hide – although many loved to confabulate on the secretive conduct of others – friends, relatives, colleagues – none of whom are identifiable. Instead, they represent only the proof of the triviality and the effective normative aspect of suspicion,

control and desire in the everyday life. The opinions of the people I talk to or observed appeared to have little more weight than a tweet or any other public social media post. In the same way, I have rightfully maintained their anonymity – but particularly because their identity, and for the most part their nationality or gender was not relevant. Even what they say is never in any way dangerous or damaging, to them or others. I have thus recollected their statements out of memory and not verbatim. They are not significant for the used words, but the perception that allow. The request to fill out consent forms and language statements were not deemed necessary because it would have specifically denied the 'data-as-given' spontaneity of the research. By approaching them with a specific aim to find out about 'secrets', none of these would have deemed to be revealed. I have nevertheless, as agreed with the ethics commission, respected their animosity – and in many respect their secrecy. None of these have been revealed, as nothing, in the true nature of its dynamics, is clear, even if it ever happened. Moreover, any controversial and ambiguous position that had no scientific value on behalf of any of the peers, has been left within living memory to be forgotten.

The methodology I offered and followed in the thesis outlined the importance of the participatory observation (as practiced by the Chicago School – symbolic interactionists) and personal involvement in the research through auto/ethnography of at times shadowing at times evident and spontaneous bystander. My engagements with subjects were mainly of a passive observer and eyes dropping listener to the surrounding ecology. The information gathered proves nothing per se, expect offering a glimpse of the reaction and the general feeling of the elements of secretive conduct. What I tried to do was to recollect some casual understanding of observations and situations that replicated elements of suspicion, control, and desire. All the subjects were informal and mainly to aware them of the nature of my research. They shared some of the perspectives informally and anonymously. All consideration of what has been personally witnessed have rested solely on my lived experience – which becomes a central disengaged offlife element 'within' the onlife environment. While indeed a lot of consideration are done on children and their surveillance, no child has been addressed, and only referred to through the shared experience of the parent/guardian. Other information used are either publicly available media, technology, film and literature. I have kept notes of my experiences and reflection in an electronic journal which are only accessible by me – and no names/place names or identifying features have been documented. There has been no risk or harm related to the subject of the subject matters or subjects themselves and any identifying feature has been removed. As nothing has been effectively being recorded and most of these instances have been perceived as a sensory ethnography nothing is stored. None of it, in respect to this work, may produce elements of harmful data.

Part II: Ecology of the Onlife Secretive Conduct

In this core section of this thesis, we will engage in the dynamics of secrecy and the tools that produce and propagate its features within the onlife dimension. This approach will be theorized and accounted for on a cultural level, referring to both cinematic and literature elements representing secretive conduct – and the relevant equivalent within the web-connected world. Central in this argument is the smartphone – quintessential smart device- that allows the idea blurring between being in the 'meat space' and yet connected to the 'metaspace' – allowing, so to speak, to call someone through the built-in antenna, and at the same time chat with the same person through the digital web-connection. One may 'snap' pictures of the meatspace and shared them just as easily in the metaspace. The smartphone may aid the intrusion of the stages and share them across devices and info-spheres. Such onlife device is the fundamental storer and gatherer of personal data – both commercially available of more cryptically kept raw within its internal memory. It is also the carrier within its fundamental features. What it also allows, is the connection between various characteristic of secretive conduct, for the user to be protected behind a veil of security – yet allowing intrusive and non-obvious uses. It connects various elements of smart technologies, involving highly precise and invasive elements – such as GPS (now GNSS) tracking, web connected micro-lenses, indiscreet instant messaging groups – permeating the seduction and induction dynamics of an incessant conduction of secrecy in potentially any space of the global west.

2.1. Hiding and controlling our conduct everywhere

In the Italian comedy 'Perfect Strangers' (2016), a group of life-long friends meet for an informal dinner, bound to become a sort of sociological carnage. In order to spice the mundane event up, or to get things off their chest, they decided to play a game: what would happen among them if they were to exchange their smartphones and allow others to freely read any text received and put calls on speaker? Of course, initially, all claim to have nothing to hide and will enjoy as a joke the first interactions. Subsequently, they raise the curtain of their privacy and reveal the backstage of their lives, in other words, the secrets. Betrays, schemes, cheat unravel is a dramatic set of event, that leaves the viewer ever more terrorized by the actual 'credibility' of its conditions and resolutions. Perfect Strangers as a film is significant for various reasons. Not only the movie is a good comedy, but an extremely relevant one to our thesis. It comes to surprise, or maybe it doesn't, that it has won a Guinness world record for the most adapted movies in history (Finos, 2019), proving how indeed the issues raised are truly global.

Such a movie helps to consider the elements of exchange we users are today faced to engage with. When an individual enters a public space (metro, airport, waiting room), he is armed with a mobile object of cover: she/he lifts the phone and is potentially locked out, by everyone and everyone from she or him[17]. One may speculate whether such attitude and conduct appear universally noticeable in any country with mobile data availability. What goes on behind the screen is hard to scrutinize for a bystander: the experience is strictly personal. The content is available only once it is processed and

[17] Arguably, since 2020 he is armed with twice as many objects of cover, smartphones and facemasks!

shared through platforms and apps in general. In this perspective, visibility behind the content is only marginal. The original source is secret. Also, secret is the choice of the selection or the intention of very selection of what is to be shared. While with the make up a 'secret' formula could be achieved and applied to produce a certain successful effect (secret formula have – I would claim – always been a very popular catchphrase in ads); there is nonetheless a general acceptance that there is a 'performance' or 'illusion' of some sort[18] taking place. In the online exposition of smartphone content the 'trick' is not revealed, nor even admitted.

Front and back and back-and-forth

When an individual enters the presence of others, she/he will commonly seek to conceal information about him/herself from others or bring into play information about him/herself that may conceal any other information previously attained, delivered, or handed out. He or she will lead forwards a performance (Goffman, 1956) of how he or she wants to appear, starting from physical aesthetics and masking in general. Richard Sennett has offered in his Fall of Public Man (1974) a detailed analysis on the role and relevance of clothes and exposition in the formation of the modern man. Moving towards the contemporary scene, we may notice the quintessential role of clothing and masking in the everyday exposition of who we are and want to appear like. The effect of 'making up' our faces, enriching features with earrings, necklaces, piercings and rings, have all naturally characterized mankind since the dawn of civilization: today we may notice not only a consumerist aspect of such 'vain' products but also the 'open' exchange of its role and features between ages, traditions, and genders. Such exposé can be ultimately noticed even in the very popularization of tattoos, that indeed covers with ink the skin with the purpose of exposing; or the actual removal of hair as to expose the skin or muscle. Moreover, this appears as a form counter-exposition with the trend of growing facial hair, a feature perceived of bad taste, even prohibited, especially among professionals and politicians, just ten years ago (Newton, 2018).

The effect is perhaps just the same: the desire to enhance features as to hide others, to expose as to shadow elsewhere. A distraction, a refraining, and even an obfuscation of what is behind the curtain: as encountered in Simmel, (Simmel, 1906) we perceive a façade to which all the windows appear covered by a curtain, as long as the subject is free to choose where curtains are pulled, and where open.

If clothes represent the curtains in the windows of our persona (Sennett, 1974), locks represent the gates and doors of our homes. Locks are the first things we deal with while entering through our door, and the last we check before exiting. Indeed, the door is very basic object of everyday life, as it has been colourfully analysed by Simmel, threading

18

Also prestige, as in Italian the word originally used for make-up is 'trucco', trickery

Doors and Bridges as two fundamentally different yet connected human fabrics that indeed change the idea of humanity and society. For Simmel, as opposed to the concept of a bridge, a "door displays a complete difference of intention between entering and exiting" (Simmel, 1997). The power of the door, with its capability of being both opened and closed (as opposed to the bridge that is crossed either ways by forming a "permanent interchange"), "its closure provides the feeling of a stronger isolation against everything outside this space than the mere unstructured wall".

Once inside our four walls, within what Goffman expressed so precisely as 'backstage', and with the outside world 'closed' out and separated, we are brought before another number of locks. From windows to drawers, daily objects are inserted in smaller and smaller containers, are closed and kept: how many of these nonetheless require actual keys to be opened? As mentioned in many occasions, the most evident one is the smart-phone, and indeed with the advent of the so called 'internet of things' our homes are becoming 'smart', raising the question of how many more keys they will contain. They have become the last object we look upon before exiting the home. Indeed, since a decade or so the Wi-Fi has its key, stored usually with an overly complex row of figures and letters. Now our thermostat may be accessed through an app, requiring another 'key'. Possibly in a near future we will lock our fridges, just as our cars, to contain our stomachs.

Locks and keys thus appear a common fabric of our lives. Locks have become something that connects and at the same time stores, while at the same time, almost paradoxically, separating. Locks and gates are a figurative image of the everyday internet user: one who cannot navigate without having constantly to prove his identity by opening locks upon locks: from the computer to the Wi-Fi, to the email, to the smart-phone. And locks are the forms of engagement with any screened device: they lock the eyes of the viewer the hands, the concentration. The same the forms of interaction, from a YouTube video through news articles to a WhatsApp Chat: and furthermore, in our everyday interaction we are locked out from the content of any screen placed as an architectural barrier before us, from the cash counter of the clerk to the monitor of a post office or bank managers. We are placed before the back of a screen: no visibility of the content, even if the information regards 'us'. We are no longer face to face: we are locks before locks, locking the audience and users out of the 'outside' world. We have become covered with a light that surrounds us and captures our concentration. The locks thus become central and essential in the production and manifestation of secrets and of secrecy itself. What goes on behind the 'closed' space is protected by the lock; yet, in an ambiguous analogy, it is the very 'portal' for what it reveals: the lock itself is the inevitable peephole.

Yet, paradoxically locks and keys are no longer invading our homes, miniaturizing the space where physical objects may be stored and kept. We used to install since the industrial revolution safes that would conserve securely cash and jewels, but these are rapidly being substituted by digital banking. Our cabinets no longer conserve under key pornographic VHS, magazines, or past lovers' letters: these again are stored in our

phone's archive – its basic folders and the most cryptic raw-data. Indeed, the home has developed a very new understanding of visibility: except for office-furniture, Ikea's home products have become minimalist, its drawers softly openable: cheap and harmless.

Store and keep

This is interesting if one looks into the etymology of the verb to conserve, as its root derives from 'servare', "keep watch, maintain" (from Etymonline): it is an action of 'keeping an eye on' something, underlining some sort of visibility. To conserve something is to guard and protect it, storing it and yet keeping it at hand. Indeed, the cabinet was a necessary object to have thing locked in homes that were once, as Ariès noted, "crowded with people" (Aries, 1960, p. 378). They were indeed much more public, especially among the nobility, with a constant flow of visitors, friendly, social and professional, and servants (custodes in Latin, which is also the root of 'slave').

Houses thus welcome no longer endless flow of strangers visiting our homes, and no store longer goods to kept locked away. What is to be showed, to return to Goffman, is rather 'exposed' in the sitting room: books, magazines, porcelain, painting, pictures that express who we are, and where a 'chosen' set of guests gather in close intimacy.
Nevertheless, homes as we know them have also become mute: thirty years ago 'voice messages' would be still recorded and heard on 'speakerphones', echoing in a repeated cinematic cliché of empty sitting rooms. The actual phone lying in the main corridor or sitting room is no longer necessary: the conversations, the discussions, the flirts take place 'cordlessly' and 'privately' inside rooms (a much-debated issue in Italian families, since the early 2000s). This is not to say that there were no lies and secrets, indeed there were codes and betrays: a famous example is Mina's song 'Buonasera Dottore' (1986), where a married man receives a (singing) phone call from his lover and he must coldly act as speaking with the doctor and yet arranging an appointment.

The first verse goes like this:

Lei: Ciao, sono io	Her: Hi, it's me.
Lui: Buonasera dottore	Him: Good evening doctor
Lei: amore mio	Her: my love…
Lui: Sì, mi dica	Him: Yes, tell me
Lei: Non resistevo più,	Her: I couldn't resist
pensavo a te	Thinking of you
Lui: Ah, bene	Him: Ah, good
direi che è importante.	I guess it's important
Lei: Quando verrai	Her: when will you be here?
Lui: Mah, adesso non so dipende...	Him: Well, I don't really know now, it
depends…	
Lei:non parlare se lì c'è lei	Her: don't talk if she's there
lascia parlare me	Let me do the talking
dì sì o no.	Just say yes or no…

Lui: Certo. Him: Of course…

Two things can be noted here: the excuse of a doctor calling in, worried of his patient and arranging a meeting, a breaking of privacy in the everyday life un-imaginable today, and a strategic conversation taking place between two lovers having the wife present. It is a very arduous task! While on modern phones, it is much too simple; almost banal.

Such ironic yet palpable situation of emptiness and loneliness in a space of congregation is extraordinary when compared to the everyday life as described by Ariès, where indeed up to the end of the seventeenth century 'nobody could be alone', and rooms had no distinction in their roles or specific furniture, instead "in the same rooms […] they ate, people slept, danced and worked and received visitors" (Aries, 1960, p. 381), often all in contemporaneity. "Social isolation was virtually impossible" (ibid, p.385); independence was exceptional. Only by the eighteenth century "family began to hold society at distance', with the first example of domestic life: privacy and isolation as a common feature not simply for nobility but middle class as well. Beds would be confined into bedrooms, as well as toilets and hygienic equipment to their appropriate rooms. It is here that we learn the essential distinction between a chambre opposed to the word salle (salon): a specific 'decent' distinction between where visitors may enter, and where there must stay out.

And from 'inside' – what may we see from the outside? This observation, now that we have lowered the curtain of our 'internal spaces' – the basic ecology of our intimacy – must turn toward the outside: what can we see, observe – whilst not been seen.

Cinematic culture of hiding and observing

In Alfred Hitchcock's Rear Window (1954), James Stewart plays a professional photographer who, being temporary injured and constrained to a wheelchair, spends most of his long summer evenings by 'spying' on his neighbours. The whole movie offers itself particularly well for sociological analysis, starting from its 'panopticon' setting (in a pure Benthamian sense) of a public display of bourgeois lives observed by a hidden (yet improvised) voyeur. With the aid of powerful camera lenses (devices that were available at the time only to few), the protagonist observes lives without intervening, with Hitchcock's masterful direction that lets the viewer himself make specific 'conclusions' or pre-judgements regarding what is going on in these homes. This is relevant also for the title of the film, which alludes to a back 'peep-hole' of our lives, as in Goffman, but also, possibly, the mirror to see behind, as in cars.
The movie enters its thriller connotation when a stormy night the protagonist 'hears' something, a shout: from that event, the movie will develop around the 'intuition' of something happening, possibly a murder, that somewhat 'extraordinarily' happens to be awfully true. His intuition and conclusion are very similar to the ones in another movie, Blow Up (1966) by Antonioni, where the story revolves around 'something' caught on camera by the protagonist, something he does not quite feel right, and yet is entirely uncertain of what it could be. Vaidhyanathan made such a clear analysis of the film that

I deleted most of what I had written on it myself, to insert instead a synthesis of his work: Antonioni being an Italian director, Vaidhyanathan notices in that very scene a particularly 'European' incongruence that demonstrates the "flimsiness of American conception of privacy" (Vaidhyanathan, 2018., p. 70). In the late 60s the "distinction between private and public spaces is no longer relevant" (ibidem). The lady protests when being pictured by someone in a public park, a fact that instead in the US is not an issue: the 'spectacle', as Debord would say, in US soil, is much more accustomed. In Europe, people felt the 'right to be left alone' even outside their 'private property': the realm of the private existed even outside four walls, in what evidently was a larger world. Today, the idea of privacy faces another threat. We might have enjoyed a form of privacy, until lately, inside a room, where to consult and write thoughts on notebooks in a single copy, while "now it's all in the heavenly cloud" (Vaidhyanathan, 2018, p. 70). Blow Up, Vaidhyanathan notices, "teaches us, long before millions of people walked the streets with powerful cameras in their pockets that one of the greatest threats to personal dignity comes not from large firms or powerful governments. It always comes from millions of individuals armed and in all places with audio, video and photographic recording devices" (ibid., p.71)

Rear Window and Blow Up describe two events, filmed in camera, that recall the idea that something might happen behind cameras, or indeed that what is recorded may be interpreted infinitely, especially following some specific intuition, or fear and paranoia.

While both films play on the idea of seeing something that was not supposed to be seen, Rear Window specifically films the concept of interpreting what goes on away from our eyes: as to quote both Checkov and Hitchcock, what cannot be seen, a curtain that is pulled, inevitably wants to be pulled down.

Though we will return to the idea of 'permanent surveillance' produced by a Harriett the Spy environment, described by Vaidhyanathan, an even more recent example of the 'abstract watchful eyes' can be drawn from the bestseller Girl on the Train (2015), where the protagonist sees or believes to see something inside a home from the window of a passing train. This is relevant in showing the building up of imagination by mixing true data as recorded on phone with (drunken) imagination, and how impressions may have an effect in the reality of events, especially in this 'mass-mediatised' society. (McLuhan, 1967)

These films, though many more may be mentioned, represent a variation of the same topic, already central since the birth of 'mediated images' within the everyday life. By this, existence is constantly monitored as is observed by an eye, then interpreted, studied and analysed. Moreover, these images may be twisted, modified and falsified.

All these were nonetheless preceded by the 1929 Soviet experimental picture 'Man with a Movie Camera' by Dziga Vertov, whose innovative camera angles and particular editing style explored the potentials of the filming medium, showing the everyday life of a Russian city, with its citizens, activities, parks and monuments, through an artificial eye, capable of fast-forwarding, jumping and reducing its views in forms and modalities unconceivable to a human eye. If we compare such tool again with the potentials of drones and satellites, we may conclude that we are living in a truly suffocating age: everything is filmable and editable, as being observed and potentially open to

misinterpretation. Ours is an age where day by day it is harder to find a space where to hide, not be seen, be in secret and thus peace.

Smart medium & secret mediation

When an individual wishes to reach his backstage, he ultimately realizes it has changed its connotation: it has become the door, behind which we isolate the metropolitan from the local, yet the 'bridge' of 'perpetual' communication with our family remains: the publicness of our lives, within our home, conserves the façade of the 'social media profile'. The secrecy of the everyday is miniaturized and the locks become sociological: privacy is not achievable in any room, because it is not necessarily: there is no need for the teenager to lock him/herself in his bedroom to listen to 'unappreciated' music or read 'unapproved' comic books; he may do so in the sitting room, with his earphones and facing the well sheltered screen. Thus, it appears society is no longer kept at a distance in the home, it is constant scrutiny, if only in different terms. The virtual is perpetually part of 'reality', aided exponentially by the technological tools surrounding our spaces. Everything is covered by Wi-Fi signal; everything is part of the networked 'media'.

When an individual enters the presence of others, she/he now usually does so with a "loaded gun": the gun is a smartphone. Any other member of a conversation is armed with the same and at any given time might be potentially interrupted. No-one other than the user or owner of the smartphone may access the screen, or the data contained. It is a safe place in public that has no place in the public: a backstage that actually leaks into the front. It owns a gateway with what appears to be public, though such feature concerns mainly only the digital and online aspect of what is to be shown. The content of the smartphone is personal and sometimes strictly, otherwise incidentally secret. Nevertheless, only a fraction – if any – of all the material produced (transactions, pictures, views, chats, scores) is shared and showed. Access is also personal and strictly secret: screens are locked with the aid of ever-complex biometrical technology, such as fingerprint and face recognition, along with pin codes and combinations.

With our online existence being "bicentric" (Lyon & Bauman, 2013, p. 37), the question of our conduct and their interconnection in the everyday life must be posed. Within the question of surveillance, the ever-growing installation and recording of our lives by now has become a somewhat ironically inflated topic. Satellites have surveyed our skies since 1974, when two nuclear-powered soviet satellites were sent in orbit as part of the Cosmos project, in order to allow a 'triangulation' of American ships (Arcangelis, 1987). This technology, soon followed by the US Elint and then Irint projects, opened the new horizon of a global collecting, interpreting and reporting of data across the globe on objects, people and situations. It allowed the common 'paranoiac' notion that we are constantly viewed, in one way or another, with eyes always above us, capable of incredibly detailed observation. In the latest years, some of the most preoccupying and powerful tools that are already 'invading' us through a physical and digital hybrid observation are characterized by the satellite's evolution: drones. These flying objects are becoming, to

common eyes, actual UFOs of uncertain technological advancement and capabilities, patrolling over cities, countryside and war-zones. They are the emblem of what surveillance is becoming: "remotely controlled, small, multi-sensory, bio-mimetic, invasive and for face recognition purposes capable of matching online information with offline activity" (Takahashi, 2012). Allegedly, this is now being implemented with a "pan-European network of facial recognition database" (Cambell & Jones, 2020), that would involve, at least for now, ten EU member states.[19]

Yet, the perpetual discussion of the pros and cons of the argument never actually managed to halt the phenomenon. The 'mass surveillance' that involves us, one formed by a global 'Pan-optimized' society, has brought an infamous definition of our times, whereas privacy is dead, as suggested already in 1999 by Sun Microsystems CEO Scott McNealy, suggesting us to "get over it" (Sprenger, 1999). This has been reminded to us repeatedly, among others, by Zuckerberg, who underlined how privacy is no longer a social norm (Johnson, 2010). Privacy, as discussed on the New York Times, refers again to the basic definition of privacy as 'the right to be left alone', describing the perpetual monitoring of our offline and online activities in the following way: in every moment of our lives we don't have any longer a place to hide, both in our private and public activities (Burt & Geer, 2017). Such point is interestingly further implemented by Floridi while discussing the conditions of the Covid Vaccine Certificate. (Sotgiu, 2021)

From a sociological perspective, as people roam (less and less) in the cities, they "seldom know that they are subjects of surveillance, or, if they do know, they are unaware how comprehensive others' knowledge of them actually is" (Lyon, 1994, p. 5). For Lyon, as stated in a more recent article, surveillance has become systematic: "routine and inescapable part of everyday life in modern times and is now, more often than not, dependent on information and communication technologies" (Lyon, 2009). This becomes even more integral with current surveillance technologies (Lyon, 2018; 2020). Such monitoring and observing reality is not only growing, but it is becoming what Lyon calls 'invisible'. If in the past all surveillance was visible and temporary, as in the case of soviet 'spying paranoia' (Verdery, 2014), as described, among others, in Tibor Déry's novels, today instead it appears as surveillance surrounding us has become mainly technological and especially discriminating.

Surveillance influences and alters our choices and the ways we are perceived. This is what Lyon explains as the growing issue of 'social sorting' (Lyon, 2003): with the tools becoming more and more remote, effortless and cheap, the individuals watched are immediately categorized and easily discriminated.

Beyond such devices, which are invisible and yet somewhat 'impersonal', for Lyon there is the "everyday practice [of surveillance] in which human beings engage routinely, often unthinkingly. Parents watch over children, employers watch over workers, police watch over neighbourhoods, guards watch over prisoners and so on" (Lyon, 2009). These

[19] Also, one may add the deep-learning technological devices that are being implemented to monitor, halt and disperse the COVID-19 pandemic crisis, concerning – beyond the already mentioned systems – laser-powered temperature sensors and state-financed algorithms to stop, monitor, warn and control potentially infected citizens. (Council of Europe, 2020)

considerations, made already in 2009, will be taken up in the vignettes that will be used as case studies and the everyday modes in which impersonal routines becomes indeed central in analysing and monitoring the very 'personal'.

As we will see, you may have nothing to hide, but again, may you have things to hide? Isn't it your right to own the right to your own personal, affectional treasures? As French post-structuralists have long ago discussed, reality is deceiving, and anything under a wrong light, an awkward filter, a convenient cropping may seem suspicious. Everything can be misinterpreted and is deceivable. Most of all, this is so when you have to justify an action that you never even considered that it needed justification. Social media are an evident example of the necessary involvement that it requires in order not to create a form of 'suspicion' on other fellow users. Indeed, few posts, little involvement and visibility only of 'old' pictures appear ambiguous: either one is totally involved, or not at all.[20]

When posting pictures, filters and effects are commonly used, with the evident desire of 'tricking' the image – indeed a magical 'philtre' such as a love potion and whatnot. This enhancement, especially in the case of advertisement, plays with a certain 'suspension of disbelief' on what is real and what 'masked'. Falsity is also an important issue, and indeed a whole technology is heading towards Augmented & Virtual Reality perception and deception of images and content. Such feature may 'transform' on a screen objects and environments, with the specific feature of being a 'live' interaction of what is real to the human eye and modified by the digital sensor and processor. A popular example can be 'toying' with the 13th IOS platform onwards, whose features allow users to 'virtually shape the natural world', promoting the initial stages of a technological progress where "the line between the virtual and the real world simply [doesn't] exist." (Apple.com, 2018).

Of course, this is an issue of 'digital modification' that goes on since the first graphic editor software, such as Photoshop, but also of the specific hardware and cinematic 'special effects' to modify reality, an issue being even raised concerning the extremely controversial issue of 'Deep-Fake' technologies, where faces and mouths of 'mediated' figures can be modified into 'appearing' to be saying or doing things that are actually 'digitally produced' (Porro, 2020). This issue is also at the basis of the 'Mind Bleeding into the World' argument by David Chalmers, whereas "mixing of the natural, the physical, and the artificial both on the side of the mind and on the side of the world that's in our future. AI augmenting the mind, virtual reality augmenting the world, and the two of them all in interaction" (Chalmers, 2017).

This is significant when considering how the devices that surround us thus not only invisibly monitor us, but actually might invisibly control us: not physically (or not only),

[20] Another example can be given by having to justify your movements and whereabouts to a police force, as in the recent Covid-19 lockdown, an event unimaginable in a democracy just a few months back.

but by influencing the surrounding environment, whether we engage with them or not. Smartphones in this perspective are no longer designed solely to communicate, but rather to store, capture and archive data: the pictures and messages that are thus sent to other phones are constantly exchanging, beyond our knowledge, information about us and to us. What becomes evident in this is that we indeed are living in an age of unreliability, where it is the non-verified nor controlled information that communicates for us, about us!

Such consideration appears worryingly compatible with the function and use of smart devices: on observation, the smart device is generally a dark object. Flat and lucid, it deceives attention – almost deflects light. Its design is nonetheless appealing, especially for more expensive models, though overall their structure is quite uniform through different brands. The imagery of Kubrick's 2001 Space Odyssey can be used to offer insights on such a condition: HAL 9000 represents the quintessential silent observant, vigilant and latent in its functions, yet never fully allowing the users to be at ease. Also, it is striking how the alien monolith resembles so precisely the Smartphone: a slim, dark, lucid surface. Smartphones appear quite evasive: this is significant especially regarding its functioning. While active, though with its screen locked, it makes no sound, hardly emits lights (very few models any longer have a small led light to indicate notifications). Contrary to other devices, such as computers (pc or laptops), that still today emit noises, flashes, beeps, and sudden fan activity, the smartphone appear – if not by close observation - by itself un-active, though perfectly responsive. [21]

We can thus understand such similarities with the predatory state of latency: a condition of dormant 'suppression', where the subject, the force, the 'secret' awaits. As we have seen, it is a masking technique, used through history as a means of divinization (shamanic and sacrificial) and obscure secret societies, yet becoming today so common and essential to social relations, almost the required feature of interaction, to the point of acquiring a required status for wellbeing. Therefore, this special predatory state needs some more clarification, first by giving further details on the already mentioned 'capta', and later by the analysis of the opaque algorithm system.

This problem is almost unsolvable due to the recent internet progress of secret, opaque algorithm systems: such recurrence of unknown, uncontrolled and potentially biased information about us being promoted, exchanged and sold. (Pasquale, 2015). For Pasquale, secret schemes and analysis take place at every internet navigation and smart phone/computer usage (not to mention credit card transaction, medical visit, highway fare, supermarket shopping). In the understanding of Pasquale, we all have (many) precise dossiers (in the likes of Stasi) on us gathering day after day data on our interest and cares, some valuable, some trivial, nevertheless being recorded and sold, 'behind the scenes'. Such schemes take place mostly unregulated and – even worse – without a clear understanding of their workings (not to mention transparency). For Pasquale, secrecy is

[21] One may note an evident shift is visible in the Apple computers that while being active had the 'apple' logo the back of the screen lit in white, while since 2015 it is substituted by a metal one, with no illumination. An answer to this issue has been found online claiming by removing the backlit logo Apple offered a 'lower profile' product. It also solved the issue of having in movies and adds the logo hidden because of its complications with lighting.

the modus operandi with which Big Tech companies operate, and indeed make money. Companies such as Google, Apple, Facebook/Meta, Twitter and Amazon use specific opaque systems of workings, so as to create "ample opportunities to hide anticompetitive, discriminatory, or simply careless conduct behind a veil of technical inscrutability" (Pasquale, 2015, p. 163)

But catching information does not only take place with the latent recollection of data. In a joint offline and online technological 'system' of control we are being watched and observed (keywords of the very secretive conduct) both while walking in the streets and while surfing the net, with a fundamental common denominator: we are somewhat conscious of this, and yet, for most of us, this form of 'indirect' surveillance involves us without ever actually 'touching' us (Giglioli, 2018). We do know that we are recorded, but the recordings, though being practically everywhere in cities, do not come to harm. We are actually 'left alone' by them, if not comforted, especially in case of crime or injustice. This applies, of course, if we abide by the security standards of our society.
Such 'security' measures are another point touched upon by Lyon, specifically focusing on the issue of 'fear' (Lyon, 2003), as a result of the post-9/11 War on Terror, that indeed resulted in alimenting the 'culture of fear' of having an "enemy within" (Furedi, 2019). Such attitude brought not only a growing level of security measures inside airports and borders, but in our streets and services, and thus creating a specific category of 'suspects' to beware of and to report, extending fear as an integral part of our modern culture (Lyon, 2020). Such manoeuvres become even more evident with the COVID-19 crisis, offering a glimpse of what could be a new form of 'fear-control', with temperature scanners and a generalised surveillance over those potentially infected, and the discovery of 'invisible' enemies such as the virus itself, with citizens filming and denouncing each other's 'conduct' disrespecting or being simply careless of the social distancing requirements, thus confirming the darkest (and yet purest) form of panoptic power.[22] The deceiving power of such system of control is based on the non-engagement or some sort of disclaimer on behalf of the citizen during its use: the continuous use of a pandemic state of emergency has demolished all previous precautions.

But even well before the pandemic, the modes in which our online conduct was registered and monitored are evident yet unclear: striking example is made by Google's ReCAPTCHA algorithm, a release designed to recognize and identify whether a visitor to a website is human or not. Yet, what is interesting is that since its v3 update automatically knows if a user is good to go or not, yet Google does not tell how he knows that; it is secret - an opaque technology. (Greenberg, 2014). Different yet similar are the functioning of free softwares and even 'freemium' apps. In the first, we may access programs such as the one provided by ORACLE, producer, among others, of free alternatives to the costly Word processor. Such corporations (previously known as Sun

[22] Moreover, a recent article (Couch, et al., 2020) lists the numerous applications by various nations and governments, underlying several devices used without the awareness of their citizens, as in the case of Italy with the use of temperature monitoring drones flying across cities without consent.

Microsystem)[23] though producers of open-source programs, function as data brokers of users' very data, alimenting the analytics industry and creating data integrations and matching. (Melendez & Pasternack, 2019)

With the freemium definition, we have a less subtle, yet just as lucrative example: freemiums are apps, especially games, which may be downloaded for free but offer purchasable services within it. Games, such as Candy Crush, would require purchases to increase the game's speed, or ease levels. Particularly significant in these games and programs is the desire factor: the need to continue the game paying for playing, or access/unlock features. Again, the contribution to the ecology of onlife secretive conducts relates to the deceiving modes in which these programs offer services, only to later 'demand the bill'[24]. People, users and citizens - thus the onlife participants - barely understand these systems of control, suspicion and desire surrounding them. More than that, as we will see in the case studies, nor does the onlife participants have effective options to resist the power of this data ecosystem.

Returning to David Lyon, it is important to underline how "the growing density of surveillance practices in everyday life is not the product of some capitalist conspiracy or the evil effects of a plutocratic urge" (Lyon, 2001, p. 2). Instead, beyond the fundamental 'non-clarity' of their functions and actions (that may lead to distress and lack of trust in authority) this condition is a result of "unintended consequences and negative dimensions of surveillance" (ibidem), leading to an actual a step-back of our human potential, creativity and expression.

This is evident since the 1996 "Declaration of the Independence of Cyberspace", published 'worldwide' by John Perry Barlow, where he made it clear to "Governments of the Industrial World" that the internet, or what it still was fancy to call "Cyberspace, the new home of Mind" was to be intended a perfectly free environment, where no foreign authority was welcome: "You have no sovereignty where we gather." Yet, such broad request would only find echo in debated programs of surveillance being set up between United Kingdom and United States, the first of which was ECHELON, operational, allegedly, since the 1960s, and coming to public attention only in 1998 (Ziccardi, 2015, p. 166).

Indeed, it is close to that date (October 1999) that Lawrence Lessing addressed the fore-coming dangers of cyberspace as a tool for control (at a distance). For Lessing, Adam's Smith 'invisible hand' was about to shape the market - virtually and physically, a precursor of the onlife ecology, transforming privacy from a right to a commodity. (Lessing, 1999).

Yet, the whole ecology of catching data is insufficient without the willing participator of the enthusiastic observer; sordid and sensational subjects, extending to voyeurism. Voyeurism gained the support of the internet, and what is more, it implies the union of all branches of voyeurism: is thus its pan version.

[23] Who's CEO, Scott McNealy, famously reminded the internet that " privacy is dead, get over it"(Sprenger, 1999).

[24] Another South Park episode explains this with clarity and wit, in "Freemium isn't Free' (S19E06, 2014).

Michel Foucault analysed society in a genealogical perspective, studying the bio-dynamics of discipline pursued and repeated first by the military and then the common people, in order to control and be controlled. The panoptic structure, as we have discussed, is a clever and cruel cage (Foucault, 1975, p. 224). Its power lies in the knowledge on behalf of the condemned that he is observed. Indeed, it is not really significant that he is condemned: any element inside the society may become subject of the panoptic power. Inside and outside: one knows there is some sort of control and surveillance, but the subject is unable to clearly define where it comes from. Curiosity, indiscreetness become central elements, alimenting the pleasure "in spying and punishing". (Foucault, 1975, p. 220)

From a contemporary perspective, technology seems to have mediated this control to a much greater scale, since the installation of the first surveillance cameras. The 'will to know' that characterizes society could offer an insight in the actual 'fuel' that aliments the Suspicion, Control and Desire formula this research wishes to grasp. It is not simply superficial, biased and discriminatory, but also never ending, as there is never enough security and control - a point taken up repeatedly by (Lyon & Bauman, 2013). Returning to Lyon, in the last twenty years surveillance has become a consumable good, and security systems a specific "urban fabric" that we have grown accustomed to, requiring and seeking it (a point that will become central in the case studies), but also an essential tool for virus containing and population monitoring. (Sotgiu, 2021)

But security is not the only issue concerning surveillance: in a 2014 article, paediatrician and professor Perri Klass had noted the parallels between our contemporary 'Surveillance State' and the Cold War children book 'Harriet the Spy' (1964). The book tells the tale of Harriet M. Welsch, an 11-year-old girl living in New York, whose aspiration is to become a professional spy. As a preparation for her carrier, she carefully observes 'the life of others' and writes down everything in a notebook. Klass notes how Harriet "is spying on domestic lives and private selves, not on public figures and official transactions" (Klass, 2014): it is the basic activity of strangers observing strangers, and more than that, recording them. Thus, the constant monitoring becomes indiscriminate: it covers all territories, events, and places.

It is hard not to notice the effects of the ever-watchful gaze in the recollection of news media: 'on-site' journalisms and 'live' immediate sources are no longer press photographers, but twitter users or simple enthusiasts who 'happen' to participate and document newsworthy events. We appear already by early 2021 perfectly 'accustomed' to film all our surroundings, to record and document any 'novelty' that surround our environments, having 'at hand', at any given time, a smart phone, with all its known features. Any worthwhile event is instantaneously recorded, filmed, pictured: almost naturally.[25]

[25] Such aspect becomes ever more significant with the neighbourhood watch reports of quarantine breaching during lockdown and the current pandemic.

The voyeurism of which two hundred years ago photographer Felix Nadar was accused by Balzac, having for the first time in history 'photographed' (and thus documented with unprecedented 'realism') the events of a Parisian party, is now a common practice. While since the early 2000s in most Asian countries shutter sound on phone cameras is mandatory and cannot be muted, specifically to prevent secret filming, this option is not required in Europe: instead, we are surrounded by what we might call an overwhelming practice of personal filming and recording. Videos are posted online with the greatest pride if becoming viral, representing more often than ever situations of friends, strangers, pets, and creatures in general in an extravagant and incredible situation – contributing to Vaidhyanathan's (2018) considerations on the odd and overwhelming 'Anti-social' elements of these media. YouTube reports of having 56.000 hours of videos loaded every day. To these, one must add all those that are kept on one's devices: it is almost impossible to participate in any concert, wedding, or social event of any sort without being filmed or photographed. In such highly uncontrollable reality, the conditions set by Simmel and Goffman for a Sociology of Secrecy seems to lose contact with reality. Indeed, as we will discuss later, we appear to be permanently and incessantly required to continue of impression management - in danger of being caught, filmed and recorded with our 'shields down'- and thus, as we will see in the case studies, risk of becoming ever more re-mediated. Part of an entirely different level of sharing, commenting and editing: to the unprecedented danger (or joy?) of becoming even an actual meme.

But the secrecy of the everyday does not regard simply the taking of pictures, it is a per se design for the intimate use of contemporary devices. While no common digital camera has a security code to access its memory card, all smart devices potentially do so. Why? Obviously, beyond the sole pictures, smart devices contain much more valuable information. But by protecting, with pins, codes, touch-ids such pictures, together with any other collected information, it imposes an unrequired emphasis on the picture itself. It is like storing in a safe both jewellery and trivial receipts: obviously, the latter are out of place, or worse, they gain an importance that was not intended.

Also, regarding software, an entirely different world of potential 'secrets' is unfolding, which includes messaging and internet navigation. In the first case, it is obvious that there is a clear change in communication, not simply with the use of a postal letter (which indeed had its envelopes to cover content), but between early gsm devices with their simple texting, as opposed to today's cryptographed instant messaging. While the early gsm device did have a short, usually 4-digit, 'personal identification number' (pin code) function, once the device was turned on, all content could have been read and consulted, as the keyboard offered not much protection other than the 'in-built', often universal, keyboard lock. It is as if the idea of trust, up to just a decade back, was considered differently: the same in fact can be said of early personal yet open access devices such as iPods and the above-mentioned digital cameras. Indeed, it has been reported by a Pew Research in spring 2017 that only 3% of smartphone users actually do not make us of any screen lock device, nor update their apps for security purposes. (Anderson, 2017).

The exposure to voyeurism, as recorded on the internet, is just on the increase and approaches infinity. If we have underlined before how clothes represent the curtains in

the windows of our persona, creating an initial 'layer' over visibility and control, locks represent the gates and doors of our homes, then concerning the internet we are naked and without resistance against any danger, attack, or harm; without any protection.[26] Locks are the first things we deal with while entering through our door, and the last we check before exiting, but now our life is unlocked. We will thus attempt to examine the various 'spaces' of retreat that contemporary life allows through a rather bold perspective, with the help of some insights about the ecology of onlife we are delineating.

2.2. Managing our onlife existence

If we have exposed the general elements of observation, control and monitoring that take place in our hands and our surrounding environments, we will now concentrate specifically on internet navigation: the use of social networks, the conditions of data mining and recollecting, the design of algorithms and the specific milieu of 'global monitoring' that the Data gate scandal underlined.

Shape and Shade

Once evident object of interaction and mobile communication, both verbal and textual, the mobile phone's features have become ever more sophisticated. The popularity and spread of smartphones across the globe should not surprise: already in 1995 Bill Gates was writing about a device called "wallet PC', soon to be entering our everyday life, brought by everyone everywhere, right in our pockets, along with keys and I.D, and cash: "The wallet will carry personal codes to open locked doors, do banking transactions at automated tellers, provide passport or driver's ID" (Andrews, 1992); (Gates, 1995). Such device would rightfully be interconnected to a highway of digital information about us and everything surrounding us, allowing an immediate and global access to 'everything'. Such machine has posed itself, in the words of McLuhan, as the quintessential medium: a prosthesis of the persona and his life. What will come, strictly speaking, the Smartphone, offers itself as a sophisticated producer of content, and at the same time container of this very content. Indeed, whatever is produced and consumed on a smartphone it done under the physical cover (curtain) of a screen. Such screen is not a two-way window, nor a transparent glass: it is a peephole into the world, though only looking in a single direction and where looking back is not desired.

Analysing further the latent features of a smartphone, on observation it is hard, if not impossible, to decide whether it is on or off without interacting with it. Because of this, as we have mentioned before, such machine appears very elusive. The screen is, when inactive, perfectly dark. Early gsm phone had also a similar feature, appearing inactive until handled or contacted, though some may recall how in general terms these devices

[26] Indeed, it would be an interesting research to question the feeling of not having any protection on ones devices, and why.

had a popular feature of a screensaver or at least the time displayed[27]. The gsm phone nonetheless was hardly as interactive and powerful in its use and features as its smart upgrade. Such features have all the basic elements to produce suspicion, control and desire, while apparently inactive, in other words while being, using Canetti, in a latent form. In such a state, while apparently 'inactive', it may potentially record conversations through its microphone, share its position though apps, pursue phone calls – with the screen off and without the need to interact with the device.

Operation and monitoring

In the same way, the smartphone's exterior aspect may hide its features and uses, its software may do so as well: its operating system may be monitored remotely, as well as the recording of any digital activity taking place. The smartphone gives and receives information, two words central in Mauss's gift-relation triangle (Mauss, 1966). It also returns, in the form of data collection and monitoring. This returning may be interpreted in the parable of the 'capta', as it is not clear to the user what information actually enters the device (Brunton & Nissenbaum, 2016). This takes place in the form of caches and cookies, two particular words and systems. The caches are understood plainly as the fast and temporary storage of information that the device, user or platform access in order to avoid a slower process of access (thus, the cache saves your email account and password as not to enter both at every access). The word in interesting nonetheless, as it is a storage, but also connected to the French cache (also cachet)[28] that is specifically a hiding place where to store things. Such reference is relevant comparing it to the notion of the custodis, as a spot, place and space that is monitored and taken care of (sheltered) rather than simply surveilled and protected. The cookies, literary a biscuit, is a sequence of information of the user memorized in the device, tracking actually the data of the user, the number of visits as such, links clicked, time visualizing, items in shopping cart (Medium, 2019)Both forms of temporary storage enter and exit information of the user from the device into the online experience. They offer information from when and where this very exit, and entry, has taken place. With the reduction of several uses into a single, highly protected and at the same time intuitive device, information produced and gathered becomes an 'invisible' data infrastructure. This reality has been described by Frank Pasquale as forming a 'Black Box Society' (2015): a condition that "concerns the increasing erosion of the privacy of individuals, leading to the escalated protection of the secrecy of commercial organisations." (Beer, 2016, p. 107). The users online become "private, hidden, and often unknown—processes become both privately owned and kept private" (Beer, 2016, p. 107), with companies producing and at the same time monitoring with greater 'technique'; they collect data on their users and at the same time "fight

[27] Only a recent Android OS allows the locked screen to display permanently date, time and notifications.

[28] Interesting how the "lettres de cachet" were the letters by which the French kings, through their police officers (who were originally the personal officers of the king, outside the legal framework that was controlled by the parliament) could arrest any person without a due process – a topic that came to interest to Foucault himself (Foucault & Farge, 2014).

regulations that would let those same users exercise some control over the resulting digital dossiers" (Pasquale, 2015, p. 4).

Devices have become personal objects that accompany us in our lives in every moment: one can observe how, since the generic and office-family desktop use, computers became mobile in the last twenty years. This is because of a consistent development of reliable and durable lithium batteries and the universal availability, first of Wi-Fi, and then a faster network service. As a result, these objects have become greater in sophistication and in storage capability, entering our pockets to guarantee an 'ad personam' usage. In the last ten years, another development of such technology is not simply their mobility, somewhat taken for granted by now, but rather their 'wearability': these objects, notorious for introducing the phenomena of the Internet of Things, allow "a more sensory connection into our informational environments" (Beer, 2016, p. 104); or, as Apple Watch advertise it, a 'haptic' experience. With such smart wearable products, the level of information-gathering reached a peak of connected personalization, culminating in biometrics and corporal analysis. At this point one can easily realize that the more these technologies become personal, the more sensible are the data they collect, including health conditions: the effect is that per design the user requires an even greater protection of his information, as in the case of self-surveillance – storing medical and health conditions.

The content of information typically collected over of a user is in fact secret: hidden inside such black boxes are "the means by which our lives are captured, but in which that information is protected by commercial interests" (Beer, 2016, p. 108). They presuppose that no-one may and should access it: rather, with an impersonal use of algorithms (which I will discuss further on) they offer an impersonal service. This impersonal use, such as cookies, allows one to question the basic assumption that it is not the content that manipulates the user, but rather the perverse modality in which some content is 'consumed'. The influential use of such devices is maintained if the user feels free to navigate within them, without the fear of being 'spotted' or 'monitored'. This is not only referred to governments and hackers, which, to the common user, seems an impersonal threat, rather to all those other 'close' peers: parents, partners, children, who may 'find out' what his 'package' of information hides. And it is this very package that the common user wishes to keep hidden. The effect is one of creating a very palpable condition where the user is afraid of having his 'data' observed not so much by a corporation, but their close peers!

Safe place

While it may be argued that any production is a lie of sorts (as in Wilde's notorious anecdote: whereas "Lying, the telling of beautiful untrue things, is the proper aim of Art" (Wilde, 1889)) and thus any artistic product is the result of a sort of jealous and side-lined production and process, with the required emphasis only on the final, approved 'piece', what concerns this thesis is the 'careful' ease in which the original source is produced and stored, even the most trivial one. Indeed, an evident example is the careless taking of dozens of selfies, only to choose, modify and share the 'best' one. The extra shots, in a general sense, stay stored, and because of their storing they stay safe. And because of their storing they're mindlessly taken. And because they are mindlessly protected they must be

as such protected in effortful manner from anyone viewing what has been mindlessly produced. The series of unobtrusive but burdensome influences and invasions of such 'data' that surround us every day can be further indicated through a comparison of 'traditional' printed family albums with the 'photo' galleries in any smart device. The first are physical photographical collections, available in every home, expressing somewhat intimately the record of family trips, holidays, birthdays, and events of all sorts, with images to be selected by their quality, not by their content: that is, when printed, very few images are actually discarded, and indeed the very value of the memory of each picture was quite different. These albums were to be shared with visitors, to the joy of most and occasionally the horror of some others, including friends, distant parents, even complete strangers, showing a glimpse into the life of a given family.

While on a first look, it might seem that these albums have been simply become digitalized: stored on a software/app photo gallery and distributed online on platforms like Facebook/Meta and Instagram. This is far from being the case. As evident today when taking a group picture, hardly anyone asks to view the picture from the photographer's device (this said, it is also hard not to have every member having a single picture taken per device). If the shot is worth anything, it will be shared through chats or posted online. The original shot – regardless of quality loss - together with thousands of other shots, is personal and stored away from all other viewers. No need to be showed or have the device per se scrutinized by others. Here one can notice the controversial heart of secrecy inside everyday life, built by technological design: what is intended to be shown is not the intimate, it is the public: and when not, if hidden – it where the hiding becomes more suspicious![29]

One may show many other small glimpses of daily life through snapshots, emails and WhatsApp. Nevertheless, they seem to fill only the void of intimacy, as they are hardly equivalent to family albums. McLuhan would agree: he wrote "the camera tend to turn people into things, and the photograph extends and multiplies the human image to the proportions of mass-produced merchandise." (McLuhan, 1967, p. 188). The object of the picture would appear the very message we are trying to replicate or store. Yet, by having the camera in our pockets, we tend to give it a meaning: but it is a meaning to the object, not the situation. The medium, again, is the message. Taking a picture, also, is not a form of exposition. Rather, it would appear as a refrain It is a control over an object exposed.

2.3. Concealment and control:

In contrast to the vague reframing within the back stage of our homes, a quite opposite development is the voluntary exposure of 'intimacy' on public forums, networks and social media. From a sociological prospective, an evident contradiction of this secretive life seems to appear with our everyday use of social media, one that appears to take on a global average of 136 minutes of our time per day (Clement, 2019). Concerning this number, one must consider the frightening reality of being a global and well inflated figure – especially during the pandemic. The most popular of such social media, with its declared

[29] Indeed, if any picture craves to be found within an apple device, is the 'hidden' pictures.

2.89 billion monthly active users, still to-date is Facebook/Meta (Statista Research Department, 2021): a company that indeed may be defined as the precursor of the online display of public (and at the same time private) life.

Confessing and observing

The social media, according to Bauman (Lyon & Bauman, 2013, p. 31) have long become electronical confessionals of every day life, evolving out of a Foucauldian priestly-based confessional-society. This, as we have seen, becoming a normative activity, has also become a very dangerous one: the observer becomes a passive watcher (Albrechtslund, 2008), controlling and controlled; he may be blackmailed and is blackmailing at the same time. The secrets, promoted as a tool to protect ourselves and our individuality, appear instead as potential tools to weaken us, leading to a particular form of Foucaldian docility: a new feature of the Panopticon, where the more one preserves secrets, the better they can be used against him as a form of control. This is evident in the use of social media, which has become a source of blackmail not of public life, but its opposite: we do not wish to show, but wish to hide what we don't want to show: this is the fundamental nature of these platforms. Indeed, we have become accustomed in keeping and monitoring the secrets of others. This is, as we have seen, is evident in the common practice of installing cameras inside our homes, monitoring our children's school grades with online school registers, checking whenever it is possible others' online/social activity. We want to see, observe and control constantly in a remote manner our environment, yet at the same time being terrified by being controlled by others, whether governments or private "spies". It is not simply a matter of sheer curiosity: we are all induced to constantly spy each other. So, we must face the necessity of creating an ethics of secrets surrounding us, as not to fall in the 'trap' of desire, suspicion and control surrounding us.

Theological confession

Regarding religion, especially for Catholicism, essential is the sacramental secrecy: it is absolute obligation (also known as the seal) to refrain from revealing what the penitent said about sacramental absolution (confession). Independent from any human authority, even judicial, as considered of divine right, it not only binds the confessor but also those who in any way had come to know of the secret itself (as stated in the Codex iuris canonici, can. 983). The direct violation of the sacramental secret by the confessor is struck by the excommunication latae sententiae reserved to the Holy See (can. 1388). An entire chapter could be dedicated on the subject of confessions, one even encompassed by Foucault in his History of Sexuality, as the obligation to confess is for Foucault thus deeply integrated into us. Introduced the 19th of April 1213, with the Forth Council of the Latheran, we see the practice of confessing becoming integral dogma of the Church, as stated in the 21 CANON: "All the faithful of both sexes shall after they have reached the age of discretion faithfully confess all their sins at least once a year to their own (parish) priest and perform to the best of their ability the penance imposed […] otherwise they shall be cut off from the Church (excommunicated) during life and deprived of Christian burial in death. Wherefore, let this salutary decree be published frequently in

the churches, that no one may find in the plea of ignorance a shadow of excuse. But if anyone for a good reason should wish to confess his sins to another priest, let him first seek and obtain permission from his own (parish) priest, since otherwise he (the other priest) cannot lose or bind him." (Fordham University, Medieval Sourcebook)

The spiritualistic connotation of cleansing sins can be found representative in medieval pilgrimage, while the confession in this light allowed a "therapeutic effect for the body" (Hepworth, 1983, p.74). The cure of the soul allowed thus a cure of the body. Again, the Manichean and somewhat Gnostic conception of intrinsic adamic (and in any case, primordial) sin becomes a constant that sheds eternal disgrace over mankind, allows a transmission of a collective sin, that puts in threat, if not constantly cleansed, the life of the entire social group. A personal seek of salvation, an individual strive for a form deliverance becomes the constant that separates the means to attain 'internal peace' from the tainted collective. Confession thus becomes morally desirable, though allowing some cathartic relevance for the individual, it required an institution that counterbalances ceremonies of degradation in deviance, and maintains the balance of social control.
In the catholic theology, truth 'demands' to grow out of ourselves, the core of secret truths cannot hold: it 'demands' surface, as a bubble of air, if held underwater. Nonetheless, "confession frees, but power reduces one into silence" (Foucault, 1976, p.60). The elements of conduction and seduction become evermore significant, whereas the seduction of these confessing tools – always at hand, instantly engaged with – promoted the 'surfacing' of the intimate realities, at any given time. They induce the user to behave this way, conduct his/hers experience and necessities. But confession is also a partial element of truth, it comes, as we has seen, hand in hand with the notion of what is stored, kept, hidden. The smartdevice yet is the keymaster of both – what is revelated (through apps) and what is kept (within the apps).

On the other side, Simmel notices who this very attitude is somewhat solved by releasing the secret, a revelation, indeed, "by the joy of confession" *(Simmel, 1906, p. 466)*: this underlines the basic distinction of secrecy: the natural degree that takes place in every day interaction, mostly unintentional, harmless and socially promoted by necessity; on the other side the desire of power and interest in keeping secrets, maintaining them and protecting them. In a more contemporary and practical understanding, the perpetual gathering of our life events as 'data', through continuous monitoring and observing may be somewhat halted without necessarily behaving secretly. Such every day surveillance, using an impressive number of devices that control us, online and offline, is as striking as evident: the bio ID, face recognition, iris scan, civil use of drones, audio-video surveillance of public transport that register conversations and networks of CCTV recording of any public environment. All these may be somewhat fought and deviated, but not only using means of counter-surveillance as mentioned before, and even, in accordance to this thesis, without necessarily having to live more secretive lives. The requirement to have everything stored, and indeed have systems and servers such as Google 'remembering all'. Hiding is associated with secretive conduct- such argument is somewhat related to the competing discussion by Frances A. Yeats on the Art of Memory

(1966) – whereas techniques of remembering and storing 'data' in the mind becomes tools, oftentimes of alchemic nature, of preserving power – especially latent power.

Latent secrets & societies of secrets

For Simmel, secrecy is founded on a mutual respect of each other's spaces (read also proxethics, developed by E. T. Hall). What interests particularly Simmel is how, and when, "the secret of the one party is to a certain extent recognized by the other, and the intentionally or unintentionally concealed is intentionally or unintentionally respected." (Simmel, 1906, p. 462). Yet, this seems a precursor of what we intend as privacy: for Simmel, secrecy is the "real sense" (ibidem), must be confronted with its practice of concealing and discovering. Secrecy is thus potentially (latently) a deliberate concealment, "that aggressive defence, so to speak, against the other party" (Simmel, 1906, p. 462). It becomes the purposeful hiding of information from others, which may have protecting purposes for the undefended, but which may turn into evilness and immorality, as it isolates the effect of immorality.
Secrecy, creates thus "the possibility of a second world alongside of the obvious world, and the latter is most strenuously affected by the former"(ibidem), a definition that can well be interpreted as a definition our virtual, online social world. Indeed, withholding from the many produces mystery and indeed desire to know.
This is a fundamental sociological technique, specifically in the form of commerce, whereas "what is withheld from the many appears to have a special value" (ibid, p.464). This can be evident with the recurring rhetoric of 'secret anti-aging formulas' as promoted by cosmetic agencies; or the secret behind celebrity's success: "Secrecy gives the person enshrouded by it an exceptional position" (ibidem). Every superior personality for Simmel has something mysterious about it, that grants him a particular influence.

Indeed, as Simmel noticed, secrecy is particularly seductive in children mentality, as what is secret, and thus not known from others, is as powerful as long as it is not unveiled. Then, it suddenly loses its force. This is the basic power, and main weakness, of secretive attitude.
Thus secrecy, for those who use it purposely, must be kept at all cost: to the extent that there is no particular secret to be kept, but the idea of it serves the purpose.

Self-discipline

"Severe self-discipline" (Simmel, 1906, p. 475) becomes central as an opportunity for "gradual adaption to the duty of reticence" (ibidem), just as we today are bombarded with the rhetoric of keeping our passwords and codes safe, so as to protect ourselves from invisible and eventual threats. But further contemporary parallels may be drawn.
Such institutions would thus constrain "the whole man", and thus underline the 'totality' of the their establishment (Goffman, 1961): reciprocity here implying a code of manners that must be respected, but also a series of rituals, which at the same time offer to the user an apparent "measure of freedom" (Simmel, 1906, p. 482) not evidently provided in

the "structure of the surrounding society" (ibidem). Secrecy thus offers autonomy, just as the secret society/social media does: indeed, retrospectively social media offers a particularly free environment, thus a sort of medium between everyday society (real life) interaction, described in the work of Goffman, and the dynamics of secret societies, as recollected by Simmel.

Social media would appear, as the word 'medium' presupposes, an in-between. The secret society in fact presents itself as a "secondary structure" (Simmel, 1906, p. 483), that mediates reciprocity (of both information and secrets), just as the digital and 'analogic' reality presupposes! In such onlife dimensional differentiation, a special society sets itself: secret but also social; it includes the whole community while excluding it at the same time.

Simmel notices how techniques of secrecy are not only based on concealment: society itself may promote an aura of secrecy that counterbalances and yet endorses the information. A secret may thus exist within society, as being very similar to the Masonic lodges, that were intended as a 'union in the union', but interestingly very similar also to contemporary social media services as Facebook/Meta.

In such environments, publicness may be truly promoted as such, but in reality, it is exchanging information in a concealed manner. Members/users may "seek 'weak' social attachments in order to protect themselves, and in the fact that they may avoid social relations when they encounter greater dangers within them than isolations" (ibid, p.478). Such an argument appears central in the way Facebook/Meta platforms are structured and have become so incredibly popular, with on the one side a fully public display of members, with names, pictures and posts; and on the other, an entire different 'backstage' dimension of private chats & intimate groups, where the other members may be integrated or actually excluded, or instead participate without being fully aware of the others presence, nor their hierarchy or dynamics – and the conduct accordingly of a secretive & normative existence.

While secret societies relate, in the study of Simmel, to an entire set of specific rituals, as in the case of the "oath of silence" (Simmel, 1906, p. 480) common to contemporary social media platforms is the anxiety concerning the way in which particular dynamics and indeed rituals may be betrayed, overruled, and even 'leaked'. In such perspective, a complete "absorption of a whole complex of external forms into the secret, the whole range of action and interest occupied by the secret society becomes a well-rounded unity" (ibid, p.481): such unity requires a specific "life-totality" and a "life-long loyalty" (ibidem), appearing, interpreting Goffman, as a 'total institution' of sorts. Though users would possess in any case an actual offline 'IRL' existence, such total involvement is potentially effective only in their online life. There, such interpretation of social media as a secret society would become evident: "even when it takes hold of individuals only by means of partial interests, when the society in its substance is a purely utilitarian combination, yet it claims the whole man in a Higher degree, it combines the personalities more in their whole compass with each other, and commits them more to reciprocal obligations, than the same common purpose would within an open society" (Simmel, 1906, p. 481).

Such considerations leads us into a more contemporary analysis on current social media, particularly Facebook/Meta, which in its very design, just as the society of secret, reproduce and replicate instances of secretive conduct.

Transparency and Secrecy on social media

The service of Facebook/Meta is a free platform and the company derives (officially) income from ads, including banners (display advertising). Users create profiles that (usually, and preferably) contain real-life pictures and a list of real-life personal interests. Users may also exchange messages privately (by messages or live chat, though the two have become practically one) or publicly, by 'posting' comments and mood status. The viewing of the detailed demographic information of the profile can be restricted to users of one's own friendship network, or also friends of friends, or made public to all web searches. Facebook/Meta users may choose to subscribe to one or more networks, organized by city, workplace, school, and religion. Famously, as compared for example to previous social media services such as Myspace and any other 'blogging' site, on Facebook/Meta you may not decorate the profiles using HTML or CSS (choosing themes, colours, music), but you may only insert texts and images. This choice, whereas the platforms graphics and the format are deeply standardized and have seldom changed (specifically, until it became normalized in the shape of a timeline profile), show the requirement for Facebook/Meta not to have users expressing their personal tastes and moods, as with a normal 'blog', but rather have them exchange information, communicating and interacting with each other. This explains the evident enthusiasm of the founder to make the Facebook/Meta experience a real and public one: fighting fiercely the use of 'fake' accounts and profiles, but even the use of aliases, caricatures, or false profile pictures. Truth is the key word in the platform's interaction, with real people discussing, liking, living and commenting other real people's lives – and indeed the potential secret for gathering as much capta as possible.

The reality of digital experience is a much-discussed theme, among many others by Sherley Turkle's work (Turkle, 2011). A perspective that interests this thesis is the notion of unreality in the everyday usage of these sites, and more specifically the existence that is lived behind the mask of publicness: the secrets that take place and are aided by the very design of these platforms. The necessity of having Facebook users being real and indeed proven individuals (that is, not specific bots or virtual spammers) is justified by many commercial advances: most importantly, advertisers paying for content want to have the guarantee that the banners are being viewed by actual people and potential consumers. Moreover, such necessity explains one of the most controversial issues concerning the Facebook requirement of a 'real' online experience: censorship.

Within the massive content produced everyday by the platform, a very solid control is kept regarding "nudity or sexual activity, hate speech and graphic violence" (Woollacott, 2018), and in the last years also episodes of self-harm (Hatmaker, 2019): such content is indeed taken down through users' reports or by an actual "Community Operations team, who work 24/7 in over 40 languages" (Bickert, 2018). While these

activities, that are effectively a form of censorship, are justified by Zuckerberg in a memo as necessary procedure "to balance the ideal of giving everyone a voice with the realities of keeping people safe and bringing people together" (Zuckerberg, 2018), another interpretation is that it is a necessary safe-guard for advertisement investors to maintain 'advertisement-friendly' all content of every page on the platform: no investor wants his product sponsored next to a post regarding violence on women or a severed teenager.

Censoring inconvenient content and thus 'hiding' it renders it clear that social media are designed and monitored not to express reality: only a certain version of it. The users' experience and behaviour within its realm follows from it, creating the false imagery of a transparent digital world that purports to show the lives of users, while allowing only a small, selected 'glimpse' into their everyday life. Indeed, in a basic analogy, users enthusiastically share pictures of their nights out, adding the who, why and when, mainly publicly, to such events. Yet, such fragment that is displayed is only the best 'possible' product of the various pictures taken in the night: the rest are stored, forgotten, hidden in the memory of the phone. There is no specific truth-telling involved, as defined by the concept of parrhesia, only a well filtered fiction: the rest is hidden from the public.

This form of internet experience is deeply different from the net and digital life-ideal, remembered as the blogosphere, in other words the beginning of the so-called 2.0 internet. The 2.0 new web-experience as such was popularized in 2004 by Tim O'Reilly after the dot.com crash (Lovink, 2007). This was characterized with a new conception of 'surfing' the net: users started to build their own platforms, forming a specific and personalized space of self-expression, described by Keen as a specific 'Cult of the Amateur' (2007). The blogosphere was (ideally) a non-profit attempt to offer an alternative media, a secondary source to the conventional information platforms. It is in this 2.0 web that, according to Lovink, the culture of self-disclosure came to be realised: the internet became "inundated with self-promotion" (Lovink, 2007, p. 38). As an ultimate stage of theatrical performance, users of the new millennia began describing their everyday events to yes, a public audience, yet a restricted one: the lucky 'few' experiencing the still initial stage of the web before the mobile 'outbreak' of internet. The identity behind the 'blogger' was still somewhat fragmented, profoundly arranged and 'personalized'. The 2.0 web interface was characterized by the first pre-themed platforms, easily 'constructed' and semi-guided by inexpert users (Lanier, 2010), aided as well by the first explicatory video-tutorials of coding: in other words, the 'building' of a web site was somewhat limited, yet the potential of expression, through the personal choice of colours, fonts, background, and general navigational freedom or layout was still evident.

Since the first enthusiastic attempts of Six Degrees (1997), social media developed with the aim not of building your own site, but of managing your contacts and communication, and ultimately, your very identity. The 'building' feature is practically pre-packed. The building up of a personality becomes fundamental and essential: questions as to 'build' yourself within the site, and never the site around yourself.

Attempting to create a new Facebook/Meta account in late February 2020, one notices how the site simply asks you to choose a profile picture and take a tour of privacy settings. By only navigating through the profile options, you finally get a chance of

forming yourself. A new feature though is particularly striking: you are offered automated images to fill the empty 'cover' images.[30]

Indeed, Facebook/Meta has opened on a global scale the issue of creating a public space, that nonetheless respected the user's 'privacy', whatever it meant (and indeed an evident contrast always transpired between what the producers perceived and what the consumers-users intended). Already in 2009 Zuckerberg had said in an interview: "You have one identity…The days of you having a different image for your work friends or co-workers and for the other people you know are probably coming to an end pretty quickly…Having two identities for yourself is an example of a lack of integrity." (Kirkpatrick, 2010, p. 200). In 'The Facebook Effect', the American author renders blatant the Facebook/Meta founders' attempt to create, in his vision, a "healthier society", by having users "behaving consistently among all our friends" (ibidem). Indeed, for Zuckerberg, "in a more open and transparent world, people will be held to the consequences of their actions and be more likely to behave responsibly" (Kirkpatrick, 2010). This approach nonetheless entailed several consequences.

Though being only an decade old article, the Wall Street Journal by Fowler discusses with a strikingly anachronistic content the 'damages' caused by going 'public' of specific 'secrets' that users have, willingly or not, shared online. Indeed, the author describes how "personal worlds that previously could be partitioned—work, family, friendships, matters of sexuality—become harder to keep apart. One solution, staying off Facebook, has become harder to do as it reaches a billion people around the world." In the article, there are brief descriptions of somewhat tragic episodes of users who, feeling protected by the privacy settings of the time, have nonetheless become inadvertently or willingly (read also maliciously) exposed in their 'secrets' by "friends, family and enemies" (Fowler, 2012).

The result, using Foucault's concept of conduct and governmentality – thus, how to behave and act - would appear extremely eclectic, if not damaging, on the user's identity formation. On such consideration we may also cite, along with (Goffman, 1956), (Pizzorno, 2007) and even (Mauss, 2016), who discussed the significance of masks, individuality and personality in the formation of character: what to hide and what to expose, but also how to define the I, differentiate from the other, while being nonetheless part of a 'group'. No matter such considerations, still by 2022, largely unanswered, Facebook/Meta's global popularity increases. If Zuckerberg's aim was indeed one of creating some sort of merge between off-line and on-line life (truly, an onlife) and somewhat subsequently the public and the private life, what it did create was — to use Goffman's analogy — an even greater 'theatre' of role playing and recitation. But this goes further: if what Goffman describes is the evident necessity in the modern everyday life of a backyard, where one can take off the masks used in everyday interactions, Zuckerberg has had ideally every user install a camera and a microphone 'behind the scene'. But what this thesis wants to claim is that the result is not a total deprivation of private and intimate spaces, but rather a kind of endorsement. Social media appears to englobe the everyday life of individual users not by hyper-realism, but quite the opposite:

[30] One may wonder if in a near future your info, generalities and preferences will also be automatically filled with suggested (retrieved?) information.

the digital profile has the pretence and requirement of being real, but it is nothing but a mask; it is a mask to be worn either in public or in private.[31] Indeed, promoting one's personality, tastes and talents on a global scale was already the ambition of the first, late 90s social media: Facebook/Meta's true achievement concerns its scale, stability and interpersonal connectivity among users. Zuckerberg, with his 2003 initial platform connecting Harvard students, and just before that with the embryonic attempt of Face-match, where females would be discarded or appreciated as a game purely based on appearance, had put together the quintessential element of the 'world wide web': communication and sex. From this perspective, Facebook/Meta proves its most powerful feature: the public profile is the mask justifying the means, the purpose is the interaction it creates. Secrecy, in other words, is as central as publicness. What goes on in front is only a smokescreen to all the 'background' interaction, especially if this implies constant of seduction and provocation.

This can be easily done both with public exposure and private messaging. As divorce lawyer James Sexton makes it quite clear in a Times article, "Facebook is the single greatest breeding ground ever for infidelity. Nothing that has come before — not swingers' clubs and key parties, not chat rooms, not workplace temptations, not Ashley Madison, Tinder or Grindr; no, not even porn — comes within a thousand miles." (Sexton, 2018) He defines Facebook/Meta as a cheating machine, an allegory that proved itself valid not only from the moment the platform became so popular, but also because its users could be so easily 'added' and both publicly and privately contacted.

Among the controversial uses of Facebook/Meta, that indeed appears to be mentioned in 30% of divorce court cases (Sexton, 2018), is not simply its massive, invasive and distracting use, but the possibility and temptation of reaching, discussing, flirting with past lovers, seductive colleagues and friends. In some cases, even perfect strangers can be indeed found and engaged with, thanks to 'communities' that after brief description, or the posting of pictures, help to detect people met in certain occasions, such as on metro, or concerts. This feature is particularly popular in universities and known internationally as Spotted. Even in our university, with almost 10.000 followers, Spotted UCC Library exists.

Sexton concludes using a common AA saying: "If you sit in a barbershop long enough, eventually you're going to get a haircut". In other words, with the Social Networks features being always at hand, the secretive conduct becomes per se the very conduct these services require. As we will see in the vignettes, hiding and exposing, monitoring and being monitored appear the common characteristics of their usage. Moreover, as we will see, with the smart mediums being always at hand the secrets only perpetuate: are created and sought endlessly. But how do these 'media' allow us to be more secretive, and suspicious and controlling over each other? In order to have an answer, in the following we will take first the examples of search engines and secret navigation, and then the so-called commercial liberty and market-led control devices, together with the thumbnail feature, revealing some elements of the algorithms system of control.

[31] An allegorical example for this is Zuckerberg's real estate modus operandi of purchasing, as in Palo Alto he bought "four homes surrounding his main Palo Alto residence" (Hoffower, 2019), in order to protect his domestic privacy.

2.4. What we do in the shadows

Search Engines and Secret Navigation

Obviously, it is an exaggeration to say that Facebook/Meta is primarily used: what cannot be denied nonetheless is that its potential is not one of public use and exposure, but of personal and private monitoring of others' lives, a question that I will discuss in greater detail in the case studies. Nonetheless, since the first versions of Facebook/Meta, popular posts sponsored false third-party apps that enabled people track whoever is viewing their profile. This is indeed very popular feature instead in other social media services, such as LinkedIn, or at the base of the entire 'popularity' system promoted by Google Inc., as the number 'views' of YouTube videos and 'clicks' of specific sites increase their visibility on online searches. Any user indeed is provided with a very well documented (and fundamentally panoptic) analysis of where such views and clicks have taken place, on what platform, what age and gender group, proving the ever-growing importance of data for market research (Beer, 2016) (Pasquale, 2015). This information is gathered with a number of tools that have in the last years been discussed and commented within a number of fields, especially regarding the invasion of privacy, and the subsequent 'tools' a user can use so as not to be tracked. Often, such tools deprive the user from his online experience: disabling cookies and general tracking of data actually denies you by now access to innumerable platforms, some of which essential for the everyday life of most westerners (GAFA products/services in primis). We are nonetheless 'allowed' to protect ourselves from an 'excessive' number of such 'monitoring', especially if 'third party', as proven by 'built-in' privacy protection features, as in the Firefox Browser. As I am writing, my current firmware 70.0.1 has blocked (by default) "700 trackers over the past week", of whom 548 were Cross-Site Tracking Cookies: these are defined as features that "follow you from site to site to gather data about what you do online. They are set by third parties such as advertisers and analytics companies" [32]

When accessing private browsing on the current Firefox feature (also known as incognito mode on Chrome) you are immediately warned: you are still being tracked. By clicking on the curious link "Common Myths about Private Browsing", where you are offered examples, mainly stating that your browsing activity is still available to third parties, and it does "not mask your identity or activity online". All it does is "automatically erase your browsing information, such as passwords, cookies, and history, leaving no trace after you end the session". Popular web search engine DuckDuck Go, known especially for not gathering meta-data of its users, made a survey in 2017 on 5,710 random Americans: results showed that "46.1% of them had used private browsing at least once, and 26.7 using it at least once a week. Their number one reason for using it is making embarrassing searches" (Duck Duck Go, 2017).

So, who uses such private features, and what is the purpose? Such consideration are not trivial nor to take lightly: already in 2014 K. Verdery, American anthropologist

[32] which raises the question: 'does Firefox have a list of all these Cookies? Is this where they make the money from?

making parallelism between the soviet secret police and the modern internet control, underlined how online users "know they are watched, but cannot avoid it without renouncing use of the internet altogether; hence, one can say they acquiescence their surveillance semi-voluntarily." (Verdery, 2014, p. 215)

As discussed before, what this proves is that rather than being afraid of third-party monitoring of sorts, what really users are concerned with is having their internet use monitored and 'discovered' by close peers. The secrecy of online activity is what private tabs require, i.e. not leaving traces to anyone who can physically access our devices. Kin, partner, co-worker: anyone you know.

Secret algorithms

The question of an actual aura of secrecy surrounding the content that is not only 'captured' from us but specifically aimed at us has developed practically parallel to the entire Social Media experience. It was Facebook/Meta the first to issue to idea of specifically aimed content in the news that one can, somewhat passively, view and consult. With the News Feed, introduced in 2006, thus practically in the embryonal state of the website, the various users could be informed of what changes, updates and opinions circulated among their 'friends', becoming thus as evermore interactive features. Yet, the modalities, the actual systems and algorithms that define what content is shared with who (as indeed, one cannot view at once all the updates of all his friends and pages) are covered by absolute secret. We do not know nor are given insights on how such a mechanism work. We only know that they are indeed present: some websites, such as the University of Cambridge project Apply Magic Sauce imitate some of the Social Media features in predicting personalities, interests, sexual preferences and other[33]. Such algorithms are essential not simply in offering the best possible content to users as to render the experience as engaging and fulfilling as possible on their Feed (an almost granted aspect, today): rather, it is one of delivering specifically targeted content, either as merchandize or, even more subtly, political ideas.

Such is the theme studied in the latest work of Ziccardi (2019), who indeed sees in the advent of the Cambridge Analytica scandal the global awareness of the actual value of the data we produce, rending clear the modalities of their use, though leaving a sort of 'trade secret' over their functioning. With the Cambridge Analytica scandal, defined by some journalist as 'Facebookgate' (Ziccardi, 2019, p. 111), it became a worldwide consideration how a private enterprise, of UK headquarters, could have an influence and impact on the entire US political campaign. Though Ziccardi underlines the actual involvement in the election was merely an allegation, what became - after the 'data breach' scandal - evident was rather the rapid and unpredictable distribution of the very users Data to third parties: their analysis and creation of psychographic segmentations, that would allow a prediction over user's interest and tendencies.

[33] https://applymagicsauce.com/demo

What these scandals allowed the public to understand was that all the likes and preferences submitted to such sites, that indeed are designed to expose your greatest secrets, are designed and incentivised in doing so: the aim is one of micro-targeting and "permanent persuasion" (Ziccardi, 2019, p. 120), as Antonello Soro, the successor to Rodotá as the Italian Guarantor For The Protection Of Personal Data, defined: to which the user is left completely in shadow. But the 'past' is still not protected: memory protection does not exist (Ziccardi, 2019).

Memory protection

In this system of locks and codes, the notion and assurance of an actual protection is hard to define. Actually, the idea of data 'protection' (and indeed, identity) itself has changed rapidly. These considerations return us to the discussions of Bauman and Lyon, regarding the "need to trust in the efficacy of surveillance devices to give us the comfort of believing that we, decent creatures that we are, will escape unscathed from the ambushes such devices set – and will thereby be reinstated and reconfirmed in our decency and in the propriety of our ways." (Lyon & Bauman, 2013, p. 90). As the two authors make it quite clear, there is never enough security, and indeed, over a certain limit, we may never do without it. However, this fear for control just generates further fear, just as surveillance requires more and more surveillance. In building up this network of security, stability, control and safety of information, a number of new features not only render our computers more and more sophisticated in protecting information, but especially containing it.

Apple Computer Operating System, for example, has since 2010 removed the possibility for users to securely erase all data from one's computer. It was an option known as 'Zero all Data', a procedure that "significantly decreases the chance that anyone who obtains your hard drive after it has been initialized will be able to recover your files. It is good to do this at least once before selling or disposing of a computer or hard drive. For greater security, zero all data two or more times. For high security applications, consider having the hard drive destroyed by a professional hard drive disposal service" (Apple, 2017).

Instead, later updates removed this feature, as "these options are not needed for SSD because a standard erase makes it difficult to recover data from an SSD" (Apple, 2015). Thus, it is now claimed that as it is too hard to recover deleted data with new technologies, you are no longer allowed to do so. Instead, today the support suggests, for one's security, to "consider turning on File Vault encryption when you start using an SSD" (ibidem). Thus, again, the message is to 'keep' all data, but protect it. Nonetheless, in a world where we don't know who knows our passwords or how easily are they given away, this is a dangerous development.

Here we come across a theme dear to Rodotà, the never-forgetting character of the data (Rodota', 2014): this is the truly worrying factor related to the 'agency' of our data in operating systems. Pictures, files, apps, programs data that define us, follow us, both online, offline, on software and hardware. They become harder and harder to control, not to mention get rid of. Unfortunately, because of their economic value, contemporary

systems appear to be concerned only in storing – aided by cloud synch and automatic back-ups. The memory of our data becomes the 'trap' into we have fallen, that must be constantly protected, monitored, secured and surveilled. Yet, it is a never-ending process, as every key is eventually breached, as the constant, incessant and recurrent need for security, privacy and policy updates show. Facebook/Meta, again, is the evident proof of the inability to totally control our data just by privacy settings: indeed, the platform is per se holder of some of the most effective surveillance licences, such as algorithms that recognize dust patterns on user's phone cameras, so as to associate users in the pictures and create connections (Pettit, 2018) .

Who controls which and which?

The panoptic elements of the mediums described appear at this stance almost reaching a plethora of instances. By referring to Goffman's understanding of the front/back stage, we will now discuss the elements of observation and control that take place in our social media, and the global exposition of our persona. As we will see, the conditions of separating the two instances appear almost obsolete: the social networks are designed to enter within their scope and extract the more information possible from the two – forming a central ecology of onlife monitoring, that takes place either online or offline, conscious or not.

We are witnessing in recent years altogether new forms of surveillance: if the original term implied the 'above' connotation of an 'eye in the sky', sociological (and artistic) studies are done on new concepts, among others, of Sousveillance. Sousveillance is an artistic and somewhat guerrilla induced form of 'observing' activity, promoted by Steven Mann, who has produced objects and devices to invert surveillance: ourselves become 'watchers', not only of those who observe us, but of all environments. And not only to watch, but also gain a sort of control, so as to be empowered to distract, avoiding and scrambling the images that observe us. As Mann defines it: "Surveillance happens when we're being watched and sousveillance happens when we do the watching." (Mann, 2016). For Mann, who has produced enthusiastic experiments on the subject, sousveillance is a further protection, a form of reconquering the agency behind the images that are being filmed of and around us.

The vignette twirls around the idea known in Latin as *quis custodiet ipsos custodes*? (who 'looks over'/guards the guards?), a point also picked up by (Allen, 2011). In the contemporary world, it appears that the always at hand availability of recording devices allow an impartial eye over events and abuses, especially ones related to authority. A much-debated case is the one regarding police violence, especially regarding video recorded on, from the historically controversial beating of Rodney King in 1991 to the current crisis over the death of George Floyd as a precursor of the entire Black Lives Matter movement.

The question of police violence nonetheless has been for long limited to the integration of what is known today as body camera technology, integrated world-wide into military and public forces. In the UK, since its initial tests in 2005, such equipment by now has become a permanent feature of police officers (Cooper, 2018). The Security Industry authority defines these features as a '"hands-free' video recording (and possibly

audio recording) device that is worn about the person in order to create a visual record from that person's point of view". The question nonetheless inevitably arises, even if one is trying not to fall into some ridiculous rhetorical trap: is this a surveillance of the surveilled surveilling the surveillers?

Though it sounds as some sort of quip, one may put some emphasis on the irony of these forms of 'veillance', resulting in some sort of excessive use of monitoring itself. To 'watch', deviating from Foucault's 'optic' consideration, becomes itself a somewhat unsatisfying and limited word, using instead a term like 'wake', thus focusing on 'vigilance'. Are surveillance and vigilance the same thing? One perhaps may come to the point of defining surveillance as some sort of active monitoring, while vigilance a form of 'prudence': again connected with custos, thus protect what is seen from being 'abused'.

Again, the physical object that allows and produces refrain appears integrate with the use and abuse of the smartphone use. Moreover, along with other technologies that are being designed and developed, such as shades that apparently blur the users features before CCTV cameras (Morse, 2019), are all interesting forms of resistance, nonetheless extremely unique and, inevitably, suspicious. Among a crowd of well monitored individuals, wearing such forms of shades is exactly the thing that draws attention to whoever is surveilling. To hide is to meld within the crowd, as Canetti noticed. We appear, in this perspective, allowed only to conform.

2.5 The onlife engagement:

In this chapter, we discussed how smart devices appear in contemporary life the quintessential object that blurs between the online and offline dimension. As the Goffmanian concept of the go-between non-person ((Goffman, 1956, p. 150), a smart phone is a hardware mobile medium that accesses, anytime and anywhere, our more private features – becoming a kaleidoscope device of front and backstage.

We have analysed the fundamental features creating the contemporary milieu of secretive conduct in the onlife existence: it is one of a virtual and AFK reality being constantly under some sort of watch, from basic security measures, from CCTV remote recording to ever growing drone surveillance, combined with face recognition technology, and online tracing and tracking algorithms, rendering the lives of every citizen constantly watched and monitored – an indeed total institution of control, whereas we users appear subject and inmates under constant supervision. In such light, smart devices appear as integrated tools: on the one side, they offer a safe space where the information gathered by users (pictures, web searches, chats) may be stored and protected, on the other they themselves through their opaque and fishy system appear to increase the aura of secrecy of the surround environment and fellow users. The internet use, navigation 'capta'-analysis, along with the perpetual surveillance docility schemes, that have all been

mentioned and consulted, have all become central characteristics of the current onlife dimension, to which we will now offer some sort of glimpse and observing features.

As Floridi, (2015) proposed, within the mundane habitat the onlife reality embraces the public and the private (front and backstage) indefinitely - combining the online existence with the somewhat anachronistic "offline" disconnection - two elements that are now inseparable and become the core elements of its ecology. This condition is ever more significant in with the premises of secretive conduct that also appear to permeate all instances - hiding, seeking, monitoring, and further controlling. Within this milieu, secretive conduct is promoted, as seen, in multiple instances. We have begun proposing the technological instances that re-propose and set the terms of this very conduct (with the smartphone *dispositif* as the fundamental conduit). As described, the smartphone represents the quintessential aspect of suspicion, control, and desire. It is characterised by an opaque functioning, an unclear and unscrupulous modality of searching and communicating. It is constantly in the user's pocket, functioning both online or in "airplane mode" - offering services of surveillance and monitoring - containing our most private information and offering a window where to express and share these, at the tip of a finger, to anyone-anytime-anywhere. By having such tool always at hand and accessing (in a personalised modality) its features at any given time (smartphone use has become normalised at any given occasion, from social, dining and even education attending) - we abide to a form of Goffmanian front and backstage alternation - heading back and forth. Anyone owning a smartphone, and thus more generally participating in the onlife phenomena (to which it is seriously complex to evade), partakes to a certain extent to the ecology of secretive conduct. This is a technical establishment: the smart tools are designed to produce and store pieces of information in such a way, and such ways produce an effect that has been here hinted and will be analysed further in the case studies.

Returning to the metaphor of concealment, the deviant triangle may be conceived in considering the desire of knowing to be as powerful as the desire to hide, and the imitation of such conduct in light of its overall availability. The Gyges affect in such perspective is not simply a fable over the dangers of unaccountable secrecy, but what would you do if you possessed a ring that allows to become invisible and thus act secretly: well, the smart phone apparently acts as the very ring. But more than that, rather what is the subject going to do knowing whoever is before him potentially owns or may use such ring. As discussed in the latter case studies, the deviant perspective strikes for the entitlement of the actions of suspicion, control and desire that appear produced and promoted by the very smart phone's 'fishy'/opaque nature.

But Smartphone is not only sending messages, but producing messages would be a definition for smartphone given by McLuhan today. The smart medium would appear as message because of the delivery of secretive conduct its use implies and requires. The device becomes the channel in which any message may be transmitted, both personally, digitally, physically, and even psychologically. By its very presence, because of its features, content and potential, it has a total social effect, changing the public attitude towards a deviant behaviour: while it is part of the norm to hold secrets, protect them, codify and cryptograph its content and cryptograph, less crystal is the conduct of wanting to 'fish'

them out, fear them and control them. It appears deviant nonetheless not the desire, the suspicion, or the control of this conduct, but the modalities in which one does so. The discipline and docility, that will be discussed in the conclusion, would appear in accepting others' secrets, even our dearest ones, as to avoid a public skimmington ride, where all social and criminological aspects of the device, as in the movie Perfect Strangers (2016), are revealed.

The smart device-induced secretive conduct appears concerning not only the protection of content, but the access to its very content as well. In the understanding of Goffman's work on total institutions *(Goffman, 1961)*, in such systems and condition there is no longer a net distinctions between the front and back stage. Everything is in constant observation, nakedly revealed *(Giglioli, 2019)*. We as users turn into the perspective of the intimate. Examples aid such concept: as we said, the screen allows only a one-way view of content. This is interesting while observing others in public spaces. Within a small minority of paper readers, newspaper and pocket edition books, occasional 'gameboy' or even knitting enthusiast, all others are either immersed in thoughts or in their screens. No easy conclusion may be proposed on what they are viewing of consulting, if not thanks to sudden or dramatic expressions. Ways for falsifying and deceiving paper content in public can be questioned to any newspaper seller: inserts hidden among other magazines, covers of soft porn novels twitched with the ones of classics: the public had innumerable ways to veil the content of their consultations. Today, such actions are for the most unnecessary. Though the acronym NSFW (not suitable for work) is popular and an important warning against 'indecent' content (used especially in chats and websites), it is indeed posed a working related environment, where screens and history may be legally monitored. In public, AFK meat-space environments, far from prying eyes, the concept of decency is less straightforward: the device offers privacy in the most crowded environments, intimacy in the public realm. Such privacy becomes central in our argument when the 'private space' of interaction promotes deviant behaviour, as in the case of infidelity, trolling, cyber-bullying, and hate-speech.

Such behaviour takes place in private but at the same time shows secretive character instincts: the 'right to be let alone' is taken advantage of: it becomes central for allowing such conduct to take place. In such perspective, the device offers chances of secretive conduct that offers strictly a cynical use, in a Goffmanian sense, of pure "self-interest and private gain" (Goffman, 1956). Such conduct would take advantage of the front stage appearance, manners and goodwill of the interlocutor to act in the interest of their private/back stage that the smart device allows. In such perspective, the backstage is lead to the front: the single personal usage of the device allows one to be in the company of a friend, colleague or a partner, while at the same time chatting with the lover or another peer. While it is obvious such 'foul' conduct have always existed, it is the curious evident lack of questioning of the very action of chatting and communicating, verbally and spectacularly, among physical peers that the next section will engage with. Indeed, the very design of the device allows such conduct, with a multi-level interaction and communication of apps is designed to allow. More than that, the device has entered the

everyday so profoundly in its availability, permanent connection and social acceptance of its use in practically any situation. If public transport still announces to key the tone of voice during phone calls low and sound on mute, the typing and consulting offers no distraction or annoyance to fellow travellers. As such, one may claim that it is socially accepted to write to others while having a conversation with someone, hardly we may ask who you are writing to. Though this is a loaded and generalized statement, it does require a particular consideration in light of Simmel's considerations of 'reciprocal discretion'. Secrecy becomes central and essential for lacking of exchange of what is been said, and the mode it is done. By chatting to a partner having the lover present, a whole set of conduct of 'having an affair' is required that goes beyond simply 'sleeping together'. One must not simply 'lead' (conduit) a specific performance with A (the partner) while communicating/flirting with B (the lover), but must and may do so contemporaneity. Any message, as we have seen, picture, notification that may reach the receiver at any given time, may also be consulted at any given time, given the discretion of B. Because of this, smartphone appear to be based on the abuse of reciprocal discretion.

The effect is one where there is an evident menace to the concept of the backstage in Goffmanian terms: the onlife does not appear to offer any relieve, where to take off masks, release the pressure of publicness: the public is always watching, the private is always hiding. The onlife thus proves, among other things, its potential of a total institution. In the next and final part, we will engage in the practical examples that delineate the ecology of secretive onlife conduct we have tried to depict and recollect across the years of this research.

Part III. Wanting to Know, See and Control Without Being Known, Seen or Controlled

If in the previous section we have introduced the theoretical conditions of the onlife ecology, with its dynamics, spaces and interaction, here we will attempt to enumerate significant examples of secretive conduct and its effects in the everyday life, forming an above stated milieu of 'Suspicion, Control and Desire'. Such condition will be analysed through the use of social vignettes as case studies, gathered through a sociological and ethnographic observation since the beginning of the doctorate (2015). As we have discussed in the previous part, the occurrence of secrecy in the everyday life is constant and entrapping: it never leaves us, as the online no longer leaves our persona. It enters all spaces and embraces, potentially, any behaviour – and conducts further elements of constant suspicion, control and desire. In this section, we will look more closely at the users involved, active partakers of the onlife realms – and the secretive conducts involved, and the social harms that arise from it. These vignettes focus on the criminologically significant 'light-hearted' use of schemes and personal devices that the subjects have regularly made use of, with simple tools and a number of justified behaviours for using them – in oftentimes invasive and harmful manner. This is particularly interesting for my thesis as these forms, digital and physical, of control are generally not 'perceived' as

particularly invasive, but actually appear handy, convenient and useful, a condition that has been already labelled as a form of 'Participatory Surveillance' *(Albrechtslund, 2008)*, a term I will try to integrate and possibly update. As proposed in the methodology, this theoretical research will engage with the spirit of 'data' etymologically and semantically meaning something given, thus a 'gift', instead of specifically producing 'capta' such as 'information'. The thesis has pursued the issue with the use of 'informal' social vignettes as representing episodes of suspicion, control and desire leading to instances of abuse and harm – either directly or indirectly. These are noticed and gathered in everyday life through informal conversations, glimpses of impressions, aided with relevant scientific contribution: they indeed offer the 'underlying' demonstration of a globally accepted use of personal devices in aid of an 'invasion' of secrecy in our everyday lives, as means to control our existence, creating a perpetual condition of desire to know and possess information of what is manifested and what instead hidden from us.

I have divided these social vignettes into three sections: a) Observing others without being observed; b) Invasive tools fulfilling the Desire to Know; c) Resisting the perpetual memory – whereas (a) will deliver vignettes that represents events in which surveillance became central though incidental and often normative through occasional monitoring of basic feature within apps, such as the 'Last seen' features; or by observing partner's traffic behaviour through smart car features. The individuals would engage in suspicion, control and desire with a trivial motive, hardly considering the consequences, the consideration, the assumptions raised by such actions – with dramatic response on behalf of their partners and kin. In (b) we concentrate on the desire factor, intruding into the lives of others with use of mediums at their disposal – regardless, again, of implications and consequences and the direct involvement of dismissal of trust. In (c) we look specifically at the adiaphatized conditions of monitoring and distributing secretive conduct online – through platforms and instant messaging applications – replicating the dynamics of suspicion control and desire in the onlife – replicating, duplicating and spreading elements of subjugation and control, as in the form of revenge porn or meme generation.

Such cases represent instances of control, abuse and social harm – in the most mundane and 'softcore' dynamics: they represent nonetheless central assets because they are so trivial, yet central.

In writing these sections and the gathering and analysis of the 'information', I have attempted to engage in a specific 'art of listening' and observing the everyday onlife reality. As some sort of sociological flaneur, I have 'caught glimpses' of daily events - the simplicity by which the secretive conduct takes place, and may become abusive. As mentioned in the methodology, there has been no use of intrusive recording equipment, but simply relying on dialogue, observation and memory. They are described and discussed here with all references and names changed, with no direct quotes or actual formal questionings. Indeed, though striking, they are not only true but also not particularly peculiar or unique: they appear as glimpses of secret attitudes and tolerance to secretive behaviour in a world apparently unaware of its danger and possible abuse. Incidentally, two fundamental features of secretive conduct have been discussed in detail: couple relationships and parenthood. The way in which these two conditions have struck

me so deeply may relate to my becoming recently committed partner and a father, but they are also the conditions that for Simmel appear central in the formation of a "right of secrecy" (Simmel, 1906, p. 462) that may become abused and harming. Another is friendship, which I do not mention directly, if not in the actual first-person testimony of some of these events, shared with me in – friendly faith and good manner, indeed, a truly reciprocal form of analysis. Also, the very fact that some of these events have been shared with me underlines some sort of indiscretion against the 'other' person, and thus implying some sort of secretive conduct taking place and directed towards others, who in fact were perceived as acting in a secretive conduct manner. I have nonetheless analysed events 'perceived' from online behaviour, that are also relatable to 'friendship' as an abusive form of secretive conduct.

3.1. Observing others without being observed

CASE 1. Monitoring through WhatsApp's 'last seen' feature:

The question of some sort of unconscious surveillance that even possesses an element of 'game' to it can be related to several neologisms. Related to social media, already in 2008, Anders Albrechtslund noticed what he called 'Participatory Surveillance', underlining the "social
and playful aspects surveillance" (Albrechtslund, 2008). Users are 'empowered', rather than violated, by the possibility of observing each other mutually (crimes and mischiefs) and sharing (abuses). Indeed, Albrechtslund shows how through webcams "the building of subjectivity and of making sense in the lifeworld" (Albrechtslund, 2008) can take place; indeed, a personal exhibition of user's content may bring them to claim their personal copyright. This thesis agrees with this perspective. Without making claims about surveillance being good or bad per se, we recall that our quest is asking the question of whether it has become or not an integral part of our society (Lyon, 2018), with secrecy being a central 'reason' for this taking place. We will now see the first case study of this work, taken place around 2016 in Ireland: the events have been referred initially at a dinner among room-mates, where the conversation shifted to the following events: all peers would engage and exchange opinions on the matter. Its features, as we will see, involve the ease in which control, observation, and 'desire to know' may take place: both in the modes in which WhatsApp is first used to 'build' relationships, and the modes it perpetuates the natural 'flirting' conditions, creating fantasies and 'obsessions' about the secretive lives taking place: the secretive conduct and the 'perception' of its counter.

Onlife ex-pat: This particular event involves of couple of late 20 year olds, in the 'early stages' of their relationship. 'Julia' and 'Karl' are trying to get to know each other and communicating through WhatsApp. The two have met a night out a few weeks before, have exchanged 'WhatsApp' contact', but no social network profile. Being both working ex-pats, they do not share many friends and manage to meet either incidentally in local clubs during nights out, or by communicating on WhatsApp. The ex-pat condition is particularly significant in the milieu secretive conduct, that indeed one can claim to

represent the pro-forma existential condition of all working abroad European citizens: though this is no place to enter this highly complex consideration, we can briefly mention the modes in which secretive conduct replicates in the modes in which European citizens interact and exchange within an onlife reality, highly mediated and hyper-connected. The WhatsApp mode of interaction is exemplary: as by device default, a phone number is required to connect. The number nonetheless, to which the user receives an activation code at the first access, is not strictly connected to the 'mobile data' provider. Thus, as easily noticeable, most ex-pats would seek a local internet provider in the country they've moved in while maintaining their original phone number. Thus, while phone sim card number would be from the provider in the country they work it, their WhatsApp number would be usually connected to their original residency Spanish, French, etc.,

In regard to the ex-pat onlife secretive conduct, by 2016 handing over someone his personal WhatsApp contact did not automatically permit phone conversation, only typed WhatsApp communication. This relates to the perception of open and free communication, while in reality the user is constricted to the single app - a sort of McLuhanian servomechanism: moreover, the medium is the message, and this is exactly where development of Julia and Karl relationship encountered difficulties.

Cat and mouse chase

As informed during the dinner, WhatsApp (again, the only effective mode of communication between the two) formed the specific of the particular mode for their meeting: through the use of the app, they would send each other 'selfies' during the night out, 'softly' inviting the other to 'find out' where the other was, and thus apparently 'invite' to 'chase' the other. The chasing game oftentimes required the exchanging opinions among friends, recognizing the design and features of club or pub. Through this game, never 'officially' nor 'directly stated', they appear (to each other and for the few common friends) to incidentally and indirectly 'bump' into each other. As understood, after a few occasions, when the 'meeting' does not take place, though both are out, Julia has actually - with great efforts - sent Karl her specific GPS live-position, as to make the unofficial 'game' easier. This 'cat and mouse' chase had being going for a number of weekends, apparently. Such condition is already extremely valuable to our study, especially considering the panoptic features of this 'relationship-building' – the trust around sharing each other's whereabouts, the people involved, the places visited. Nonetheless, the modality of their device use becomes even more complex, and discrepant.

By the night of the dinner, Julia admits it's been a while since the two have managed to meet. After showing older location-selfies and playing with the friends the "do you recognize the place" game, Julia admits the relationship is becoming furthermore complicated. She claims the two chat a lot, balloons and balloons of conversations are shown on the screen of her device, some of which with very passionate and romantic content, proving some sort commitment of his behalf 0 these as all have been read aloud to the entire party. We can already note the modality in which we are shown, and can be shown at any time, the personal and private glimpses of intimacy in a recorded and chronological fashion – an imaginable condition without such a fundamental tool for

monitoring and storing conversations. *Scripta* non only *manet*, but may be perpetually displayed. Indeed, further in the conversation, while together, the two are, according to Julia, in perfect symphony. She claims he is also happy – given the transparent considerations over their relationship: yet he has never shared his position and does not make it easy on 'her' to find him. Such aspect would appear somewhat trivial, if the entire conversation would have not shifted on the 'last seen feature' on his WhatsApp profile. The conversation appears thus valuable as a social vignette.

Timestamp control

The *last seen feature* is known as 'timestamp', introduced in WhatsApp 2014, soon after it was acquired by Facebook/Meta. It was first compulsory to all users and later updated as to protect privacy, and thus with the 'disable' option. (Sigauke, 2014) It is distinguished from the online 'feature', defined respectively as "Last Seen and online tell you the last time your were using WhatsApp, or if they're online. If a contact is online, they have WhatsApp open in the foreground on their device and are connected to the Internet. However, it doesn't necessarily mean the contact has read your message. Last Seen refers to the last time the contact used WhatsApp. Through our privacy settings, you have the option to control who can see your Last Seen. Please note you can't hide your [sic] online." (WhatsApp Inc., s.d.).

It is indeed an option that a user may not provide, depending on his privacy setting: nonetheless, a user may not be aware of its effect and use it is done by other users, who may analyse what he may be doing: a 2018 article on Mashable describes a condition practically identical to the one witnessed with Julia: the interviewed was "checking this particular feature on a daily basis in order to gain some kind of insight into his night-time activities." (Thompson, 2018).

Control obsession

Apparently, Julia was making all sorts of consideration, not only on Karl's whereabouts, based on the information he was sending; but to whom he was writing to depending on the time he appeared online. Indeed, on WhatsApp you may not only see where someone is, but whether he is typing. Julia appears obsessed by this feature, especially when Karl apparently would type, but not send he anything. She did not know if he did it on purpose, but she did come to the point of believing so. Also, the time he would spend apparently 'idle' online would be thus compared by Julia with common WhatsApp contacts, so as to judge and consider to who he might actually be writing to. It became clear that Julia did not trust any longer Karl, not simply because he would not reply to all of her messages, but appeared online as wondered if he was chatting in the middle of the night with other girls. She came to the extent to try to navigate in his Facebook profile through a common friends profile – as they had not yet requested each others friendly. This is evidently a common feature, and indeed a problem perfectly at hand to any WhatsApp user: the suspicion of something being wrong and the desire of knowing what is happening on the other side of the phone may become an 'uncontrollable' obsession.

The web offers even a number of somewhat easy 'hacks' that allow users to remotely track, control and observe in detail the activity of a user, using all 'public' information, as in the 'Internet Protocol Guide' (White, 2019)

Interestingly, this condition that for one user appears as a "torture", may actually for other appear as "an unobtrusive way of assuaging your fears without bothering or confronting someone." (Thompson, 2018). Indeed, through the Last Seen feature mothers may find it "very useful for checking that her daughter is safe and well without disturbing her at work." (Thompson, 2018). It becomes a means to produce an onlife judgment of someone considering his 'online' activity: it is handy and useful, fast and simple. What is important, nonetheless, is the danger of making assumptions on what is going on, yet not being actually able to ask in person – a point central also in the study of friendly social media surveillance *(Horst, 2020)*. As noticed in the social vignette, Julia would never admit of making these assumptions, with the fear of being mis-judged by the boy and so mis-understood. Yet she could not resist the temptation and had no problem is discuss this with her friends, asking advice and opinions. She knew that Karl would not agree with her monitoring, yet she never considered actually not doing so: everybody else apparently did so, and would come up with the same conclusions: Karl is hiding something.

The technological medium with whom Karl and Julia exchanged information while chatting appeared actually participatory in their relationship: it was apparently the tool for confessing, admitting, flirting, with a later 'In Real Life' an unrepeated form confidence. Again, McLuhan would simply nod at what appears as trivial (but is unfortunately not): the medium is the message, and without it the message, even a loving one, seems less effective (or harder to replicate). The existence of two peers, communicating online, and thus briefly meeting, becomes arranged around what is from a single view/screen observed and potentially promoted as such to maintain an 'aura of secrecy'. The control again of the information exchanged - from the whereabouts to the actual intimate confessions - revolve all around a number of themes. The most obvious is the technologically induced environment, as discussed by Turkle (2011), of deciding, by this shadiness, to underline a non-'involvement': in the intentional taking advantage from the very shady, superficial yet at the same time engaging set of tools that the smart phones, and indeed the very WhatsApp offer, in order to appear- at least to the mind of one - of being partners, or potentially becoming one - though having no intention whatsoever. Such condition becomes explicatory in the next case study.

The second theme is the inevitable conclusion that indeed Karl is hiding something, or he's simply completely misinterpreted. Such prospective, that indeed during the dinner seemed almost to be more definite, the secretive conduct is rather produced by Julia, and she is also the controlling figure: again, the secretive conduct reveals its ambivalent and ambiguous connotation. It is never clear, as secrecy itself presupposes, who is the victim and who is the prey when secretive conduct is involved, and thus no definite clarity nor 'transparency' exists within couples. In this perspective, the dichotomy appears of an effectively dichotomist onlife reality: we are only offered, as

criminologists, but even as friends and kin, a single perspective of what is perceived as reality.

This case study has discussed the eventuality of perceiving secretive conduct, considering the devastating effects in killing off relationships since the very beginning. The perception and fear of something going on 'in the background' - conducted in secret - becomes integral in the very use of the devices that are being used. Again, the medium is the message, and thus it appears that Karl and Julia could not take their relationship further because of the conduct they picked up in forming their relationship. The intimacy gained by chatting was no longer reproposed in face to face, even in the most intimate conditions. The medium became the fundamental tool of engagement, yet it is not a clear service, and its features are devastating without a proper awareness concerning its conditions of use. Within the onlife ecology of the secretive conduct, we see the evident formula of suspicion, control and desire replicating itself. Julia wanted to be with Karl, but not let him know it too clearly, and thus perhaps acting too shadily. We have tried to describe ways in which Julia (and possibly Karl) could control and observe each other without the other knowing, in what appears as a perfect Panoptic condition. WhatsApp is fundamentally designed to allow such a feature, promoting such a condition, and indeed opens a wide range of other possibilities where this has become possible.

The timestamp in this particular case proved the 'deus ex machina', showing the discrepancies of their shared lack of communication and understanding. It is worthwhile mentioning that even other Apps - and even Signal itself, albeit being the most 'off the grid' system' - use certain versions of timestamp: it is thus a feature and a system of secretive conduct that can be replicated through devices across platforms. To the best of my knowledge, it was WhatsApp (and especially its Facebook/Meta acquisition in 2014) to render the timestamp feature so popular and apparently pro-forma of the messaging experience. It is thus a fundamental feature, a normative aspect, through which secretive conduct thrives.

This discrepancy between Julia and Karl leave nothing but an incognita. We may not know what really the communication potential was of the two without the influence of such a medium: there was simply not enough 'quality' time between the two. What only transpires is that the timestamp feature caused harm, possibly to both parties. It changed the relation, the perspective of the relation. It separate the two, though designed to allegedly unite. The two navigated in a connected onlife environment, to which nonetheless the impression and considerations never transpired. In the next case study, we notice a variation of such a condition: no longer fantasy fulfilling the communication blanks, but a normative condition of secretive conduct within the couple, and an unconditional requirement of a secretive conduct to sustaining it.

CASE 2. Parallels secretive conducts: When privacy and secrecy collide.

If in Julia and Karl we have seen the discrepancies of onlife secretive conduct, with another couple, Aaron and Claudia, we will consider the modes and conditions to actually cohabit with this condition, to the extent of living apparent 'parallel lives'. Before

considering the specifics of this case study, we will briefly show some cinematic and literary examples, as integral to our methodology, that indeed show how such issue is integrated and considered in the everyday life. If McLuhan aided the understanding CASE #1, here we will rely more on the work of Simmel.

Fragmented relationships

Paula Hawkins's popular bestseller Girl on a Train (2015) describes very well the parallel lives that can be lived inside couples, especially with the aid of personal devices. In the novel, protagonist Rachel Watson witnesses something from the window of a moving train, a kiss between a man and a woman, except the man is not that woman's husband. From this preamble, the story unfolds, showing the delicate balance of un-told realities and multi-level relationship fantasies western citizens confront every day. In Paula Hawkins's novel, we may yet recollect a more mundane exercise of secretive conduct in between partners: wives trying to guess their husband's computer password while he is away, while once he returns, the husband checks the computer's vent heat to check if his computer has been used lately. On the other side, the wife searches online occasionally news of her ex-boyfriend - where does he live, what is he up to, where does he work - only to delete then all evidence from the chronology. Other films have played around with the idea of living secret, parallels lives, as - to mention a hyperbole - the film Mr. and Mrs. Smith (2005), where a married couple discovers they are both secret agents, creating a somewhat incredible, yet famous allegory on how love and work may be perfectly separated. Nonetheless, it appears, and here we may use some of Bauman's and Eric Fromm's conceptualization of love (and Kundera' novelization of the same sentiment) that today's relationships are as fragmented as ever, never confronting, always assuming, never taking the step of becoming stable. The hidden and the intimate seem to have 'unglued'. The secrecy dynamics in this condition is evident: as described in Hawkin's novel, the lives of partners may exist parallel, sharing 'bridge' moments of care and 'love', yet at the same time sharing the same 'bridge' moments with other peers, actual partners or even simple flirts.

What's my ex up to?

We have mentioned before in chapter 2 of the idea of 'checking up' and monitor partners and past loves online: indeed, an entire online-ethnography could be proposed in analysing the modes and the frequency by which this actually takes place. If Julia and Karl showed a certain 'control freak' aspect of monitoring one's partner without letting the other aware, many Reddit threads discuss the matter, either calling it 'cyber-stalk' (R/AskWomen, 2013) with 35 comments or simply 'checking on' ex's (r/AskWomen, 2020) with 80 comments. The general impression that transpires is one of being a 'normal thing to do'- especially being curious - but 'normal' (astonishingly) does not necessarily mean healthy.

'The Girl on a Train' bestseller does not state that this is normal, indeed it is rather perceived as abusive, harmful and (hopefully) deviant: yet it appears as perfectly common

and somewhat 'defensive' towards the relationship's wellbeing. On this matter, a number of simple 'tricks' can be consulted as to hide tracks of activity or indeed aiding its monitoring: as if it were a principal source of the novel, WikiHow offers advice on 'How not to get Caught Cheating'' (Wikihow, 2020). Its first advice is to 'Keep Them in the Dark': setting up alternative email addresses; clearing (partially) the internet browsing history; using 'private browsing'; locking one's smartphone with a personal code; buying a prepaid phone; avoiding the use of credit cards on suspicious purchases. All these are pretty basic rules of behaviour indeed, and one may assume are done on a regular basis by users, whether they are cheating or not: they are simple precautions taken by a user that wishes to have his privacy respected. This leads to the question: is acting in favour of privacy suspicious per se? Is keeping others in the dark necessarily bad? In 'The Girl on The Train, it is still perceived that 'somebody' behaving in secret has something to hide. Yet, trying to find out what someone is hiding also appears somewhat reprievable. Indeed, the character of Rachel is obsessed with wanting to find out more of what she believes she has seen, though this very obsession appears deviant: she is, after all, a job-less alcoholic (her alcoholism also may be interpreted as part of her secretive conduct). At the end of the novel, we come to recognize that all her considerations and suspicions were reasonable: we all have things to hide, but things hidden need to come out. But for how long such 'happy ending' will be perceived as rightful?

Private relationships within intimate relationship…?

As a premise to the core case study of this section, it is worthwhile mentioning a self-ethnographic significant instance, related to the dating App Tinder. With this tool, singles across the world may encounter – based on similar affection – each other within a specific radius. Yet, this very radius is particularly relevant, and the visibility of it. When having an App such as Tinder on your phone, it may be safely assumed that such person is seeking interest in mating – no matter your civil status or partnership. It is indeed an assumption: nonetheless, while the Tinder app could be stored within your device behind a biometric key, your presence in the 'single market' is still visible to any other user. Your 'seeking' someone is much less iniquitous as with Ashley Madison, though such website, as it now well known, was far from being privacy-wise *(Redden, et al., 2020)*. This is significant not only for whoever may encounter you on the app, but the onlife impression your being online, on such service, leave on you. Indeed, a funnily relevant anecdote involved me as my being on Tinder was raised long after I gave up all interest in the app. A friend, renamed Claudia, had found me within her radius: and the thing made her laugh because she knew I was in a relationship with a friend of her. Yet, the fact that I was present came hand in hand with the realization that the person who noticed me there was also present (available) on the Tinder, though being, to the best of my knowledge, in a relationship as well. Us being both on such a dating app, not conscious nor particularly interested raised the question of what parallel instances may take place – either we know or not. But this realization made Claudia admit that yes, she was in the app as well, only because she wanted to find out if her partner, Aaron, was – and for what purpose. She apparently had spent hours scrolling through the device users, in the attempt to find out

if he was using it or not – not being able to access his device physically. My wondering what was going on in their relationship offered insights for next case study used. The elements of secretive conduct taking place, the assumption, the surveillance, are all related condition – will be from here analysed focusing on this couple – to whom only one party, Claudia, disclosed its dynamics.

According to Claudia, Aaron, a British businessman of 30, is admittedly very committed to their relation: he wants them to get married soon, have a family and buy a house. Indeed, they've been meeting a bank consultant regarding a mortgage, which Aaron could not apply to with his wage alone. Claudia nonetheless, as she made me understand, is not convinced: everything is moving too fast, at least for Italian standards. Aaron accepts this, and indeed decides to meet Claudia's parents in Italy, so as to prove his 'commitment'. Yet Claudia is still not convinced, as much as she claims she's in 'love' with him: Aaron has some sort of 'secret' life, which she cannot fully grasp but perceives clearly in certain attitudes.

Firstly, Claudia claims Aaron has never introduced nor talked about his own parents to her: they are, according to Aaron, not 'important' for the sake of the couple, plus Claudia would 'not like them'. Claudia senses this 'oddity' as a cultural barrier, Italians being apparently more attached to their parents, and possibly that's not part of Aaron's culture. Nonetheless, Claudia notices that Aaron does communicate often with his mother, she calls him, and he does go to visit them on a regular basis. They live outside of London and he usually leaves for the entire weekend.

Moreover, Aaron, who works in a big firm as a consultant of some sort (she is also uncertain about his work), sometimes happens to return home with greater delay, occasionally even sleeping out. He justifies some of these events as 'over-work' in the office, alternated with dinners and 'drinking' out events with colleagues. He does not drink particularly much, Claudia notices, but often does return late. At a certain point, Aaron has decided, finding himself late in the night at the other side of the city, that he would rather check into a hotel than return home.

Again, the cultural barrier is put in question: something that is quite unconceivable for Claudia's standards may appear quite normal for Aaron's colleagues, some of whom are married and with family. Yet, where is the boundary so necessary in Simmel's reciprocal discretion? Indeed, Claudia's suspicions grow, as well as a form of paranoia, alimented by the fact that her very colleagues and friends to whom she talks struggle to understand fully what is the problem: does she trust him or not?

Claudia decides finally that she does not. She begins what she herself claims as a not so proud checking of Aaron' bank movements, using specifically the statement that they had handed to the bank consultant. Here Claudia's suspicions seem to be justified: apparently, Aaron had slept these nights out in a hotel just behind their current home – why had he not simply come home?

As I was later informed, when confronted about this, Aaron had appeared shocked and demand her to respect his private life. This is not something she must worry about, nor does it concern in any way their relationship or fidelity. He insists that there is

a part of his life that she must not be aware of. He states that she has no right to control him. When she claims that he has 'no right' to behave in such a secret manner, he does not agree. Again, these considerations come directly in contrast, or so it would seem, with the level of nescience and discretion among two individuals: what one may exchange, where the trust relays. Apparently, Aaron does not claim he has nothing to hide: but that what is hidden is not important. But important to whom? Not, in his opinion, to Claudia? So, if it is not important why not share it? And if it is trivial, even better? If instead it is something serious, something 'deep' and why not, 'ugly', how can one truly separate such reality, and not engage with it with the partner?

Indeed, it is at this point that Claudia starts to seriously put in doubt their relationship: she claims to me that allegedly she would be willing to forget and forgive what he had been doing, not even having to specifically know what it was, as long as it stopped. For Aaron, instead, it would not stop. In this condition, again the question of trust is posed.

Eventually, Claudia claims that she is willing to trust him, until, because of Aaron's distraction, she manages (it is not clear how) to spy the content of Aaron's phone. She finds an FB 'Messenger' group in which her name is mentioned, and where Aaron with his friends are making fun of her being 'paranoid' of their 'parties'.

At this point, that coincides with our conversation, the trust in actually broken: the desire to 'know' is too majestic. She has installed Tinder in order to find out is he is one it (thus the premise of this chat); she wants to find out what is going on, but Aaron won't tell her. She claims that she does not care if he is taking drugs, having "orgies with prostitutes", or his friends, as long as she told him what happens during his 'parties'. At a culminating point of these consideration, Claudia 'jokes' about the possibility that he could potentially be some sort of a serial killer, she could not know. The trust, nonetheless, is broken.

As later understood, however, the conversation or better to say accusations continued. Aaron won't tell her, she accuses him of being manipulative and psychopath, and they break up.

The question of trust in the case of Claudia and Aaron is quite ambiguous and indeed somewhat abused: the question of space within a couple, and indeed the conditions in which one partner is aware of whereabouts and the life 'far from home' is the basic principle of a relationship even for the catholic church. An 'error' concerning the personal qualities of the 'spouse' is a reason to have the wedding annulled (Corrado, 2017); in other words, if she believes and is told that he is a doctor, while indeed is only a student of medicine, the Church may recognize that such a wedding is no longer valid. The nescience concerning each other, as discussed by Simmel, is unbearable. The secretive blasé condition that – as discussed – would create a condition of both indifference and dullness to the others secretive conduct, appears as a specific secretive conduct Claudia cannot bear. In collecting the data of this work one can already notice the problem of not having perspectives on both sides of the issue - and indeed it is the central condition that forms discrepancies of suspicion, control and desire secretive conduct. What would Aaron have to say about all this? Potentially, he would claim Claudia's conduct was a secretive conduct. But this is a central difficulty for the character of this research: we may not

question Aaron; it beats the purpose of studying secretive conduct. The actors do not confront, and yet they stage the same play.

Law of trust

This leads us into considering that in the onlife ecology there is no longer some sort of exchange of what is to know and what is reserved, at least if it is in the interest of both. Instead, we come to consider the very idea of Giddens on the 'friability' of a society without the component of trust *(Giddens, 1991)*: what happens if trust is not a routine of everyday interaction, but rather the routine becomes a lack of trust, or more specifically, a secretive life. Here, two aspects of secretive conduct, both online and offline come to intertwine, showing a discrepancy in the reciprocal knowledge of each other we have repetitively expressed as onlife. In this condition, the lack of a rational of openness as opposed to one of concealment, finds no way out: it turns into what appears as a potlach of secrecy, where the over abuse of reframing, concealment and hiding becomes more central to the relationship than the actual visible signs of affection.

In the case of non-persons or 'objects', these can be interpreted as the technological alternative of the subject, in the form of web-based algorithms, AI and smart devices in general: "present during the interaction but in some respects, do not take the role either of the performer or of audience, nor do they (as do informers, shills and shoppers) pretend to be what they are not" (Goffman, 1956, p. 150). The 'non-person objects' appear similar to servants, but specifically because of their uncertain effect of being present, though not really there (Goffman mentions cab drivers and elevator operators): even more interestingly, the Canadian author senses the importance of such roles in the "growing body of technical personnel - recording stenographers, broadcasting technician, photographers, secret police, etc. - who play a technical role during ceremonies but not a scripted one." (ibid, p.151). Such roles appear astonishingly similar to the ones now taken up and offered by the functions of algorithms, with the "capacity to shape what and who we know" (Beer, 2017, p. 112),

We have here discussed a more extreme, yet not necessarily peculiar, condition of secretive conduct. Aaron did not specifically use the elements of the onlife to deliver such condition, but rather Claudia could not bear the 'nonchalance' approach to such a conceal of visibility. Again, it could all add up to a mere form of cultural clash (with Italians apparently being more open to their partners, British more discreet), but such simplicity does not add up: the perception of secretive conduct appears unbalanced rather in the modes in which secrecy offers freedom and at the same time obsession. Freedom in the case of Aaron represents apparently the wish to do whatever as he pleases, without constrain or need for justification (not to mention comprehension) – as long as the boundary is not breached. Claudia in the form that such secret offered no freedom at all: she needed to know and led a secretive conduct in trying to discover and unveil the 'secret' around Aaron's conduct. In more blatant terms: Aaron wanted more privacy, Claudia would attempt to breach it in whatever means possible. The balance between 'knowing' and 'nescience', so central in Simmel's conception of a Sociology of Secrecy, is not attainable.

As we will discuss in the next case study, the very breaching of privacy is the most common secretive conduct procedure, especially when the boundary, as in the case of Claudia and Aaron, it is not clear. Claudia feels evidently harmed and distressed by the situation of not knowing, she is suspicious, desires to know more, and is frustrated by not being able – but we are left only to the verge of what is truly going on. Such condition opens new perspectives, the transgressive aspect prevails, and the centre, the relation, the norms and pillars, cannot hold.

CASE .3 Eyes in the Home: invading privacy within the private realm

As noticeable, fundamental in the choice of these case studies is the intimate realm, especially because its conception requires some forms of conceal, as intended by Goffman, a specific backstage to relate to and act far from 'others' eyes. Indeed, Goffman is central for the recollection of this case study involving an Italian family, though after an intensive parallels in digital ethnography can be drawn, as it will be shown, across the entire onlife reality. Other than Goffman, this case study returns to the ever-recurring theme of the Foucauldian panopticon and the realm of perpetual surveillance, finding its quintessential encompassing condition with the aid of smart devices and their essential fulfilment of the 'desire to know'.

Secret conduct

As a premise of this case, a sort of incidental 'social vignette' is relevant, taking place in a recent reality TV prank by the Italian program Le Iene (25/11/2019) I happened to watch: in front of hidden cameras football player Stefano Sensi receives a compromising message from a fan while sitting on the couch with his (accomplice) girlfriend. The immediate recorded reaction of Sensi is of great sociological relevance: he claims he needs to go to 'pee', and in front on another hidden camera pointing the toilet seat, he rapidly checks his phone and swiftly answers the fan: he even continues talking loudly to the girlfriend while doing so, pretending he is following her conversation. The spontaneity of this action, one of reading and of viewing compromising content in the privacy of the bathroom, proves the net inadequacy in our contemporary 'privacy' policies: indeed, we are overwhelmed by privacy procedures, yet we have no cover to 'experience' its features.

The toilet seat indeed, as a common denominator of both bath and rest room, is the only enclosed space of actual time for ourselves. It is the social space of pure actual and virtual a-sociability. Cameras do not reach there (in restrooms they may). We are finally alone. This is a space where we are naked, intimate, mainly comfortable, and funnily, most of us with phones in our hands. Already in 2012 CBS reported that 75% of Americans admit of such, with males being the majority of users (Castillo, 2012). Two reasons justify such behaviour: visits to the toilet are the ultimate moment for a temporary 'peace' of mind, checking the latest social updates, playing a little 'angry birds', and releasing the pressure of the day with mindless web surfing and chatting. But also, toilet visits are the space of exclusion where one can freely behave in secret. No other space is

any longer socially acceptable as secretive in the everyday environment: no door anywhere else is locked so naturally.

Quite the opposite, the less we possess spaces where to release the pressure of the public (Goffman, 1956), the more these spaces become frequented and necessary: inevitably, one could claim the result is that these very spaces become more and more suspicious. The excuse of 'going to pee' in order to 'finally' check our messages, especially ones compromising to colleagues, friends, children and partners, becomes quickly indiscreet: to cover oneself from the camera too often becomes per se a motive of suspicion, and more than that, generates a desire to know what is covered. It is in this condition we come across the secretive conduct involving Aldo and his daughter Sara.

Smart Home surveillance

The conditions and possibility of contemporary surveillance are technologically limitless, and thus their 'moral' problematic has also changed their conditions and possibility. In the case of Aldo – a middle aged Italian father, he had acquired in June 2019 a 60-euro worth surveillance camera in Lidl and installed it in his kitchen for observing and preventing possible 'thieves'. Apparently, his neighbour had bought the same equipment – and his motorbike pals all made regular use of similar tools. Such specific camera is connected to the Wi-Fi, where one could view through its lens on the smartphone and even activate the microphone. Aldo has used the associated App to joke with the family while at work, barking and making funny noises through the microphone.

The following episode tool place while we were working together. On a normal weekday, Sara, the twelve years old daughter of Aldo, stayed at home from school because feeling sick. As to check on her condition, Aldo called her phone around 11 am, and did not receive an answer. He tried again and thus contacted the house telephone, still without answers. At this point, just in front of me, he becomes alarmed. He calls the wife, mother of Sara, to ask her if she heard recently from the daughter. She has not, though she believes Sara is at home. They both get worried, and Aldo decides to activate the camera. He observes the corridor and cannot see her. At this point, he calls the wife and asks her to rush home. Having observed the scene, I try to calm him, telling him that Sara has been not available for less than 15 minutes. He replies she's 'always got the phone in her hand', and activates the camera again, afraid that there is someone in the house. As for the further arguments, especially concerning the problem of using the camera to 'observe' the daughter's whereabouts, Aldo answers: 'when your child is 12 you'll do the same'.

Eventually the mother found the daughter, 10 minutes later, drying up in the bathroom after a shower. Before me, Aldo orders the girl to always have the smartphone on her when at home alone. Also, he accuses her of giving them a great scare. None of the other colleagues is particularly concerned on the dynamic of the events – relieved that nothing serious has happened.

Normalization of spying

How spying, monitoring, observing has entered the everyday conduct of citizen would require another Ph.D. – and indeed Foucault had in many ways foreseen its implications with the Panoptic analysis (1975). It is worth mentioning nonetheless how this risk is represented. Lyon and Bauman define an 'adiaphorization' of control and surveillance, "in which systems and processes become split off from any consideration of morality" (Lyon & Bauman, 2013, p. 13). The lack of a specific morality is what renders possible the potential total 'desire' for monitoring that is nonetheless far from a total monitoring activity. The question of (smart) home security cameras, as opposed to the idea of intimacy, is a much-debated issue: Already more already more than ten years ago Nelson (2010) discussed the problematics of baby monitors entering the most intimate spaces of parents - with subsequent effects over control and anxiety; with Horst (2020) we see how social media itself may become a form of 'Friendly monitoring" device among parents, again to address– mainly - their anxiety. Such normalization of tools to fulfil parental anxiety comes hand in hand with the potential perception of constant control, and thus anxiety of hyper-control, of siblings – but also potentially our elderly parents. Central is the way in which smartphones – and more recently home and self-surveillance tools are being implemented to monitor and aid elderly living alone, offering a cheap and sadly alienating solution to caretakers *(Kelly, 2021)*. This concern people who are at the late stages of their lives, and their independence is perhaps at stake in a condition where they do have, for the most part, experience it. Instead, it would be relevant to question Sara, not even adolescent, about what her take on the way she sees or perceives control and surveillance within the home is: would she invite friends over, knowing that she may be watched? Does she care to fully dress, while being home alone?

Previously, when discussing Goffman's work, we mentioned the roles of the non-person, that indeed in this case seems to underline not only the smart phones, an automated and highly efficient tool to fulfil the desire to know, but actually the somewhat Gyges effect form bystander role of a parent wanting to know, to see, observe and control. Again, this is no place to indicate some sort of malignant influence of actual devices in the behaviour, and the actual conduct of parents over the education of their children: the society's use as a whole of such devices perhaps is. The anxiety aroused by 'not knowing where our child is' is a well discussed theme – nonetheless the societal pressure in having to know where your child is at all times is relatable to the pressure I personally experienced concerning needing a smartphone – as one cannot live without it. But indeed, one can live without – as essentially parents may live without anxiety *(Wuyts, et al., 2017)*. Though it sounds, for most people, absurd to fear one's kin of being observed while being naked, such perspective appears more considerate when we realize that most of these smart-cameras are web-based, and potentially a risk being hacked *(Priest & Martin, 2021)*.

Indeed, the breach of privacy is a central result in this sense, when searching online - not the observing, controlling and spying per se. Security cameras themselves are subject to a serious hijacking flaw (Unterfingher, 2019), and may be used to invade your privacy by whoever manages to enter the backstage (as, among others, much criticism is done towards the Amazon Ring product internet (onlife) connection). Again, the onlife reality appears fundamental. Who is permitted to enter? If only vague 'terms and conditions'

apply, to which we all - to a certain extent – adhere, regardless the rules. By all the world being online, all the world may also be observed and controlled online, with the smart phone as the central 'remote control tool'. We have allowed such tools to enter voluntarily – not through a coercive consent form—but a purchasing and consuming mechanism. But what do we truly understand of these products and devices?

Remote smart harassment

In 2018, Nellie Bowles wrote a striking article for the New York Times on how 'smart-home' technologies, apart from of their already mentioned convenience, "are now also being used as a means for harassment, monitoring, revenge and control" *(Bowles, 2018)*. Such perspective becomes even more central when considering the hypocrisy of building the rhetoric of protection from COVID-19 by staying at home, while domestic violence and upsurge is strictly home-related, and indeed where the most toxic conditions arise. This is connected to an actual 'remote' domestic abuse, caused by the "losing control of Wi-Fi-enabled doors, speakers, thermostats, lights and cameras", usually "controlled by one person in a relationship [who] takes charge of putting in the technology, knows how it works and has all the passwords. This gives that person the power to turn the technology against the other person" *(Bowles, 2018)* The article cites an 'anonymous' victim: "If you tell the wrong person your husband knows your every move, and he knows what you've said in your bedroom, you can start to look crazy," she said. The 'invasion' of such tools, used primarily for one's own commodity and good, strike in its turning against us, especially when others are not fully aware of its potential: Indeed, "it's so much easier to believe someone's crazy than to believe all these things are happening" (ibidem).

Again, taking the extreme out of the equation, the notion of being in control of such means and indeed controlling them remotely is impressive, especially when the home-surveillance is not only installed with common agreement and only later turned into abuse, but when it is installed without having other peers (family/house-mates) knowing about it, and hiding its 'spying' components in different parts of the house. *(Szakolczai, 2021)*. Here the suspicion, control and desire of knowing what is going on in the home remotely is at a dangerous peak of abuse, yet it is relatively cheap and easy to install, compared to what this technology required and cost even a decade before.

Camouflaging control

The potential breaching of the backstage, in any domestic and private establishment, is evident and encompassing. In 2020, by searching on Amazon 'spy hidden camera', one could acquire impressive devices for as little as 29 euro; the camera is hidden inside a USB charger that may be unsuspiciously plugged into the wall and left with motion sensor recording for as long as 50 hours in full HD. It is described as a product "Ideal for installing […] in places that people won't notice to help improve the security of homes, offices, stores, and warehouses, so that you can rest assured that you won't miss anything".

These products raise another question as well: not only how someone in the house or the office may control 'secretly' family members or colleagues, along with babysitters, housemaids and cleaning staff, but these, conversely, may control, observe and surveille

themselves the household, workplace. A small camera such as this may be placed potentially in front of the home/office safely, and later removed, without leaving any trace. This is thus no simple science fiction, as one proposed in the novel the Circle (2013). It is rather an ever growing covert recording and monitoring of any intimate environment, to which privacy only faintly allows a protective 'mental life' assurance.

Moreover, these are simple propositions, derived by a basic google search on these products: any abused wife or overly controlled employee may do any such basic searches and wonder if some of these products (along with the so frequent Amazon purchases) are some of these spy-cams and hardware: in this perspective, the potential of paranoia and anxiety towards the equation of 'suspicion, control and desire' has no limits.

Docility and dullness

Again, in the realm of legality, as long as these devices are placed in the privacy of the home, avoiding strictly-intimate places (as, we have seen, bathrooms and not many other places), potentially an 'abuser' may get away with it: not only would he hardly be found out, or even if he is, the shock of such recording would not be as scandalous as once, if the recorded have not indeed been deprived of their 'secrets'. As understood in the relation between Sara and her father, there is no actual 'rebellion' on her behalf to the idea of a perpetual control and indeed being monitored: in such perspective, that returns to Simmel's notion of a blasé outlook, both parents and daughter believe they may perfectly live a 'healthy' adolescent life along these contemporary technological means of surveillance. They are, as it appears, only 'superficially precautions' of such technology and how it can be abused. Instead, they appear perfectly sensible to such medium, and at the same time, in the words of McLuhan, servomechanized to its functions: intimate relations change when such mediums are installed. Thus, if we allow a generalization of Aldo' family, a perpetual monitoring, or potential monitoring of our whereabouts and backstage may lead to an actual docility to such procedures. We may become accustomed to surveillance, and simple 'remote' observance is no longer scary nor controversial: as with Simmel's Mental Life discussion, a dullness becomes accustomed as we have learned how to behave, and – most important of all – of never lowering secretive conduct defences.

More tools can be analysed: beyond the idea of a home-based observing station, monitoring family, strangers and potential thieves which – as we have seen – add up to the 'smart-home' technologies represented, among others, by the Amazon Ring Doorbell product, which as stated on Amazon: "Lets you see, hear and speak to visitors from your phone, tablet and PC" (Amazon.co.uk, 2020); the doorbell has a motion sensor and "Works with selected Alexa devices to launch real-time video with your voice." This is what the already mentioned Ziccardi calls a 'Soft dependence', central to the onlife ecology, where we ourselves facilitate the tools of control and do not offer any resistance: they are useful, and indeed any technology justifies its purposes. The role of Alexa itself is impressive, considering especially the already mentioned non-person role that may enter and exit the backstage, recording and monitoring the two 'regions', and offering 'data' of both. It is a device installed in our home, connected to the internet and perpetually in 'active' mode that possesses our information and shares it indistinctly,

offering a service in exchange to an uncertain number of *'capta'*. In the AirBnB I am currently staying, two of these devices are installed one in front of the other: the two neighbours doors facing each other have a "rear window" in the other's live. We do not know if I, entering, am observed. I do not know if I am by someone recorded, taken note of my movements – if there is a note on who has entered with me, how long, and what time. It is, as other smart devices, the fundamental encompassing latent feature. Also, especially regarding other Alexa integrated tools, without properly introduced to visitors, we are not made aware of its presence. Yet, did *it* notice our presence?

In this section, we have taken in consideration the fundamental controlling aspects of smart technology, quintessential tool to fulfil the 'desire to know'. It allows the perfect panoptic system: the potential of perpetual observation without any signal of actual monitoring. Moreover, the surveillance, perfectly integral with secretive conduct, is remote and invasive of the backstage/private real. The observer is the 'king of his castle', to which the 'right to be let alone' - in other words privacy - appears perfectly compatible with his counter-approach to the 'right to observe (alone) where he usually is alone'. As we have seen, the technologies are being evermore obliging to such secretive conduct. They have become microscopic, hidden, cheap and easily acquirable. And when not hidden, such as in the case of Amazon Ring, they are inconspicuous: we know they are there – but make no notice of them.

In the next section, we will investigate more detail about the available technologies that render the 'desire to know' evermore invasive yet normative, and how the modes to evade such control go just as well hand in hand, opening an endless spiral of deceit, suspicion control and desire.

3.2. Invasive tools fulfil the desire to know

In this section, as mentioned in the methodology, we will venture more rapidly among the instances of secretive conduct and its counter within everyday life, re-proposing the spontaneity in which these instances, personally witnessed, take place.

The question of actual monitoring outside the home emerges in the specific case of parents wanting to know what their children are doing at any given time – a particular vicious and perverse modality of the Nietzsche-Foucaldian 'will to know'. The idea of parental control and surveillance potentially goes back to the birth of society, with animals and children being observed and kept behind the same fence, under the close look of adults (Mumford, 1961). The idea of surveillance as connected with the concept of care is also possibly at the base of society, an idea, discussed by Lyon and Bauman, whereas surveillance indeed is concerned with "the service of care for the Other" (Lyon & Bauman, 2013, p. 84). After all, already Goffman noticed how we all have something to hide (Goffman, 1956). Yet, as we've come across in Trottier's analysis, the "need of privacy can bring about greater surveillance and the scrutiny around private spheres" (Trottier, 2015, p. 167). To surveille in this understanding is specifically the action of 'lifting the veil', in other words to dis-cover what has been covered, and thus put away.

The danger is one of forming a specific 'creeping' phenomenon, and such privacy violation can become "part of an increased normalization of the social media visibility" (Trottier, 2015, p. 66).

I will offer two specifics of this secretive conduct. One on the ease in which monitoring and surveillance takes place, and the offer analysing with some depth the onlife dynamics of parenting.

Creeping up to creepers

We have previously discussed the flaneuristic aspect of social medias, and indeed the blasé' approach to its most controversial features, to with today we seem quite accustomed. It is hard to find oneself today meeting with someone after a long time and not end old talking about past acquaintances. When we do so, it is quite easy to fall into the habit of seeking that other on his social media. On one of these occasions, being myself quite unfamiliar with the specifics of Instagram – a friend showed me the account of a common acquaintance who ended up becoming a not particularly talented model. Not one friend, but all the friends found themselves exploring the persons in question account, and watch her 'stories'. The action appeared as a normative thing to do, and that particular model was not even the only person that had been observed that night. It is also interesting that, while I do believe such forms of observation are almost a trivial recurrence, this particular occasion surfaced a sort of patronizing and 'care' connotation, meaning 'look what happened to X' – or even posing judgement on the quality and embarrassment the social media representation creates. Such posing judgement is particularly interesting even when encountering new people, perhaps finding them attractive, only to be somewhat 'turned off' by their online presence – the value or content of post and pictures – another episode that indeed was referred to me, again with quite nonchalance, as if the superficiality towards personal media equals superficiality in real life – confirming the onlife ecology dynamics. This idea also appears to confirm who in such occasion, the creeper is not who observes, but rather who does not own a profile worth seeing.

Yet, in such occasion, while effectively gossiping on 'X' professional carrier, I caused a disaster. Convinced I was zooming on a picture by double-tapping the screen; a feature to which I was accustomed with – the Instagram App instead produced a 'heart' – to the horror of the person showing me the image on his phone. With remarkable immediacy, all the friends surrounding us got involved as if this was the joke of the night, but also offered advice on how to 'get-out-of-the-situation'. Everybody offered theories, such as 'if you remove the hearth before 10 seconds the other person does not receive the notification' – no proof found online; or given hearths generously to other random picture of the profile to create 'noise' and 'confusion' (this was the option chosen). Another solution, that was seriously considered, was to temporarily disable the account, so X would receive the notification but not know who from. This obviously if she was not online at the moment – or has not seen it already: which is quite probable.

In another relevant occasion, though taking place already by the early 2010s, I found myself talking intimately with a friend of a past partner while having lunch in a restaurant. As this past partner of mine had quite common name, I believe my friend happened to mention her by her surname several times during our conversation. When we got up, I noticed that some stranger sitting behind me was scrolling on his phone my ex-partner's social media. As I've never seen this person before, he must have overheard the conversation and decide to have a look, given the tool, to who we were talking about. We both stared at each other in a moment of shock – to which no better action was taken than to ignore each other, and pretend nothing happened (in accordance to my admitted *esprit de l'escalier*)

This instances, to which many blogs and social media magazine offer likewise accounts *(Reinstein, 2018)*, reinforce the Onlife dynamics of perpetual monitoring, invasive tools and constant and highly engaged concern to what such 'virtual reality' – perpetual scrutiny and rating dynamics – implies. In these instances, we have seen not only the normative entertainment of observing without being seen, but how this 'not being seen' is the key to this entertainment: it is a shield that justifies the Gyges ring leading to secretive conduct. Yet, if this episode is somewhat light-hearted and taking place within a 'friendly' environment, we will now indulge more deeply in rather the family dynamics in which the Suspicion, Control and Desire formula is even more engaged with and indeed justified as a practice of care – albeit requiring invasive tools.

Graceless caring

Within parenting, it is an almost taken for granted condition that they must ensure a safe environment for their children. In this perspective, secrets are necessary in both directions: both on behalf of the parent who is watching without interfering, and of the child who behaves secretly as to perceive fully his independence. But even before that, already in 2009 Sonia Livingstone made a profound consideration on the role of Children online, making it clear that sharing "photographs of one's friends and family on the internet is so common among internet users that many will not consider this deviant." Livingstone considered the emergence of not only a 'Risk Society' as perceived by parents, but even a risk of a risk society, "with parents peering over children's shoulders, websites advising on what information to disclose and when, and safety initiatives providing guidelines on how to test if people are really who they say they are" *(Livingstone, 2009, p. 180)*. In this perspective, Livingstone emphasises how control only generates further control, and hiding eventually produces more hiding.

Indeed, to this conduct we have two quite opposite establishments, with "parents peeping over children's shoulders, websites advertising on what information to disclose and when, and safety initiatives providing guidelines on how to test if people are really who they say they are, there is surely little left ungoverned in young peoples' lives" (ibidem) Family dynamics are becoming ever central with the use of social media groups – an element that indeed appear to take over any intimate condition, even among friends and colleges. Allegedly, one could claim that it is hard nowadays to be part of a community of some sort without being asked to join a WhatsApp group representing it.

Such dynamics raise a number of concerns within the elements of secretive conduct - one that indeed come in contrast with the fundamental consideration of Simmel and his Sociology of Secrecy. There, by joining a group with diverse elements, some of which effectively strangers – the dynamics of intimacy do not effectively take place – yet, with an auto- ethnographic consideration, one may claim that indeed there is some sort of informal perception, or nescience, of it. We face forms of over-excited exchanges – use of hearts, smiles, *emojiis* – even picture/selfie taking (in private or in group) that indeed breach intimate spaces with a somewhat constructed form of 'taking confidence'. At the same time, based on a personal observation, such groups allow some other breaching of the Goffmanian the front and back stage, making direct intervention or personal remarks on issues. In a personal example witnessed in a work-related group (work related yet strictly exclusive to a fraction of the interested colleagues of an association), some private matters would be discussed in public – or raised to public awareness without specific necessity – forming an odd form of social control, where everyone was informed, and at the same time everyone could be pointed out.

Surprise groups

The nature of the secretive conduct becomes a shared issue with the use of chatting media, especially WhatsApp, during birthdays or any surprise event. I would receive an invitation to an odd-named group, with a set of friends or colleagues as members. To avoid assuming it is a spam of sort, the title of the group happened to be something trivial and vaguely related as 'Social Media Class Tutoring', or 'Cork Dog Owners'. The group would open with a random text, only to mention, under the text, that in reality this group is created to discuss the surprise birthday party or present of a common colleague, or friend. This example has taken place almost as a pro forma among both Irish and Italian friends, rendering the mode in which secretive conduct is justified in organizing and chatting about someone without raising any suspicion. When raising the issue some friends about their use of secretive groups, I've discovered that in a single-family member would possess private-secret groups for practically any member or kin, leaving out the person in question. Marco, fourth member of a family of six, showed me an ever-long list of groups among only his family members (2 parents,2 sisters, 1 brother) picked up annually to discuss presents, parties, or even more private matters. He was member of a group among mother and father, the three males of the family, all the females, only the sisters. Such divisions are repeated within friends, colleagues, classmates, only to be slowly archived and forgotten after the event. When questioned if he ever thought of how many groups are out there about him, discussing him, he didn't seem concerned, alas offering a witty reply: "I did get a surprise party after all, didn't I?"

Again, the question is not if this is in any way new: surprise parties and back-talking always existed. We must nonetheless consider if, and how, the medium used did and does have an effect in the secretive conduct, leading also to a potential secretive conduct of suspicion, control and desire. What goes on in the background of our friendships, colleagues, kin: not visible, actually hidden, from our eyes. Falsified behind a deceiving title, to which we are not aware and left apparently unconcerned. We may not know: it

cannot be analysed quantitatively, and hardly qualitatively. We may, nonetheless, assume only that such potential is present, constant, and easily achievable.

Pandemic conspiracy

As with other technologies, of which this thesis is concerned, the COVID-19 pandemic increased exponentially their uses and abuses. A mid-2020 Guardian article focuses directly on the issue of WhatsApp groups, noticing how: "A WhatsApp group can exist without anyone outside the group knowing of its existence, who its members are or what is being shared, while end-to-end encryption makes it immune to surveillance from third parties." (Davies, 2020). Davies, more-than-once mentioned technology-columnist of the English newspaper, claims that "by late March, usage of WhatsApp around the world had grown by 40%.": one can only assume the use of the very secretive conduct related to groups also increases as such. Davis discusses the spread of fake news, actual political manipulation and conspiracy theories circulating- which indeed appear to be an effect if not complimentary to "a communication medium that connects groups of up to 256 people, without any public visibility, operating via the phones in their pockets, is by its very nature, well-suited to supporting secrecy". (ibidem).

Persistent monitoring

The modes in which devices and groups actively monitor, and yet 'act in the background' has become, as we have mentioned, a repetitive and somewhat 'unescapable' condition - to which everyone must be part, appear to be engaged, no matter the interest. There are significant elements of the Panopticon in this, but more (or more subtly) than that we can find correlation with Simmel's consideration on the nescience of individuals - where they pretend to know about each other, or require that everything is somewhat exchanged, or only offering an illusion of it - an essential characteristic of secretive conduct. Nevertheless, the recorded elements of all talks, all discussions, all jokes and complains are there - they can be searched, scrolled, screenshot, shared and shown around - which are more specifically elements of secretive conduct.

Another example may be offered, for clarity: during a dinner among friends, a particularly bad singer picked up a guitar and decided to sing a local song, full of obscenities and humorous takes. Among the general laughter, someone took a video - to which the singer called out: "don't post it!". Yet, with a second song, I noticed another of the participants sitting next to me turning on the hands-free 'voice message' option on WhatsApp and nonchalantly laying the phone on his lap, with the screen blank, pointed at the singer. When the song finished, he picked up the phone again and sent it to a group, exchanging a series balloons with unknown members. Here we can find the fundamental arousal of suspicion, control and desire, correlated with the secretive conduct. Whom did he write to, in what context or purpose? Such information is not to be known – in everyday life, it is ok to film, but not to ask why, or whom to. Secretive counter conduct - in what could be a concluding remark - appears as something to get away with, more than good sense. When we witness it taking place, it is not comfortable, nor righteous to ask why does it happen: apart from me, nobody else noticed, or appears to have noticed. I, as an observer, felt intruding: intruder of an invasion.

Other than messaging& filming, the smart features of modern devices, as we have seen, appear ever more integral in the secretive conduct of our devices. In a recent case, such induced integration has been referred to me regarding the acquisition in 2020 of a new car. Featuring all sorts of 'smart' functions, such a car of an American brand offered with the 'package' a special app that allowed to control the consumption and all sorts of 'data' from the car, including the driving style and its location. [34] Francesca, who referred this instance to me, felt the need to share a recent example of a shock, under my thesis's concern with suspicion, control and desire. Indeed, Francesca claimed the last car she owned with her partner had not only faced several incidents because of her 'clumsiness' but had both to face some fines for parking in 'pedestrian areas' of the city centre. When deciding to buy a new car, they had agreed to take extra care of all sorts of fines, scratches and all, and indeed Francesca admitted being quite paranoid about the new car. Yet, as she confessed, her paranoia was nothing as compared to her husband's, who the day before had called her after parking again in the same spot where she tended to receive many fines. After an initial shock, Francesca had the husband admit he happened - out of precaution - to check through the integrated GPS, which she wasn't even aware of, where she would drive and park. They agreed, after a big fight, to uninstall the app from their phones.

Interestingly, this example of apparent abuse, of which Francesca insisted her husband had never previously shown signs of, offered grounds from Francesca's description of another case study, this time, in her words, of 'real abuse'. In this case, yet another couple was involved, and an app – though installed 'as game' in both phones. The app's name is not important, as many others can be found offering the same features, meaning a system to always live-view the partner's or family member's location. The functions may be integrated with seeing the others 'battery level', or receiving a notification when the kin approach a certain location. The control mechanism of this app, downloaded voluntarily in this example, but potentially imposed in other circumstances, should already set a number of alarm bells, once we recognized the dangers described in this work. Nonetheless, as Francesca informed me, the couple - her husband is a colleague of the other husband - played a certain 'couple' trust game, as many (apparently) do – sharing, for example, social network passwords or 'screenlock' codes.

The use of such an app, after an initial hype (indeed, one struggles to offer a particular 'sane' functionality to any of such apps), Francesca claims they both forgot about the 'game' – a point that is only reasonable when we consider the amont of apps and information flow that goes through such devices, and the way in which the interest and navigations changes on daily, if not hourly basis. When Francesca's husband called the colleague over for a beer, suddenly, while they where together in Francesca's house, this collegue was phoned with great anger by his wife. In the general astonishment of all,

[34] It is important to notice such 'bundle' also appeared to levy on the cost of the insurance.

an odd portrait unfolded: the wife had been suspicious of his whereabouts, and indeed became increasingly suspicious when she noticed – in a complete coincidence – that the husband was nearby the home of an old babysitter they had, of whom, apparently, she had been very jealous – though never before mentioning so. Such examples again, to which certainly all have or may find direct parallels, show again the simplicity of falling into the trap of systems of control – especially when even the slightest tendency of suspicion and doubt are ripe.

A number of events may be found in the local news, of specific abuses that may take place with the use of similar software's: in some cases, hackers managed to 'catch' users masturbating and subsequently requesting a ransom *(ABC News, 2016)*. In this specific case, it is worth mentioning how the hacker requested money in exchange of not posting such images to all the victims Facebook friends, to which the user decided to self-shame himself: he posted a note telling his friends of the hack, and requesting them not to open such file, if ever received. Apparently, this reverse-shaming is one of the most efficient ways to fight back such blackmail. Again, the idea of revealing the secret finds its healing power: by admitting the threat, the user has somewhat exorcized its influence. Same has indeed has been done as to respond to these 'non-consensual images': a pilot effort developed by Facebook to tackle revenge porn in Australia proposed to have potential victim load nude images of themselves directly to reserved service of the platform known as PhotoDNA. The service would analyse the pictures and create a 'hash' matching with other reported content, as to "allow victims of 'image-based abuse' to take action before pictures were posted to Facebook, Instagram or Messenger." *(Solon, 2017)*

Summing up, we notice two perspectives: a form of 'healthy' secretive conduct - to make good, such as convenient and socially fulfilling WhatsApp's Groups created to discuss a present or surprise for someone who is not authorized to know about the group - and the idea of filming, evidently, someone, with the potential intention to store a memory, or even post or share its content on a social network. We notice furthermore the constant possibility to reveal such secretive conduct. When someone receives a present - ordered, chosen and discussed within a secret group - one can thus reveal the group, even as part of the gift itself, as proof of the effort in organizing the event. And when an event is filmed, one can obviously be shown the file had become thus somehow an active participant of the secretive conduct.

Again, the apps represent the tools and means through with devices induces episodes of secretive conduct: raise suspicion among users, even when participating in a voluntary game of sorts. Become objects of assumption and distress, even when sold to consumers as functional and convent tools. But beyond everyday tools on onlife interaction, we will not look into the actual virtual dynamics proposed by such environment. How the internet itself, with its audience and instant exchange, its anonymous users and peer, is a fundamental element in perpetuating such instances of harm.

3.3. Resisting the perpetual memory

The discussion of the following case study is somewhat depressing, though significant, especially for the incidental onlife (indirect yet first-hand) experience of its abusive content, that became, until its tragic ending, a recurring feature and conversation in the onlife of common friends. It involves the tragic death of an Italian woman - that, in respect of her battle 'to be forgotten', I'll rename Emma. In 2015, she was willingly filmed by her partner producing six 'amateur' pornographic clips. These clips were shared, apparently in live version and allegedly with her consent, to a private chat between common friends. The videos nonetheless were minutes later shared 'outside' the intimate space of the group and became overnight extremely popular in Italy and among Italians across the globe. This happened not only for the explicit content, but for the inadvertent 'humoristic' exchange between the two during the intercourse, becoming by this somewhat of a 'meme' to be shared with wit. The popularity, among Italians in particular, became impressive. The clips and memes have circled among Italians for days, either in shock, mockery, humour, to the extreme of appearing online not only in humiliating Facebook/Meta groups and fan pages, quoting some of 'expressions' used, but the content and 'catchphrase' was followed by "T-shirts, smartphone cases and other paraphernalia" (Masters & Borghese, 2016). The event became somewhat of a national case, leading to the tragic suicide of the woman. (Bufi, 2015)

Gyges Bystander involvement

Again, WhatsApp is to be cited incidentally, only proving its fundamental involvement (not as a corporation, but as a social media in general), as it is there that first the meme, and then the original video was forwarded inside a number of groups to which I was a member (before I got rid of my account). This is significant, as the naturalness in which the memes of Emma were exchanged made the entire issue perfectly 'ok'- until the tragedy of her death that rendered the whole joke a 'no-no'. The groups where such videos and memes were exchanged were not specifically 'Sex related'- but happed to host humorous post- being the members either part of old class mates or one of occasional soccer match organizers. The videos were shared to a group of people 'for a laugh'- part of a specific provocation and 'irony'- to which 'meme' websites such as '4chan' are the perfect precursors, forming what has been defined as a memetic antagonism (Tuters & Hagen, 2020). The effect is one of posting content with the specific aim of being 'awkward'- offensive and yet provocative- especially taking advantage of the difficulty in recognizing the actual members of the group. This attitude could be defined as a form of 'trolling'- though the preamble of trolling is - mildly put - one of creating 'anger' and hate speech to unknown commenters. With the memes shared among a limited group of people, the aims are possibly aided by the Gyges effect a psychological condition mentioned before, whereas the users/members would change attitude and opinion by taking advantage of the actual 'veiling' system of communication. But this is also

reductive: with sharing memes - especially if they are cynical and provocateur - it is not simply a disinhibition, but rather a 'taking the piss', without fearing consequences of offending anyone. The Gyges effect rather appears to take place with the viewer - and indeed here lies the real secretive conduct: how a vulgar and sexist joke makes you truly smile and laugh without fear of judgement or being seen. Or how such a pornographic video - and its catch-phrases - from a provocateur prank truly 'turn you on': the WhatsApp group does not transpire any of these feelings. It does, nonetheless, increase its effect and refile its features almost infinitely. To these, we are nothing but bystanders. We may express disapproval or ignore: yet the secretive conduct permeates.

Invisible dangers

While these considerations on the secretive conduct of receiving and sharing such content are indirect, the case of Emma is significant also as it is directly tackling the issue of suspicion, control and desire. Yet, although the phones and computers of today, principal 'archives' and actual 'secretaries' (managers of secrets) of such content, possess the most advanced passkeys and locks available on the market, such content is far from being fully safe. An interesting exercise is to actually visit one's personal google account and visit the 'pictures' application: there I have found entire gigabytes of pictures gathered 'in the background' in the last years I wasn't even aware of, old back-ups of previous phones or unintentionally cloud storage of USB key content. To these, other than physical 'menaces' (such as partners, colleagues, parents, strangers) who may find or pry the data, digital menaces lure constantly the net, seeking such precious content from our hard-disks. These attacks may be done with the use of ransomware and malware in general, that may steal such content and blackmail us by making them become public.

The case of Emma strikes principally through the tragedy, nor the first nor the last, of such abuse of 'publicity', as hardly one can find a more evident example for a backstage invading/leaking into the front. It also underlines the question of blackmail, and how such systems become an easy target: what is hidden from the public is permanently in danger of becoming revealed. The secret is per se a latent blackmail whose nature needs to be inevitably stored and protected.

Pornographic material contained in phones is a clear example. Either downloaded, viewed, or actually filmed (all being simple tasks in modern phones), these quite fundamentally private and intimate contents are stored in phones that a user is willing to protect by all means from strangers. As discussed in Part II, before contemporary technology such material would be hardly at hand at any given time. This is not to say it was more private – indeed, interestingly, pornographic magazines were once viewed and purchased in local stores. Filming of intercourse between couples was obviously possible, but the technology was hardly immediately at hand, and in such quality. Data would be recorded in a tape, a CD or more recently an SD card. Material would be yet 'objectified': its content physically 'placed', and indeed stored with physical safety. The same can be said with magazines, tapes, and other pornographic content.

Returning to 'Emma' the question of a right to be forgotten becomes central; a request formally proposed and insisted upon by the mother of the woman. Such right, as discussed by Rodotà, is fundamentally compatible with the necessity of a *damnatio memoriae* of our online identity: The perpetual storing of memory and indeed data around our digital and IRL person forms the actual 'damnation', rather than its destruction, recalling what in Ancient Rome political hegemony required for what it perceived as dangerous to the community, and thus 'damned to forgetfulness'. For Rodotà, in the digital age the past is perpetually recurring, both for the search engines indexing, but also for the patterns and algorithms that distinguish our on/off line conduct. As we notice in the cases of this woman, in the case of Secrecy there is no specific 'warrantor' or protector: the amount of data that the citizen produces and stores on his behalf is permanently 'leakable' and potentially exposed and appears unprotect from public shaming. Data surveillance, along with its notorious revelations, to use Foucault words, becomes a machine that nobody controls, as it is one in which everyone is caught, those who exercise the power as well as those who are subjected to it.

The intimate pictures that may be and are produced with our contemporary phones are of a completely different nature: not only do they leave a trace in online searches and traffic, as discussed previously, but such content is stored in a single – and potentially in cloud – memory storage. Figuratively, it appears as if all books, CDs, tapes are all stored in a single shelf: yet this shelf contains both children material and 'Not Suitable For Work' selfies. With this perspective, the need to protect such 'shelf' from being viewed by others, with all possible technological means, sounds not only reasonable but vital.

Through the realm of secrets, that reveals itself as a border between public (front) and private (back), one evidently requires a technological keychain to be accessed, as an altogether new 'space' is formed: the secret non-place. This space is essential for exerting power: a central incognita in the exerting of a sort of secretive life, endorsed through the constant use of contemporary technologies. The secret ultimately leads to the formation of 'docile bodies', producers and yet subjects of their very secrets (stored and filmed). They, especially visible because of their social media activity, behave and act with their intentions and existence resulting hidden and thus secret, though pretending and expecting them to be not known to anyone else.

Final remarks

In this chapter, I have attempted to describe instances of the secretive milieu, and its counters - in its most natural and commonly observable and experienced form. The intention was to achieve, with this somewhat experimental methodology, the true glimpse of the onlife ecology, and the dynamics of suspicion, control and desire that are aroused within it. Some of the cases have been personally experienced, or recollected online, in blogs and forums. Also, their occurring has been fundamentally incidental, taking place

across countries in its most casual and trivial conditions. When talking to some of the people involved in the cases, their experiences where shared in respect to their 'data as given' formula. I have thus avoided to record and take notes of the events, but jumped into conversations and made treasure of their considerations. These elements helped to contribute into the living feeling that secretive conduct, albeit difficult to observe because of its nature, could be well considered and studied in relation to its abuse, especially when the specific circumstances of its conduct do not clearly draw a line in what is normative and what transgressive.
With the case studies, I have analysed a series of social vignettes , using the theories and concepts outlined in the theoretical framework of the thesis, where the secretive conducts transpire, along its abuse counter-part. Of all these instances, many more have been recollected and witnessed: more have been forwarded to me, though their recurrence appeared either difficult to approach academically, or sounded repetitive in the overall talking of the issue. The intention of this section was to underline the normative aspect of 'living with secrets', but also watching them, controlling them: keeping them always stored, always at hand, and yet always with an eye open to the secrets of others. Such condition appears the case by rephrasing a well-known saying: 'keep your friends close, but your enemies closer', by 'keep your secrets close, but your enemy's secrets even closer'. With such considerations in mind, the subtle variation between what is normative and what transgressive appears as vague as the online and offline existence: there simply appears to be no longer a border - just as, in the words of Bauman, there is a liquid state of permanent secrecy and the revelation/discovery of it. The backstage and frontstage, as advanced by Goffman, appear truly to have lost their meaning, not simply for what - last of all - Zuckerberg described as the 'end of privacy', but also connected to fictional Eric Cartman's statement of everything being of 'public domain'. Rather, it is the condition of ever-obsession with secrecy: the mask is no longer taken off, anywhere: because everywhere the public may enter the private. What transpires is the secretive conduct that overcomes all norms, while secretive conduct justifies all transgressions.

CONCLUSION

This work is the result of a seven-year study on different fields and themes, all twirling around the 'intuition' of something quite not right in our contemporary understanding of the use of secrecy, especially when we compare its understanding with themes such our privacy and the collection of 'data'. Because of a recurring change in supervisors and fields of interests, from sociology to criminology and zemiology it had needed all this time to indeed find a solid base on which to gravitate my thesis.
This thesis has given an account of, and the reasons for, the widespread use of secretive conduct and the toxic elements that replicate within its boundaries. It has done so by engaging with the onlife scenario, a blurring line between the on and off line existence of all global north users (and growing).

My original idea was that if it is true that never up to today we had access to so much data and information, the same could be said regarding the number of secrets users and citizens may obtain and conserve. These concentrate around a series of keywords this thesis used: surveillance of secrets, control of such data, and desire to hide or seek more of such data. Central importance of this approach, at times complex and necessitationg many re-writes, is that contemporary life has never been so ambiguous as today. This is especially true when we try to understand 'reality' of its existence and the multiple dimensions of its 'essence'. Our western-technocratic existences are fundamentally shared within an online, internet-induced, digital and especially 'virtual' world, combined with a concrete, 'in real life' (IRL), away-from-keyboard (AFK) and 'terrestrial' existence. My approach was to acknowledge that we could not limit our understanding in what is part of the cyberdimension, but it is a rather complex and growingly 'blurring' space. Indeed, we are possibly heading towards the virtual that may bleed into reality (Chalmers, 2017). As in many ways the current COVID-19 crisis is proving, our everyday life has become as elusive as ever: the digital media interacts and at the same time interferes with any media, and thus society itself. Within this sphere, secrets form and leak in continuous flow. In the same way, they are controlled and observed, covertly and unilaterally. Central for the conceptualisation of my thesis was also the acknowledgement that these elements of suspicion, control and desire take place both in corporate, data-mining agendas as well as in household, domestic values. The two intersect and aliment each other. We are part of a system of constant hiding and perpetual revelations, with very few examples, awareness and agency in regards of resistance and control.

Weakness and limitations

In the social and political theories, secret has been of ambiguous use, an essential characteristic to obtain power and to maintain it. Trying to understand what the dynamics of this condition have been one of the main difficulties. Studying secrets as discussed in the methodology is an ethically and methodological difficult theme. Secrecy is something that is not clearly visible. Problematic with what I've been researching has been that most people could've just made up what they told me. I have no way to prove otherwise. This is the power of influence. This is again why secrets are so important to be looked at. They can change and alter reality depending on how they looked upon. However, in this thesis, I did not try to decode secrets or their narratives. I tried to catch a glimpse of how secrecy is indeed surrounding us and how it's influencing all reality.

For this purpose, I tried to access the lives of individuals as an observant but nonetheless a participant one, that is somewhat external to devices and schemes that smart phones allow. This approach has allowed to access of findings and of information in a particularly novel form. However yet again it offers a glimpse that is specifically based on personal observations and personal consideration. Also, it was very hard throughout the entire thesis to maintain some sort of objective respect and trust for the onlife scenario. What I do offer some sort of recognition to its qualities, this own life scenario proves throughout of the thesis, the damaging and enduring reality we are nosediving into for at least two decades. Yet again it is difficult to discuss this without a

normative approach. I have not offered any particular solution if not in the final remarks of this concluding chapter. I do not have answers to how serious secretive conduct may become. How dangerous these new technologies are and what dangers we may be facing. However we put it, this is the reality that is surrounding us. And this is the research I've made out from it.
In the following sections, I will attempt to wrap up the concepts raised in the work, and try to offer a possible solution to the ecology of secrets and its ever-growing scenario. The secrets surrounding us appear a central element for oiling the desiring machine, It is also the fragile system and ecology within the forces of suspicion and control shift perpetually - an evident spiral to which the balance of abuse and stability is evermore hard to maintain. Technological tools, especially smart-induced devices, are particularly 'shady' and 'vicious' in promoting and replicating the secretive manoeuvres that consists of the every day life. They enforce the secretive conducts to the extreme of producing the cases of counter-counted characterized by suspicion, control and desire, that I have tried to analyse and discuss.

Focusing on the findings

One of the more significant findings to emerge from this study is that the individuals that engage in secretive conduct within the onlife scenario appear evidently blasé about the dynamics that involve them. Conversations and observations all suggest that there is a well aware 'concern' with the use and abuse of secretive conduct, but nevertheless appears as a recurring and normative aspect of onlife users. However, if we consider the relatively novel emergences of smartphone dynamics, the 'normality' of these recurring features of 'suspicion, control and desire' seem somewhat striking. As I have trying to analyse, user have long become accustomed to living in secrets, but this shift from being online and offline has proven an incredible set of new dynamics, that seems just 'what it is'. People can control, observe, record, watch and even literally 'spy' on others with very limit amount of 'resistance' or 'friction'. The justification of these dynamics seems to embrace conditions of 'safety', 'security' – especially within the dynamics of intimate relationships. There, to 'check upon', oftentimes in patronizing and hegemonistic conditions becomes a recurring aspect, that is only resisted with further 'hiding' and 'scheming'. Apps that allow forms of monitoring are 'neutralised' by simply agreeing that these Apps are, indeed, harmful and damaging for a number of reasons, one recurring being the idea of 'trust'. However, as we have discussed, the smartphone per se neutralises trust by its very design and features. It is evidently very diffictualt and demanding to base anymore relations simply on the trust that 'nothing bad will happen' or that each single member and party will 'behave'. Secretive elements of our everyday life, as I have described, have become so enthrenched into the everyday fabric that they have corrupted the basic notion of 'being' without having, or giving the impression, of having something to hide. Smartphones allow producing and at the same time potentially entering deep inside that hidden space, in covert and inconspicuous modes. It has become an integral and yet toxic element of our lives. In regard to secretive conduct, smartphones are not simply tools that allow constant and precise forms of

'contact', but they do so with latent features. They can record, film, monitor and spy without the user knowing so. And this does not necessitate any particular tech skill: it is an embedded aspect of their covert and 'fishy' design. While their harm and damage seem evident to most, they are an integral and inevitable aspect of the onlife scenario. While recurring encounters and conversations have ended with have praise and 'envy' my 'offlife' approach (of being without a smartphone), no one ever showed any intention of limiting or refusing their use. None of the people I have ever discussed my work, while perhaps nodding to the dangers of smartphones, has really changed his or her mind. While I will in the final section discuss how we can conceive of a different onlife reality, and different use of its tools, on no occasion, has any of the individuals I approached and observed made any indication that they could do without smartphones. It did not sound as even a possibility. This is an important point. It proves that while my arguments are not convincing, secretive conducts and its elements are something embedded that most society cannot do without.

Limitations of the current research

To address the use and misuse of a fundamental technology such a smartphone is still to date partially a controversial theme. Most of the literature still today focuses on the abuse of the secondary effects of smartphones, such as the data they produce, and the platforms it allows to access, but there is little focus on the actual device per se. To address a specific 'malevolence' and 'hazard' of the tools per se finds only literature within the 'conspiracy' agenda, one that insistently seeks the 'health' hazard truth of antennas, radiation and the likes. My interest has never been to enter in the merits of any of these arguments. Instead, this work acknowledges that many of the toxic aspect of these devices come from misuse of otherwise commercially interesting features. For example, the Black Box features of devices mentioned by Pasquale (2015) create covert data collecting tools that come to aid pharmaceutical and insurance companies. These aspects are well integrated within the devices as 'haptic' experiences, such as with smart watches, but offer other, less visible and covert reasons and results. They do offer what the costumers want – part of and fulfilling self-surveillance system and fetichism- but they also replicate the elements of suspicion, control and desire. This is perhaps an unintended result, but it is a palpable one. More study and investigation should be addressed towards it. However, in the current scenario, I could only offer the alternatives suggested in the final sections.

Everyday life of secrets

Approaching secrecy through the lens of a cultural criminologist, this work has produced an analysis on the cultural elements that surround the users behaviours conducted in secret – the elements in the everyday life that lead the very secretive conduct, oftentimes in a disinhibited condition and unaware environment. The culture of these elements, surrounded by device and biometric lock, are the core of the social harm associated to the onlife reality.

As we have examined, the current ecology of the onlife has reached a culminating point where in fear of being controlled we control each other with our every day technologies and gadget: stranger "voyeurs looking into your daily life" (Lyon & Bauman, 2013, p. 40) constantly monitoring each other's network profiles; home-installed security cameras brought on amazon or even Lidl for less than 60£; platforms enabled for checking chats and behaviour of siblings, employees, partners. Regarding such relation with technologies, modern cause and solution to all our strains, who claimed already fifty years ago how "any extension of ourselves" (McLuhan, 1967, p. 8), or, more plainly, "any new technology" changed, indeed our relationship with it changes.

Using (Foucault, 1975) and also (Nietzsche, 1887) we can recognize how we have long been living in an age of perpetual desire and will to 'know'. The technologies and systems surrounding us insists on this aspect, in order to control our very surroundings – the shape our essences in all political, capitalist, corporate institutions. The panopticon becomes only one of the many structures that aliment such requirement and desire – the rendering users mastered ad subjected by the very conduct the machines enforce on them. To become all watchful and at the same time all powerful – yet always protected in a sort of 'Goffmanian' comfort zone, aided by McLuhanian tools to detach oneself yet be always in control; perpetually mediated and yet perpetuating the illusion (or indeed, effect) of being always fully aware. Such full awareness of our surroundings, this 'need to know' aided by the mediated tools – without which none of these case studies could have taken place – is at the same time corresponding with the desire to be detached, to be able to see, control and observe without being seen, controlled and observed. The society surrounding us seems one where all technological interaction is mediated through a one-way mirror – just as the ones seen in movies' interrogation rooms. To be watched without knowing so seems fundamentally – and cinematographically – an aspect of true confession: who we really are, where nobody is watching. Goffman described much of this, in his Presentation of the Self, underlying nonetheless how even in these 'backrooms', where we act far from prying eyes, are also potentially modified, staged – and indeed easily observable. This, today, has become ever clearer, and almost self-evident.

Floridis' onlife reality underlines how turning off a computer does no longer 'log off' your online existence. They are one and the same thing. Simmel, in the analogy that I have tried to propose, seemed to offer the same consideration regarding our secret and public life. The two cannot be plainly nor easily separated, but rather they be directly dealt with and balanced. In this thesis, I have tried to underline how this balance is ever harder to attain, especially because the very mediums that surround us, rather than building walls – as they tend to claim with pin, passwords and privacy measures that are endlessly integrated – they evermore tear such walls down. We appear open and disassembled constantly by corporations, who sell us products and offer platforms where to navigate in the forms of 'capta', and at the same time, as noted in the case studies, tend to reintroduce the very dynamics in our everyday life. The tools/medium surrounding us become spaces where to store and hide data only to perpetually offer the means to dis-close and dis-cover the same data – turning effectively to reintroduce the same practices of 'capta'. The ecology of secretive onlife becomes thus per se a space where the secretive

conduct of suspicion, control and desire is a recurring feature, or indeed the only feature that allows the protection and at the same time the interaction among users.

This becomes an essential feature of everyday life: one where there is a constant requirement of one acting in secret – and perpetually leading a conduct in danger of a threat – and indeed the threats are practically everywhere and always at hand. Any computer, server, account may be hacked at any given time by any one at any price as all data may contain anything, even things that you had no idea that where stored – or what meaning do they have to a potential thief. No moment of the onlife ecology allows the user/citizen to 'lower' his defences, no backstage where to 'give up'- especially because it is the backstage that is most lucrative and generator of pricy secret 'capta'. Such 'capta' because fundamental tool of control, suspicious and desire within the couple and the intimate space, as we have discussed in the case studies. The modalities in which the 'capta' are gathered and achieved, the remote monitoring, distant observation – the recollection of information and forming of assumption - become everyday activities in which the algorithms described by Frank Pasquale seems to be imitated by human and social interactions, not the other way around. This other way around, namely that algorithms would appear to replicate human and social interaction, seems indeed with the case studies somewhat of an obsolescent consideration.

As we have seen in the cases study and the auto-ethnographic analysis of this work, the result is a society obsessed with hiding and perpetually curious in finding out what is being hidden, in every sphere: from the personal to the intimate, from the professional to the political; from the public to the private. The need to know, the desire to observe and the impulse to control have become central conditions of conflict, aided by a global insecurity and the wide distribution of monitoring devices. A locked phone is a treasure coffer, which we constantly carry and store with all its treasure in front of everyone. Nobody is allowed to know what's inside, because if we did, we would have to show what we also keep: even if there's nothing. The same aspect is evident with data and its recollection - the mining and the marketing. The onlife system promotes the distribution of tools to produce and at the same time divulge data - in other words secrets - info-instances of our lives and existences. In the terms of data-secrets, the Foucauldian Docility thus becomes central: our secrets, whatever their nature, must be kept and stored at all costs, for fear of their leakage: the password is an essential item for the new-century individual, that is perpetually in danger of being revealed, so it must be complicated, cyphered and protected from visible and invisible menaces. Reality is constantly put in question, with virtual secrets 'bleeding' into physical 'intimate' spaces is the fundamental understanding of the onlife nature (Floridi, 2015)As we have discussed, the effect is one of turning blasé to our secrets in our online navigation, accepting terms and conditions, downloading apps, accustomed to data breaching, collecting and reselling data, though somewhat blasé concerning what it all implies. A hyperreal reality that have become our new norm: camera and algorithms can recognize and identify us globally, and we in turn seem to be not only accustomed, but take advantage of their presence. We repeat their functions and elaborate their processes in a series of instance we have described in the case studies. This counter-conduct of perpetual suspicion, control and desire - aided by the smart-induced technological tools - become a system to which we may hardly find exit. It is an ever-englobing phenomena: the secretive existence becomes per se a 'suffocating' reality, as

analysed on a psychological level by (Slepian, 2019). But how can we indeed seek a liberation from such formula and hazards?

Research answers

All in all, this work was inspired by a number of insights, themes and experiences that led to the idea that something was not quite right in our contemporary understanding of the technological gestation of our 'secrets'. To develop the framework and tools to properly engage with the ecology of its features, I have first incidentally, then purposefully, side-lined myself from using social networks, thus social media, and eventually avoiding categorically the use of smart phones and correlated technology. I have thus engaged in a (partial) offlife existence, that I sensed could offer a 'fresh' prospective on the secretive conduct all smart-phone users relate to, willingly and oftentimes unconsciously. Indeed, my theoretical baseline appealed to the idea that, if it is true that up to today we never had access to so much data and information, the same could be said regarding the number of secrets users and citizens may obtain and conserve. These considerations concentrate around a series of keywords analysed throughout this thesis, in light of their secretive use: surveillance, control, and transparency. In the social and political theories secrecy has been of ambiguous use, an essential characteristic to obtain power and to maintain it. Hence, my project aimed in:

1. Outlining the circumstances of every day secretive conduct in the onlife ecology, derived by an incessant global concern with privacy and produced by our daily engagement with 'onlife' and fundamentally 'smart' technological devices.
2. Recollecting/Analysing from a cultural criminology perspective the change in social environments caused by the influence of these mediums and the deviant effect it has on every day interactions
3. Interpreting the specific elements of secretive conduct formed by instances and repetitive occurrence of suspicion, control and desire.
4. Witnessing and introducing the vignettes as theoretical framework recollecting instances of secretive conduct in the everyday ecology of the onlife, specifically in cases of surveillance and control – especially in domestic spaces.
5. Offer considerations of possible alternatives and resolutions to the ever-growing spiral of transgressive, abusive and malignant onlife conduct and technological advancement 'in the wrong direction'.

In trying to answer in a coherent manner the themes and key questions posed throughout the thesis, we have thus recognized and outlined a series of issues that may be summarized as such:

1 The onlife is one of extreme information flow and endless conditions of engagement. It appears truly as the ultimate objective of the internet – one that has been promoted and enforced by Big Tech gurus since the infosphere influence. Its elements of information exchange, societal building, and general human progression have nonetheless been paralleled by several criminological topics – from surveillance, social control, and cyber-crime – all aspects that have been at least mentioned throughout the thesis. More specifically, the deviant elements have emerged concerning secretive conduct – in detail the modes in which the onlife ecology favours an englobing condition where the deviant elements of permanent suspicion, control and desire arise and are enforced?. Deviance appears central in the unclear distinction of what we should do and can do with these new smart tools surrounding us. The new ethics that need to be posed in controlling our children, observing remotely our partners, peaking within our colleague's browser history – a future frontier in with the disinhibition appears central and normative. Secrecy thus represents the Gyges ring we may all wear to conduct these actions, but also the environment that allows the trivial modalities for these actions to take place.

2 The correlation between deviance and technology is a controversial theme that needs to be addressed with caution and another Ph.D. altogether. However, this work has specifically analysed the theoretical and indeed practical instances with which the smart technology – and in specific the smartphone – allows the proliferation of a certain and novel characteristic of deviance: secretive conduct. This may take place in any environment: in a perfectly remote and private condition. It requires secrecy and involves secrecy – it seeks to protect one's secrets while engaging and surfacing others. One may look up, control, and observe one's existence at all instances – do so in secret – as a perfectly panoptic environment- whilst being observed and controlled by another. What is controlled, observed, and viewed returns to the constant variation of this work. Not simply someone's data – but 'secrets' – they themselves become the central element of interest in any interaction – the things hidden – either willingly or not. But what is hidden, and why? Oftentimes, as we have discussed, there is nothing specific being hidden: the system itself, the protected yet flowing information creates itself instances of perpetual suspicion, control, and desire of anything stored- for whatever purpose. Secrets gather and are exchanged behind the false pretence of being data: therefore, they are so controversial and valuable.

3 The elements to make sense of such a system again are not per se fallacious and indeed enter within a cultural analysis of the trivial, unaware elements of deviance and criminology. The cheapness of specific technologies, the easy availability and plug-and-play features may produce – and have done so – a condition where it may appear 'ok' to monitor our children or spouses. With the rapid implementation, it may just as well socially accepted or simply normalized that specific abuses may take place – without even being time (or place) to address the issue and highlight its dangers. As shown in the case studies, a cheap CCTV camera brought in a supermarket to monitor the domestic space against

burglars may become a tool to monitor and 'check on' family members. This is because potentially the child may be observed but does not know it. No mother is never informed when the camera is turned on. And when she does, oftentimes, as in the case study, the end justifies the means – or it is fun. The remote, high-speed internet connection becomes in this perspective enough of a Pandora box that allows all these instances. The smart device, its free apps, and HD resolution are enough to propagate its abusive counters. Again, it is central to underline the agency element that is fundamental in every user. We do nonetheless underline that the onlife is exactly characterized by an odd blurring whereas the rapid changes; the vantage of technical grasp; the secretive/hidden feature of the tools; allow all the engagement with deviant conduct either we are aware or not.

4 Given the analysis undertaken in this thesis, the panoptic elements seem to have become integrated within our society. But this is nothing new. Rather, the panoptic society has turned into a total institution where not only everything is potentially monitored and observed, but it is stored and gathered: no clear distinction is made between the 'inside' and the 'outside'. The users, just as inmates described by Goffman, need to perpetually 'check in', prove their identity, their conformity – and the blurring line between the front and backstage lose its track. In the onlife ecology, the secretive conduct appears as a way out – as to finally be in private, find a 'secret' space within the onlife. Nonetheless, such perspective is rather an illusion. Secretive conduct is not the 'way-out' for an over-oppressive panoptic environment – but rather the inserting of the very panoptic elements even closer inside our personal space. Instead, as I will discuss in the concluding remarks, we must engage in a 'forgetting' non-space. Allow an element of 'offlife' – where data is not captured – nor secrets endless pile up within our existences and their clones in our servers.

If we agree that the principal questioned raised in this work have been appropriately answered, or at least properly addressed, we may further consider the implication of this concept: where do they come from and where do they lead.

Resisting the 'formation' of smart-secrets

As suggested by *(Ziccardi, 2015)*, while navigating the web, one may use TOR browsers that allow users to maintain their IP address anonymity (without necessarily hiding their browsing history). One may make easily use of a temporary email address, avoid using ordinary credit cards by preferring cash transactions, using crypto-currency so as to avoid leaving traces – or even using less complex/smart phones, without traceable features such as cameras or GPS.

Regarding the notion of surveillance and monitoring, nothing prevents future technologies to progress into a less invasive form of security and control, promoting for example motion sensor alarms surrounding certain areas, rather than remote cameras:

these would be still effective yet not gathering and potentially misinterpreting the data of anyone 'filmed' in the area. The same can take place with the self-destruction of data on a regular basis, both manually than automatically. Users could, and should, attempt to 'restart fresh' their social media accounts on a regular basis, so as to 'relieve' the weight of information available on them (at least publicly): deleting unused contacts, posts, images. By damning (damnum- guilt) them, in other words, from digital memory. Such data – that necessarily must be distinguished as 'capta' - would still remain on most corporation's servers for a number of years on servers, proving how these 'tabula rasa' *(Nietzsche, 1887, p. 35)* schemes are still possible today, but possibly only for a limited time.

On these note, as suggested by Rodota', data/'capta' may be ideally programmed to self-destruct itself automatically on a regular basis, cleaning itself with some sort of timer from servers and search algorithms: a concept similar to the Snapchat images that may be viewed only for a single, temporary occasion. Such approach would become central, as Pasquale (2015) noticed, also to prevent the algorithm discrimination – and the social sorting instances denounced by *(Lyon, 2003)*. Secretive conduct, in its most cultural and criminological conception, would cyclically lose, regardless, its influence and basic weapons for suspicion, control and desire.

All these are not only legal and non-criminal solutions, but promote a non-suspicious behaviour to personal peers: our activities are more open, less ambiguous. They are 'there' to question and even debate, not arousing nonetheless suspicion or ambiguity, quite the opposite, they cannot contain as 'secrets' anything that otherwise surround us. The lack of any technological or shift into this possibility proves the value, and importance, of our data in the contemporary web service and experience.

Surveillance without control?

As we have seen, much of the themes in this work revolve around the idea of surveillance, the desire to see what surrounds us, the suspicion that something is going on while we are not aware of it, while at the same time we want to have control over it. The results of such conditions are easily recognizable with the current 'army' of security systems, both at homes and in workplaces, in retail shops and on public transportation, extending to leisure and even education. Any space requires an object that knows what is going on and who are present, even with some assurance concerning their direction or motivations. Surveillance becomes thus a condition, as we have seen in *(Lyon & Bauman, 2013)*, of constant monitoring, controlling, and preventing, in a potentially surreal and limitless installation of tools. We may nonetheless play with the idea of what could be alternative technologies, as a kind of 'forma mentis' that may somewhat 'release the pressure' of this trap of Suspicion, Control and Desire counter-conduct. Regarding technology, an evident problem lies in the object and use of lens/camera. It allows the view of a determinate space, with ideally a viewer (or the threat of one) that monitors remotely whoever enters the space, or behaves suspiciously. This technology is being evermore integrated with microphones, motion sensors, alarms, face-recognition and night vision. Lens have become a fundamental feature of social interaction, a tool which we seem cannot do without – and indeed we cannot buy devices lacking it. Also, we have

seen how some of these technologies, cheaply available on most e-commerce services, promote hidden, conceit solutions- invisible to strangers or anyone filmed. The conditions of such tools are odd for a number of reasons, as we have seen: there is the problem of privacy, of 'misinterpreting' information, of social sorting, and especially it is problem when used as an actual prevention of crime. A funny anecdote told me by a local officer can be used to prove the paradox of this condition: the villas on the Florentine hills are since years being broken into by what appears to be the same dealer. He has a warehouse nearby, and has been repeatedly been arrested. Nonetheless, he manages to get away most of times, because he films the breaking into the houses with his phone. By this, if caught, during trial he manages to prove he is actually a thief, not a dealer. The first is a minor, somewhat victimized accusation, the second a serious offence. This is an evident case of sousveillance, where the thief actually films the crime as to prove his partial involvement: the surveillance camera does not scare him off, nor accuse him: it is an alibi.

The perspective of home security should be intrinsically reconsidered, preferring eyes in the home that indeed exert some sort of control over the situation area 'visual' property, rather some sort of 'sensory'-veillance. Smart sensors would come to aid in the surrounding spaces, doors and walls, only activated in case of proximity or actual contact. There would be no need to 'record' and 'hold' audio/visual data, product further 'capta' that perpetuate the secretive control-conduct. Instead, by 'passively' have sensors in alert, rather than in observation, such system could become ideally, a return to the notion of a watchdog: he does not know what he is seeing, he just knows if it's right or not. This as we mentioned before, such approach would come hand in hand with the notion of custody- protect rather than store-hide away.

Other issues though may be raised: surveillance without control could intend a smaller need for hiding, as what is to be seen is visible, according to a common agreement. Concepts of social surveillance or community surveillance have been brought forward by Bauman (coining 'liquid insecurity') and even Eric Fromm (To Have or To Be?). In their perspective, the (re-)formation of an actual community would help 'self-monitoring'. In criminology, such notion could be connected to the Theory of Defensible Space developed by Oscar Newman in 1972. Newman studied how the opportunity of crime, the diffusion of fear of crime, and the perception of security among citizens are influenced by the urban and architectural environment of a determinate area. Indeed, Newman noticed how the possibility that determinate crimes may take place grows considerably in presence of buildings with hidden entrances or scarcely illuminated areas; inside courts and non-visible gardens. Thus, Newman affirmed that an adequate mean of prevention is constituted by a specific type of architectural design that maximizes the 'defensible space' of community residents. From this theory derives a policy orientation aimed at the reduction of crime rates and of perceived insecurity by operating the right changes to the urban structure: the construction of buildings supplied with well visible entrances and exits, a reduction of badly illuminated zones, the collocation of gardens and courts near non-isolated streets, and the subdivision of the city in less extended areas, more easily controllable by the population and the police force *(Triventi, 2007, p. 2)*.

Of course, the gap between control and lack of freedom is somewhat thin: the 'deviant' would 'gently' feel constantly observed, and thus prevented from actions, just as ideally cameras do now. The stranger, entering such a minimized community (read also ghetto) would immediately raise concerns of 'suspicion, control and desire'. It appears that the issue raised may be only solved in the micro-level, with the requirement of public space being considerably reduced and/or constantly monitored.

Transporting the issue online, the idea of a defensible space easily falls into the idea of a 'gentrified' one, where the unregulated digital world would be neatly, monetarily, and obediently channelled. This is a thesis brought forward by Jessa Lingel (2019), who noticed "a connected but separate set of issues in the kinds of online spaces and relationships that are increasingly encouraged or restricted online". By calling the contemporary internet gentrified, Lingel's goal "is both to diagnose a set of problems and lay out what internet activists can do to carve out more protections and spaces of freedom." *(Lingel, 2019)*. Facebook/Meta becomes a prime example, offering a clean, safe, censured environment, where users are prevented from touching certain topics, posting certain content, and are 'gently' invited to behave properly by 'moderators' and fellow users, and thus returning to the theories of Trottier on Social Media as Surveillance *(Trottier, 2015)*.

Crash or land?

The vision of our future, tech-obsessed and docile to its influence, fill dystopian novels since possibly industrialisation itself. From Zamyatin, Orwell to Huxley, just to mention the most notable, we have seen words of producers and soldiers, all rigorously subject and obsessed by order. Such perspective is a known debate, to which uncountable authors have offered different perspective. Interesting, among the many, is French writer Houlellebecq's consideration that we cannot do anything against social change: all society is on a flying plane, to which perhaps the pilot cabin is empty: without direction nor a lead. We'll want perhaps to eventually find out who actually is piloting, take over and control of the plane: but to go where? We have, after all, built ourselves this machine, we've taken off (conscious or not)… but where will it lead us?

Such metaphor of the plane connects broadly to another writer, Saint-Exupery (expert plane pilot and author of the Little Prince (1943)) - who in his 'Land of Men' offers a significant consideration on machines and mediums. Saint-Exupery discusses the connubiality between instruments and their pilots - specifically the plane - and how their relations, from an initial fear and 'friction', somewhat dissolves, turning into some sort of 'home'. The machine - just as today's smartphone - as it fine-tunes becomes invisible behind its function – in other words, normative, not so scary, and also not that influent. This invisibility is important to mention, as in Part 2 we have insisted that it is one of the fundamental elements of smart-device-induced secretive conduct. We have interpreted its fishy, elusive elements as central for producing secretive conducts, described in the case studies. Yet machines, for the French writer, exactly as part of their quality during its evolution, dissimulate. The perfecting of their invention lies in the eventual absence of its invention.

It is in this consideration, one we may connect with the already mentioned 'Thumbelina' by Serres, that we may find the somewhat re-equilibrizing element of smart-device abuse: one where its power of influence over our conduct, our essences and secretive realms is no longer powerful: it may no longer catch our attention, and our existence, in such fashion: turning from a deviant perspective into a normative reality. In a post-pandemic era, where indeed we have witnessed an unforeseen abundance of smart-device use – and indeed the inflation of its controlling elements – we may take this opportunity to reconsider our use, re-calibrate its significance in our everyday life.

Offlife ecology

The secretive conduct, in such condition, would loosen its grip over the most intimate aspects of our lives. A solution, as suggested by my auto-ethnographical considerations, is perhaps to attempt an offlife subcultural existence, even if only partially. This idea, forwarded for example but not being necessarily restricted to smartphone usage, allows the user not to produce incessant content and 'capta' food. The simple/basic gsm phone (though it is uncertain for how long compatible with current antennas) offers for the time being a device that still represents some communication qualities that are deterrent of the secretive conduct. Its SMS may be read by anyone finding the phone, picking it up. Does this make it less of a protecting/protected machine? After all, anybody finding your personal notebook, with scribbled thoughts and ideas, has the similar 'insight' in your lives. Yet they are fragments: and this is the central difference between smart phones and gsm technologies. The smartphone embraces all aspects of our lives, the gsm only offers partial 'windows' – SMS, some pictures, phone numbers (with often contact naming). The design of its features renders them cheap 'informationally': they own very little on us. They can vaguely be used against us. They are not 'loaded guns'.

But other technologies may also be considered in the 'smart' hemisphere. A somewhat sensible rendezvous point was achieved in the first models featuring iPod Touch technology. Such device offered smart features – such as gaming, internet navigation, picture taking and social networking, but its main feature – and reason of purchase – was listening to music. This is important as the device, among many others, maintained its purpose, while the 'phone' affix to hardly implied the need to 'converse' with one another. The smartphone has gained innumerable meanings to this day and age, with ever more purposes with its 360degrees worthwhile apps (even allegedly to halt the COVID spread). In the iPod Touch instead, though being still part of the smart device 'arena', offering a 'touch screen' and apps usage, does not possess a GPS system, nor allows mobile data (thus no compatibility WhatsApp), nor again owns any touch ID or Face ID protective tech – fundamental features abused in the secretive conduct. It is not strictly speaking a dual-usage device. It is not a medium between harm and care.

Summary and Contribution

In summary, we must underline the dangers and misconceptions of what an onlife ecology is and what it may become. The ecological problems with smart technology compatible with secretive conduct are:

- mobile data connectivity: because of its perpetual onlife connection, the devices are always at hand and 'connected to the net'. Its invasive aspect, the possibility to be always online, update and synchronized is inevitable. Wi-Fi based devices, such as computer and tablets do not offer such a feature, having rather an 'unconnected' function. They can go 'offline' – or indeed could, technically, function perfectly without ever be connect to the web. They per se allow a secretive conduct.
- GPS: the satellite positioning system is integrated into most smart devices, including cars and computers. Nonetheless, its features are strictly smart and most surely avoidable and unnecessary. Other than for navigation purposes, their features are solely one of tracking – an object that is strictly in need of protection from most users, yet it is basically implemented and endorsed. Interesting in this context is the recent tracker devices that bring the GPS monitoring outside of the smartphone – rendering surveillance ever more trivial.
- camera integration: appear 'intrinsically' part of every mobile device, indeed lenses may represent the main and most popular features of the secretive conduct, with its abusing risks. This is no place to question this 'plethora' of lenses, though one may doubt the actual need to record – whatever the quality – all of these instances our life. As understood through Vaidyanathan work, never as today have we been surrounded by so many tools to film and record. In this reality, we are evermore 'under the eye' – perpetually under surveillance and 'blasé' to this very surveillance. By achieving an offlife reality that is less implemented by cameras, we could possibly achieve an environment with less 'requirement' to report, record and prove our whereabouts, our peers and whoever we frequent.
- 'fishy'/ hidden features - lacking of led/lights or sounds clearly signalling recording/filming that are per se features of smart phone. As shown in the case studies, it is exactly this ambivalence, and lack of clarity, that allow users to film and record, though giving barely any signal that they are doing so.

The Offlife 'paradoxical' reality that is being described would thus imply the use of the same tools, only coming to terms with its most 'invasive' features – ones that come to terms with the 'data' as given and not bend to the 'capta' dynamics. Again, this work wishes in no way to aggregate itself to a luddite or *passéiste* agenda. Rather, it sought to find more meaningful and compatible ways to 'live' our technologies, as not become outlived by them. To avoid, strictly speaking, the totalitarian aspect of the onlife institutionalizations. In accordance with Stefana Broadbent and Claire Lobet-Maris, writing for the Onlife Manifesto, "Ecology is also a means of spreading forms of cultural vigilance which can be promoted in schools and the media." The requirement and care in developing and seeking " 'clean technologies'— that is, technologies which are sustainable in respect to our attention and our capacity of self-determination and accountable regarding the processes they perform to fabricate identities and differences" (Broadbent & Lobet-Maris, 2015, p. 112)

In this perspective, the *offlife* ecology would presuppose an environment where users are more in control of their information and their secrets: they can share without being afraid that in some years' time anything published would come back on them. This is the philosophy behind recently popular private messaging service Signal launched in 2014, who's CEO Moxie Marlinspike specifically noticed how "Anything that I've ever written or created, one way or another, about anything is sort of embarrassing to me a month later. Even more so five years later." (Wiener, 2020). For Marlinspike, true encryption would allow users to 'take back their privacy'. This work is not sure about this statement, but agrees that indeed, anything online on us needs to be offered a true 'great reset' – at least on a regular basis. The need for all our data – even when published voluntarily – to free itself from a *'capta'* establishment that perpetuates the conditions of suspicion, control and desire: one that to this date are only fought with privacy, secrecy and deceit. To know who is watching, when, why and for what purpose. And within the domestic space, to create ethics on what is allowed to be seen, managed, stored. To render clear what is 'not ok' – and truly 'odd', 'weird', 'not cool' - with a clear, coherent agenda. This is central and need of an imminent position as what we have talked about are not-on-the-surface conducts that differ in every family and ever couple – yet all share the same potentially free apps, inconspicuous smart-phone use and e-commerce platform. What would appear perfectly normal is one family (spying over children) would appear scandalous in another, without each other ever knowing of such difference.

In an age of strong liberal values, and decade long battles against bias, it should be granted we should no longer live in the embarrassment of who we were, what we appear to have been, or appear to be today as compared to what we were. Most of all, none of the technologies that indeed perpetuate *'capta'* conditions should not constrain us, of in fact lead us to transgression among each other, only because they have rendered the possibility trivial and always at hand. To this reality, I rather opt out going offlife. By mid 2022, it still is a (partial) possibility. Tomorrow, it may become harder and could require even more tools, a specific 'obfuscation' – forms of sousveillance and whatnot. Or perhaps, on the contrary, technologies will truly head towards a new perception of the data as given; smart technology more 'clever-oriented', and thus less abusive and invasive: helpful in selecting 'data' rather than delivering 'capta' – deleting unused information and clearing navigation cookies on a regular basis. More than that, perhaps it will be preventing users from falling into the trap of the secretive conduct, and thus limiting all those instances of monitoring, control, conceit, counterfeit, latency, surveillance and other terms of everyday abuse we seem to have become 'desensitized'. Technologies, in other words, that are not simply concerned in the immediate profit of producers and aiding the power of governments, but indeed attempt to foresee 'checks and balances' for decades to come.

More could have been said also in reference to the COVID-19 pandemic, especially with regards to the new domestic dynamics caused by lockdown constrictions and the social distancing protocols in increasing, enhancing and refile secretive conduct in the entire onlife scope: again, it is perhaps too early to draw conclusions (not to mention that is difficult to continue my form of ethnography, given the social restrictions. It appears clear

that whatever is ahead of us is filled, evermore, of unwrapped variations of what of secrecy to which we have built codes and walls – and we cannot climb over nor see beyond the view they've covered.

Again, it might become a more 'clever technology', a form and tool of communication, exchange, sociability and engagement of what we could be proud of in years to come, and not one we wish we never owned: the one that contains all the secrets and mistakes we again and again feel the need to hide.

BIBLIOGRAPHY

Statista Research Department, 2021. *Facebook: number of monthly active users worldwide 2008-2021.* [Online]
Available at: https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/
[Accessed 23 08 2021].

ABC News, 2016. *'Webcam hackers caught me wanking, demanded $10k ransom'.* [Online]
Available at: https://www.abc.net.au/triplej/programs/hack/webcam-hackers-catch-man-wanking-demand-ransom/7668434

Agamben, G., 2005. *Homo Secer.* 2005 ed. Milano: Enauidi.

Agamben, G., 2009. *What is an Apparatus?.* 1st ed. Standford: Standford University Press.

Akers, R. L., 1998. *Social Learning and Social Structure.* Boston: Northeastern University Press.

Albrechtslund, A., 2008. Online Social Networking as Participatory Surveillance. *First Mondays.*

Allen, A., 2011. *Unpopular Privacy.* UK: Oxford University Press.

Anderson, M., 2017. *Many smartphone owners don't take steps to secure their devices.* [Online]
Available at: https://www.pewresearch.org/fact-tank/2017/03/15/many-smartphone-owners-dont-take-steps-to-secure-their-devices/
[Accessed 03 12 2021].

Andrews, P., 1992. Pc In Your Pocket: Bill Gates Previews Wallet That Knows You Well. *The Seattle Times*, 02 02.
Angwin, J., 2015. *Dragnet Nation A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance.* NY: St. Martin's Griffin.
Anon., 1865. Riding the Stang. *Cork Examiner*, 28 08.
Apple Inc., 2008. *Apple Sells One Million iPhone 3Gs in First Weekend.* [Online]
Available at: https://www.apple.com/newsroom/2008/07/14Apple-Sells-One-Million-iPhone-3Gs-in-First-Weekend/
[Accessed 10 01 2021].
Apple.com, 2018. *Augmented Reality.* [Online]
Available at: https://www.apple.com/ios/augmented-reality/
[Accessed 28 Nov 2019].
Apple, 2015. *Apple Support.* [Online]
Available at: https://support.apple.com/en-us/HT201857
[Accessed 14 05 2021].
Apple, 2017. *Apple Support.* [Online]
Available at: https://support.apple.com/en-us/HT1820
[Accessed 14 05 2021].
Arcangelis, M. d., 1987. *La Storia Dello Spionaggio Elettronico.* Milan: Mursia.
Aries, P., 1960. *Centuries Of Childhood.* s.l.:Penguin Books.
Back, L., 2007. *The art of listening.* Oxford: Berg.
Barron, C. M., 2013. 'I had no credit to rng you back': strategies of negotiation and resistance to parental surveillance via mobile phones. *Surveillance and Society,* 12(3), pp. 401-413.
Baudelaire, C., 1863. *The Painter of Modern Life & Other Essays.* s.l.:Phaidon Press.
Bauman, Z. & Lyon, D., 2013. *Liquid Surveillance.* 1st ed. Cambridge: Polity Press.
Becker, H. S., 1962 [1997]. *Outsiders.* Ebook: Free Press.
Beer, D., 2016. *Metric Power.* London: Palgrave Macmillan (UK).
Beer, D., 2016. *The Metric Power.* London: Palgrave Macmillan UK.
Beer, D., 2017. *Algorithms: the villains and heroes of the 'post-truth' era.* [Online]
Available at: https://www.opendemocracy.net/en/digitaliberties/algorithms-villains-and-heroes-of-post-truth-era/
Beer, D., 2017. *Algorithms: the villains and heroes of the 'post-truth' era.* [Online]
Available at: https://www.opendemocracy.net/en/digitaliberties/algorithms-villains-and-heroes-of-post-truth-era/
[Accessed 10 09 2021].
Beer, D., 2021. *The end of social media.* [Online]
Available at: https://davidbeer.substack.com/p/when-will-we-stop-calling-social
[Accessed 04 01 2021].
Benţa, M. I., 2020. *The "new normal" is at the doors. Here are a few tips for your techno-dictatorship survival kit.* [Online]
Available at: https://www.bentza.com/the-new-normal-is-at-the-doors-here-are-a-few-tips-for-your-techno-dictatorship-survival-kit/
[Accessed 15 04 2021].
Benjamin, W., 2002. *The Arcades Project.* Harvard: Harvard University Press.

Bickert, M., 2018. *Publishing Our Internal Enforcement Guidelines and Expanding Our Appeals Process.* [Online]
Available at: https://about.fb.com/news/2018/04/comprehensive-community-standards/
Bigo, D., 2008. Globalized (In)Security: The field and the Ban-Opticon. In: *Terror, Insecurity and Liberty. Illeberal practices of liberal regimes after 9/11.* NY: Routledge, pp. 10-48.
Boland, T. & Griffin, R., 2015. *The Sociology of Unemployment.*. Manchester: Manchester University Press.
Bowles, N., 2018. *Thermostats, Locks and Lights: Digital Tools of Domestic Abuse.* [Online]
Available at: https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html
Broadbent, S. & Lobet-Maris, C., 2015. Towards a Grey Ecology. In: L. Floridi, ed. *Onlife Manifesto.* Open Springler: Springler, pp. 111-124.
Brown, M. & Carrabine, E., 2017. *Routledge International Handbook of Visual Criminology.* 1st ed. London: Routledge.
Brunton, F. & Nissenbaum, H., 2015. *Obfuscation, A User Guide.* Cambridge: MIT.
Brunton, F. & Nissenbaum, H., 2016. *Obfuscation: A User's Guide for Privacy and Protest.* Cambridge: MIT Press.
Burke Winkelman, S. et al., 2015. Exploring Cyber Harrassment among Women Who Use Social Media. *Universal Journal of Public Health,* 3(5).
Burkert, W., 1987. *Ancient Mystery Cults.* s.l.:Harvard University Press.
Burt, A. & Geer, D., 2017. The End of Privacy. *New York Times,* 5 October.
Calasso, R., 2019. *The Marriage of Cadmus and Harmony.* s.l.:Penguin Classics.
Cambell, Z. & Jones, C., 2020. *Leaked Reports Show EU Police Are Planning a Pan-European Network of Facial Recognition Databases.* [Online]
Available at: https://theintercept.com/2020/02/21/eu-facial-recognition-database/
[Accessed 25 02 2020].
Canetti, E., 1984. *Crowds and Power.* UK: Farrar, Straus and Giroux.
Canetti, E., n.d. *Crowds and Power.* s.l.:s.n.
Canon, G., 2020. *Facebook's 'monopoly' must be split up, US and states say in major lawsuits.* [Online]
Available at: https://www.theguardian.com/technology/2020/dec/09/facebook-lawsuit-antitrust-whatsapp-instagram-ftc
[Accessed 05 01 2021].
Carratelli, C. b. G. P., 2001. *Lamine D'Oro Orfiche.* 3rd ed. Milan: Adelphi.
Castillo, M., 2012. *Survey: 75 percent of Americans admit to using phone while in bathroom.* [Online]
Available at: https://www.cbsnews.com/news/survey-75-percent-of-americans-admit-to-using-phone-while-in-bathroom/
Ceres, P., 2022. *Kids Are Back in Classrooms and Laptops Are Still Spying on Them.* [Online]
Available at: https://www.wired.com/story/student-monitoring-software-privacy-in-schools/
[Accessed 08 08 2022].

Chalmers, D., 2017. *A Conversation With David Chalmers.* [Online]
Available at: https://www.edge.org/conversation/david_chalmers-the-mind-bleeds-into-the-world
Chen, J., 2017. *5-star vs. thumbs-up: When to use which rating system.* [Online]
Available at: https://www.appcues.com/blog/rating-system-ux-star-thumbs
Choe, E. K. et al., 2011. Living in a Glass House: a survey of private moments in the home. *UbiComp'11.*
Christl, W., 2017. *CORPORATE SURVEILLANCE IN EVERYDAY LIFE,* Vienna: Cracked Labs.
Christl, W. & Spiekermann, S., 2016. *Network of Control,* Wien: Facultas Verlags.
Citron, D. K., 2009. Law's Expressive Value in Combating Cyber Gender Harassment. *Michigan Law ReviewMic,* 108(03).
Clement, J., 2019. *Statista.* [Online]
Available at: https://www.statista.com/statistics/433871/daily-social-media-usage-worldwide/
[Accessed 22 11 2019].
Cohen, S., 1972. *Moral Panics and Folk Devils.* New York: Routledge.
Cooper, J., 2018. *Smile! Police will soon be filming you as body worn cameras are introduced.* [Online]
Available at: https://www.plymouthherald.co.uk/news/plymouth-news/smile-police-soon-filming-you-1954506
Couch, D. L., Robinson, P. & Kamesaroff, P. A., 2020. COVID-19—Extending Surveillance and the Panopticon. *Journal of Bioethical Inquiry* , 25 08.
Council of Europe, 2020. *AI and control of Covid-19 coronavirus.* [Online]
Available at: https://www.coe.int/en/web/artificial-intelligence/ai-and-control-of-covid-19-coronavirus
[Accessed 27 May 2020].
Davis, M., 1990. *City Of Quarz.* July 2018 ed. s.l.:Verso.
Dearden & Parti, 2021. Cybercrime, diffential association, and self-control: knowledge transmission through online social learning. *American Journal of Criminal Justice,* Volume 46.
Deleuze, G., 1992. Postscript on the Societies of Control. *October,* Volume 59, pp. 3-7.
Deleuze & Guattari, 1972. *Anti Oedipus.* 2000 ed. Minneapolis: University of Minnesota Press.
Dodds, E. R., 1951. *The Greeks and the Irrational.* Oakland: University of California Press.
Drucker, J., 2011. Humanities Approaches to Graphical Display. *Digital Humanities Quaterly,* 5(1).
Duck Duck Go, 2017. *A Study on Private Browsing:Consumer Usage, Knowledge, and Thoughts,* Paoli (US): s.n.
dw.com, 2022. *German police under fire for misuse of COVID contact tracing app.* [Online]
Available at: https://www.dw.com/en/german-police-under-fire-for-misuse-of-covid-contact-tracing-app/a-60393597
[Accessed 10 04 2022].
Economist, 2020. *Creating the coronopticon.* [Online]
Available at: https://www.economist.com/briefing/2020/03/26/countries-are-using-

apps-and-data-networks-to-keep-tabs-on-the-pandemic
[Accessed 04 05 2021].
Eikren, E. & Ingram-Waters, M., 2016. Dismantling 'Your Get What Your Deserve': Towards a Feminist Sociology of Revenge Porn. *Ada New Media,* Issue 10.
Elliott, M., 2012. *Find someone's Amazon Wish List by his or her e-mail address.* [Online]
Available at: https://www.cnet.com/how-to/find-someones-amazon-wish-list-by-his-or-her-e-mail-address/
European Commission, 2013. *The Onlife Initiative: concept reengineering for rethinking societal concerns in the digital transition,* s.l.: s.n.
Faulkner, W., 2003. *Privacy.* Milano: Adelphi.
Feloni, R., 2014. *Peter Thiel explains how an esoteric philosophy book shaped his worldview.* [Online]
Available at: https://www.businessinsider.com/peter-thiel-on-rene-girards-influence-2014-11?r=US&IR=T
[Accessed 31 08 2021].
Feloni, R., 2014. *Peter Thiel explains how an esoteric philosophy book shaped his worldview.* [Online]
Available at: https://www.businessinsider.com/peter-thiel-on-rene-girards-influence-2014-11?IR=T
Ferrell, J., 1996. *CRIMES OF STYLE Urban Graffiti and the Politics of Criminality.* Boston: Northeastern University Press.
Ferrell, J., 1999. Cultural Criminology. *Annual Review of Sociology,* pp. 395-418.
Ferrell, J., Young, J. & Hayward, K., 2008. *Cultural Criminology.* s.l.:s.n.
Finley, K. & Pearstein, P., 2020. *The WIRED Guide to 5G.* [Online]
Available at: https://www.wired.com/story/wired-guide-5g/
[Accessed 16 06 2021].
Finos, A., 2019. *Paolo Genovese: "Al nostro cinema in crisi servono sceneggiatori".* [Online]
Available at: https://www.repubblica.it/spettacoli/2019/07/15/news/paolo_genovese-300872447/
[Accessed 11 10 2021].
Floridi, L., 1999. *Philosophy and Computing: An introduction.* New York: Routledge.
Floridi, L., 2015. *The Onlife Manifesto: Being Human in a Hyperconnected Era.* Open Access: Springer.
Forssell, R., 2016. Exploring cyberbullying and face-to-face bullying in working life – Prevalence, targets and expressions. *Computers in Human Behavior,* Volume 58, pp. 454-460.
Fors, V., Pink, S., Berg, M. & O'Dell, T., 2019. *Imagining Personal Data.* New York: Routledge .
Foucault, M., 1975. *Sorvegliare e Punire.* 2004 ed. Milano: Enauidi.
Foucault, M., 1978. *Security, Territory, Population.* 2009 ed. s.l.:Picador.
Foucault, M., 1978. *The History of Sexuality Vol. 1.* 1st American Edition ed. New York: Pantheon Books.
Foucault, M., 1978. *The History Of Sexuality Volume I: An Introduction.* USA: Random House.

Foucault, M., 1979. Life of Infamous Men. In: *Power, Truth, Stragegy*. 2006 ed. s.l.:McArthur Press, pp. 76-92.
Foucault, M., 1983. PREFACE. In: *Anti-Oedipus*. s.l.:University of Minnesota.
Fowler, G. A., 2012. *When the Most Personal Secrets Get Outed on Facebook*. [Online]
Available at:
https://www.wsj.com/articles/SB10000872396390444165804578008740578200224
Fowler, G. A., 2020. *At CES, Apple, Facebook and Amazon are preaching privacy. Don't believe the hype.*. [Online]
Available at: https://www.washingtonpost.com/technology/2020/01/08/ces-apple-facebook-amazon-are-preaching-privacy-dont-believe-hype/
[Accessed 11 10 2021].
Frazer, S. J. G., 1890. *The Golden Bough: A study of magic and religion*. s.l.:Project Gutenberg.
Frisby, D., 1985. *Fragments of Modernity*. 1986 ed. New York: Routledge.
Furedi, F., 2019. Fear Today. *First Things: A Monthly Journal of Religion and Public Life,* Volume 289.
G.T. Marx, V. S., 2010. Marx, G., & Steeves, V. (2010). From the beginning: Children as subjects and agents of surveillance. *Surveillance and Society,* 7(3/4).
Garland, D., 1986. Foucault's "Discipline and Punish. *American Bar Foundation Research Journal,* 4(11), pp. 847-880.
Gasser, U. et al., 2020. Digital tools against COVID-19: Framing the ethical challenges and how to address them. *Berkman Klein Centre for Internet & Society*.
Gasser, U. et al., 2020. Digital tools against COVID-19: taxonomy, ethical challenges, and navigation aid. *Lancet Digital Health,* Volume 2, p. e425–34.
Gates, B., 1995. *The Road Ahead*. NY: Viking Books.
Ghazi-Tehrani, A. K. & Pontell, H. N., 2021. Phishing Evolves: Analyzing the Enduring Cybercrime. *Victims and Offenders,* 16(3).
Giddens, A., 1991. *Modernity and Self-Identity: Self and Society in the Late Modern Age*. Cambridge: Polity.
Giesbrecht, D., 2017. *This is how Netflix's top-secret recommendation system works*. [Online]
Available at: https://www.wired.co.uk/article/how-do-netflixs-algorithms-work-machine-learning-helps-to-predict-what-viewers-will-like
[Accessed 03 12 2021].
Giglioli, M. F., 2019. *I Labirinti della Sorveglianza Informatica*. Milano: Il Mulino.
Girard, R., 1972. *Violence and the Sacred*. 2005 ed. London: Continuum.
Girard, R., 2017. *Anoressia e desiderio mimetico*. Turin: Edizioni Lindau.
Goffman, E., 1956. *Presentation of the self in everyday life*. 1971 ed. London: Pelican Press.
Goffman, E., 1961. *Asylums*. 1991 ed. London: Penguin Books.
Goffman, E., 1961. *Asylums : essays on the social situation of mental patients and other inmates*. New York: Penguin.
Google Inc, 2022. *Help your family create healthy digital habits*. [Online]
Available at: https://families.google.com/familylink/
[Accessed 28 02 2022].
Google.Support, 2020. *FAQs on privacy: Google Nest*. [Online]
Available at:

https://support.google.com/googlenest/answer/9415830?co=GENIE.Platform%3DAndroid&hl=en
[Accessed 06 01 2021].
Gordon, F., McGovern, A., Thompson, C. & Wood, M. A., 2020. Beyond Cybercrime: New Perspectives on Crime, Harm and Digital Technologies. *International Journal for Crime, Justice and Social Democracy.*
Gottfredson, M. R. & Hirschi, T., 1990. *A general theory of crime.* Stanford: Stanford University Press..
Greenberg, A., 2014. *Google Can Now Tell You're Not a Robot With Just One Click.* [Online]
Available at: https://www.wired.com/2014/12/google-one-click-recaptcha/
[Accessed 11 02 2021].
Gregg, M., 2013. Spousebusting: Intimacy, adultery, and surveillance technology. *Surveillance & Society,* 11(3), pp. 301-310.
Guerra, C. & Ingram, J. R., 2022. Assessing the Relationship between Lifestyle Routine Activities Theory and Online Victimization Using Panel Data. *Deviant Beheviour,* Volume 43.
Guttari & Deleuse, 1972. *Anti Oedipus.* s.l.:s.n.
Habermas, J., 1989. *The Structural Transformationof the Public Spher.* Cambridge: Cambridge.
Hall, E. T., 1966. *The Hidden Dimension.* New York: Anchor Books.
Han, B.-C., 2012. *The Transparent Society.* 2015 ed. Standford: Stanford University Press.
Harridge, E., 2020. *What is SMART workplace technology? And how can it help businesses return to the office in the new COVID-19 normal..* [Online]
Available at: https://www.unico.com.au/insights/smart-workplace-technology/
[Accessed 21 03 2021].
Hatmaker, T., 2019. *Instagram and Facebook will start censoring 'graphic images' of self-harm.* [Online]
Available at: https://techcrunch.com/2019/02/07/instagram-self-harm-cutting-facebook/
Heidegger, M., 1967 (1998). *Pathmarks.* 1st ed. UK: Cambridge University Press.
Herrero, J. et al., 2021. Smartphone Addiction and Cybercrime Victimization in the Context of Lifestyles Routine Activities and Self-Control Theories: The User's Dual Vulnerability Model of Cybercrime Victimization. *Int J Environ Res Public Health,* 18(07).
Hess, A., 2020. *The Social-Distancing Shamers Are Watching.* [Online]
Available at: https://www.nytimes.com/2020/05/11/arts/social-distance-shaming.html
Hillyard, P. a. T. S., 2004. *Beyond Criminology. Taking Harm Seriously.* London: Pluto Press.
Hoffower, H., 2019. *Mark Zuckerberg spent almost $60 million on 2 waterfront estates in Tahoe last winter. Here's a look at the 10 properties he owns across the US, from a modest Palo Alto home to a Hawaiian plantation..* [Online]
Available at: https://www.businessinsider.com/mark-zuckerberg-real-estate-lake-tahoe-palo-alto-hawaii-2019-5?IR=T
[Accessed 03 04 2021].
Horst, H., 2020. Friendly Social Surveillance . In: *Kinship through Data.* Amsterdam: Amsterdam University Press.
Jaishankar, K., 2007. Establishing a Theory of Cyber Crimes. *International Journal of Cyber Criminology,* 1(2).

Johnson, B., 2010. *Privacy no longer a social norm, says Facebook founder.* [Online]
Available at: https://www.theguardian.com/technology/2010/jan/11/facebook-privacy
[Accessed 22 02 2020].
Jung, C., 1961. *Memories, Dreams, Reflections.* 1965 ed. NY: Vintage Books.
Kane, S., 2004. The unconventional methods of cultural criminology. *Theoretical Criminology,* 8(3).
Kapaló, J., 2020. *Faith – Trust – Secrecy: Religion Through the Lenses of the Secret Police.* Budapest: Vera and Donald Blinken Open Society.
Kaufmann, M., 2021. This Is a Secret: Learning From Children's Engagement With Surveillance and Secrecy. *Cultural Studies ↔ Critical Methodologies,* 21(5), pp. 424-437.
Kelly, H., 2021. *For seniors using tech to age in place, surveillance can be the price of independence.* [Online]
Available at: https://www.washingtonpost.com/technology/2021/11/19/seniors-smart-home-privacy/
[Accessed 06 12 2021].
Kerenyi, K., 1979. *Miti e Misteri.* Turin: Boringhieri.
Kirkpatrick, D., 2010. *The Facebook Effect.* NY: Simon & Schuster.
Kirn, W., 2007. *The Autumn of the Multitaskers.* [Online]
Available at: https://www.theatlantic.com/magazine/archive/2007/11/the-autumn-of-the-multitaskers/306342/
Kirn, W., 2015. *If You're Not Paranoid, You're Crazy.* [Online]
Available at: https://www.theatlantic.com/magazine/archive/2015/11/if-youre-not-paranoid-youre-crazy/407833/
[Accessed 01 09 2021].
Koch, R., 2020. *Cookies, the GDPR, and the ePrivacy Directive.* [Online]
Available at: https://gdpr.eu/cookies/
Koselleck, R., 1988. *Critique and Crisis.* Oxford: Berg Publishers.
Koselleck, R., 1988. *Critique and Crisis.* s.l.:Berg Publishers.
Kracauer, S., 1974. The Spectator. In: M. a. Cohen, ed. *Film Theory and Criticism.* New York: Oxford University Press.
Kumar, P., Gruzd, A. & Mai, P., 2021. Mapping out Violence Against Women of Influence on Twitter Using the Cyber-Lifestyle Routine Activity Theory. *American Behavioral Scientist,* 65(5).
Lane, J. D. & Wegner, D. M., 1995. The cognitive consequences of secrecy.. *ournal of Personality and Social Psychology,* 2(69), p. 237–253.
Lanier, J., 2010. *You Are Not a Gadget.* New York: Penguin Random House.
Lanigan, R. L., 1994. Capta versus Data: Method and Evidence in Communicology. *Human Studies,* Jan.17(1).
Leach, N., 1997. *Rethinking Architecture: A Reader in Cultural Theory.* s.l.:Routeledge.
Lessing, L., 1999. *Code and Other Laws of Cyberspace.* NY: Harper Collins.
Lieber, C., 2018. *Amazon's Alexa might be a key witness in a murder case.* [Online]
Available at: https://www.vox.com/the-goods/2018/11/12/18089090/amazon-echo-alexa-smart-speaker-privacy-data
[Accessed 05 12 2021].

Lingel, J., 2019. *The gentrification of the internet.* [Online]
Available at: http://culturedigitally.org/2019/03/the-gentrification-of-the-internet/
[Accessed 26 02 2020].
Livingstone, S., 2002. *Young People and New Media: Childhood and the Changing Media Environment.* https://dx.doi.org/10.4135/9781446219522: SAGE Publications Ltd.
Livingstone, S., 2009. *Kids Online.* Cambridge: Polity Press.
Lord, E., 2008. *The Hell-Fire Clubs: Sex, Satanism and Secret Societies.* Yale: Yale University Press.
Lovink, G., 2007. *Zero Comments: Blogging and Critical Internet Culture.* London: Routledge.
Lovink, G., 2011. *Networks without a cause: A critique of social media.* Cambridge: Polity Press.
Lovink, G., 2019. *Sad by Design.* London: Pluto Press.
Lowry, P. B., Zhang, J., Wang, C. & Siponen, M., 2016. Why Do Adults Engage in Cyberbullying on Social Media? An Integration of Online Disinhibition and Deindividuation Effects with the Social Structure and Social Learning Model. *Information Systems Research,* 27(4).
Lyon, D., 1994. *Electronic Eye: Rise of the Surveillance Society.* Cambridge: Polity Press.
Lyon, D., 1994. *Electronic Eye: Rise of the Surveillance Society.* s.l.:s.n.
Lyon, D., 2001. *Surveillance Society: Monitoring Everyday Life.* New York: McGraw-Hill Education (UK).
Lyon, D., 2003. *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination.* London: Routledge.
Lyon, D., 2009. Surveillance, Power and Everyday Life. *Oxford Handbook of Information and Communication Technologies* .
Lyon, D., 2018. *The Culture of Surveillance: Watching as a Way of Life.* London: Polity Press.
Lyon, D., 2020. *Pandemic, surveillance culture and data justice.* [Online]
Available at: https://www.biennaletecnologia.it/sessioni/pandemia-cultura-della-sorveglianza-e-data-justice-pandemic-surveillance-culture-and-data
[Accessed 08 01 2021].
Lyon, D. & Bauman, Z., 2013. *Liquid Surveillance.* Cambridge: Polity.
Mahdawi, A., 2022. *In-person teaching has resumed in the US – but electronic snooping hasn't stopped.* [Online]
Available at: https://www.theguardian.com/commentisfree/2022/aug/06/school-surveillance-software-students-week-in-patriarchy?CMP=Share_iOSApp_Other
[Accessed 08 08 2022].
Mann, S., 2016. Surveillance (oversight), Sousveillance (undersight), andMetaveillance (seeing sight itself). *IEEE Conference on Computer Vision and Pattern Recognition Workshops.*
Marcum, C. D., Higgins, G. E. & & Nicholson, J., 2017. I'm watching you: Cyberstalking behaviors of university students in romantic relationships.. *American journal of criminal justice,* 42(2).
Marx, G. T., 1998. Ethics for the New Surveillance. *The Information Society,* 14(3).
Matei, A., 2022. *'I was just really scared': Apple AirTags lead to stalking complaints.* [Online]
Available at: https://www.theguardian.com/technology/2022/jan/20/apple-airtags-stalking-complaints-technology
[Accessed 23 06 2022].

Mathiesen, T., 1997. The Viewer Society: Michel Foucault's `Panopticon' Revisited. *Theoretical Criminology*, 01 05, 1(2).
Mauss, M., 1966. *The Gift.* London: Cohen & West.
Mauss, M., 2016. *La nozione di persona. Una categoria dello spirito.* s.l.:Morcelliana.
McCarthy, P. A., 1984. Zamyatin and the Nightmare of Technology (Zamyatine et le cauchemar de la technologie). *Science Fiction Studies.*
McLuhan, M., 1964. *Understanding media : the extensions of man.* 1994 ed. Massachusetts: M I T Press edition.
McLuhan, M., 1967. *The Medium is the Massage: An Inventory of Effects.* UK: Penguin Books.
Medium, 2019. *Everything You Need To Know About Internet Cookies.* [Online]
Available at: https://medium.com/online-io-blockchain-technologies/everything-you-need-to-know-about-internet-cookies-2eb4aa85dd02
[Accessed 08 09 2021].
Melendez, S. & Pasternack, A., 2019. *Here are the data brokers quietly buying and selling your personal information.* [Online]
Available at: https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information
[Accessed 12 02 2021].
Melossi, D., 2008. *Controlling Crime, Controlling Society.* Cambridge: Polity.
Momigliano, A., 1931. *Claudio Imperatore.* [Online]
Available at: https://www.treccani.it/enciclopedia/claudio-imperatore_%28Enciclopedia-Italiana%29/
[Accessed 04 01 2021].
Mordini, E., 2008. Nothing to Hide Biometrics, Privacy and Private Sphere. *Springer-Verlag Berlin Heidelberg.*
Mordini, E., 2011. Pulcinella's Secrets. *Bioethics*, Volume 9.
Morse, J., 2019. *Fight facial-recognition technology with Phantom glasses.* [Online]
Available at: https://mashable.com/review/review-reflectacles-phantom-anti-facial-recognition-technology-glasses-frames
[Accessed 05 12 2021].
Nelson, M. K. & Garey, A. I., 2009. *Who's Watching? Daily Practices of Surveillance among Contemporary Families.* Nashville: Vanderbilt University Press.
New York Times, 2021. *German Intelligence Puts Coronavirus Deniers Under Surveillance.* [Online]
Available at: https://www.nytimes.com/2021/04/28/world/europe/germany-coronavirus-deniers-surveillance.html?action=click&module=Top%20Stories&pgtype=Homepage
[Accessed 10 04 2022].
Newton, L., 2018. *Beards, business and a history of facial hair in the workplace.* [Online]
Available at: https://theconversation.com/beards-business-and-a-history-of-facial-hair-in-the-workplace-107126
[Accessed 20 08 2021].
Nielsen, 2020. *COVID-19: Tracking the Impact on Media Consumption.* [Online]
Available at: https://www.nielsen.com/us/en/insights/article/2020/covid-19-tracking-

the-impact-on-media-consumption/
[Accessed 26 08 2021].
Nietzsche, F., 1887. *Genealogy of Morals.* 2006 ed. Cambridge: University Press.
Nietzsche, F., n.d. *On The Genealogy Of Morals.* s.l.:s.n.
O'Dea, S., 2021. *Number of smartphone users by leading countries as of May 2021 (in millions)*.* [Online]
Available at: https://www.statista.com/statistics/748053/worldwide-top-countries-smartphone-users/
[Accessed 03 12 2021].
OECD, 2020. *Tracking and tracing COVID: Protecting privacy and data while using apps and biometrics.* [Online]
Available at: http://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protecting-privacy-and-data-while-using-apps-and-biometrics-8f394636/
[Accessed 15 May 2020].
Oulasvirta, A. et al., 2012. Long-term effects of ubiquitous surveillance in the home. *UbiComp '12.*
Papadopoulou, L. & Maniou, T. A., 2021. Digital Media and New Forms of Journalism. *Encyclopedia of Information Science and Technology,.*
Parker, R., 1990. *Miasma Pollution and Purification in Early Greek Religion.* Oxford: Clarendon Press.
Pasquale, F., 2015. *The Black Box Society: The Secret Algorithms That Control Money and Information.* Cambridge (MA): Harvard University Press.
Paul, K., 2019. Zuckerberg defends Facebook as bastion of 'free expression' in speech. *The Guardian*, 17 10.
Pausanias, 1971. *Guide to Greece. Central Greece. Vol. 1.* s.l.:Penguin.
Peters, M., 2008. *The Paradox of Self-Promotion with Social Media.* [Online]
Available at: https://www.socialmediatoday.com/content/paradox-self-promotion-social-media
[Accessed 05 01 2021].
Pettit, H., 2018. *Privacy International.* [Online]
Available at: https://www.dailymail.co.uk/sciencetech/article-5262297/Facebook-track-using-dust-camera-lens.html
Pham, S., 2019. *TikTok hit with record fine for collecting data on children Sherisse Pham byline.* [Online]
Available at: https://edition.cnn.com/2019/02/28/tech/tiktok-ftc-fine-children/index.html
[Accessed 25 02 2020].
Pianigiani, 1907. *Vocabolario Etimologico.* Florence: Albrighi & Segati.
Pink, S. et al., 2015. *Digital Ethnography.* Sydney: SAGE.
Pizzorno, A., 2007. *Il velo della diversità. Studi su razionalità e riconoscimento.* Milano: Feltrinelli.
Pizzorno, A., 2008 [1960]. *Sulla Maschera.* Bologna: Il Mulino.
Plato & Bloom, A., 1991. *The Republic of Plato.* 2nd ed. USA: Basic Books.
Porro, G., 2020. *Twitter segnala il primo deepfake. E indovinate chi l'ha postato? Trump.* [Online]

Available at: https://www.wired.it/internet/social-network/2020/03/09/twitter-trump-deepfake/
[Accessed 20 09 2021].
Priest, D. & Martin, T., 2021. *Security camera hacking: It can happen to you. Here's how to stop it.* [Online]
Available at: https://www.cnet.com/news/best-home-security-systems-comcast-xfinity-vivint-simplisafe-and-more/
[Accessed 26 08 202].
Przybylski, L., 2020. *Hybrid Ethnography.* CA: SAGE.
Pullen, J. P., 2011. *How Vimeo became hipster YouTube.* [Online]
Available at: https://fortune.com/2011/02/23/how-vimeo-became-hipster-youtube/
[Accessed 25 02 2020].
Putnam, R. D., 2001. *Bowling Alone: The Collapse and Revival of American Community.* NY: Simon & Schuster.
Rajaraman, S., 2009. *Five Stars Dominate Ratings.* [Online]
Available at: https://youtube.googleblog.com/2009/09/five-stars-dominate-ratings.html
Redden, J., Brand, J. & Terzieva, V., 2020. *Data Harm Record.* [Online]
Available at: https://datajusticelab.org/data-harm-record/
[Accessed 05 12 2021].
Reinstein, J., 2018. *The Instagram DM Heart Is The Easiest Way To Embarrass Yourself Online And It Must Be Destroyed.* [Online]
Available at: https://www.buzzfeednews.com/article/juliareinstein/instagram-dm-heart
[Accessed 10 09 2021].
Rodanthi, T., Majid, Y. & O'Brien, M., 2005. 'Con me if you can':Exploring crime in the Americancinematic imagination. *heoretical Criminology,* 9(1), pp. 97-117.
Rodotà, S., 2005. *Intervista su Privacy e Liberta.* Milano: Laterza.
Rodota, S., 2002. *Discorso del prof. Rodotà di presentazione della RELAZIONE PER L'ANNO 2001,* Rome: Garante per la Privacy.
Rodota', S., 2014. *Il mondo nella rete. Quali i diritti, quali i vincoli.* Rome: Laterza.
Rooney, T., 2010. Trusting Children: how do you surveillance technology is alter a child experience of trust, risk and responsibility.. *Surveillance and society,* 7(3/4), pp. 344-355.
Rudolph, K., 1983. *Gnosis: The Nature and History of Gnosticism.* New York: Harper & Row.
Russo, S., 1957. Data vs. Capta or Sumpta. *American Psychologist,* 12(5).
Sawers, P., 2018. *Amazon-owned Ring embraces neighborhood watch with home security networking app.* [Online]
Available at: https://venturebeat.com/2018/05/08/amazon-owned-ring-embraces-neighborhood-watch-with-home-security-networking-app/
[Accessed 13 05 2021].
Sennett, R., 1974. *Fall of Public Man.* 1992 ed. USA: W.W. Norton & Company.
Serres, M., 2012. *Thumbelina.* 2015 ed. USA: Rowman & Littlefield.
Sexton, J., 2018. *Divorce Lawyer: Facebook Is a Cheating Machine.* [Online]
Available at: https://time.com/5208108/facebook-cheating-infidelity-divorce/
Shariff, S., 2014. *Sexting and Cyberbullying.* Cambridge: Cambridge University Press .

Sharma, S., 2008. Art of Listening By Les Back. *British Journal of Sociology*.
Simmel, G., 1906. "The Sociology of Secrecy and of Secret Societies". *American Journal of Sociology ,* Volume 11, pp. 441-498.
Simmel, G., 1906. The Sociology of Secrecy and of Secret Societies. *American Journal of Sociology (AJS),* pp. 441-498.
Simmel, G., 1971. The Metropolis and Mental Life. In: D. N. Levine, ed. *Georg Simmel on Individuality and Social Forms.* Chicago: University of Chicago Press.
Simmel, G., 1997. Bridge and Door. In: *Rethinking Architecture: A Reader in Cultural Theory.* UK: Routledge.
Slepian, M. L., 2019. Confiding Secrets and Well-Being. *Social Psychological and Personality Science,* 10(4).
Slepian, M. L., Chun, J. S. & & Mason, M. F., 2017. The experience of secrecy. *Journal of Personality and Social Psychology,* 113(1), pp. 1-33.
Smith, A., 2009. *Josh Harris: The Warhol of the web.* [Online]
Available at: https://www.theguardian.com/film/2009/nov/04/josh-harris-we-live-public
Smith, B., 2020. What's Facebook's Deal With Donald Trump?. *NY Times*, 21 06.
Solon, O., 2017. *Facebook asks users for nude photos in project to combat 'revenge porn'.* [Online]
Available at: https://www.theguardian.com/technology/2017/nov/07/facebook-revenge-porn-nude-photos
[Accessed 25 02 2020].
Solove, D., 2011. *Nothing to Hide: false tradeoff between Privacy and Security.* New Haven: Yale University Press.
Sotgiu, S., 2021. *Green pass e hacker, l'Italia onlife di Draghi vista da Floridi.* [Online]
Available at: https://formiche.net/2021/08/green-pass-e-hacker-litalia-onlife-di-draghi-vista-da-floridi/
[Accessed 03 09 2021].
Spencer, S., 2020. *Netflix Movies: The 10 Most-Watched In September.* [Online]
Available at: https://www.newsweek.com/netflix-most-watched-movies-september-2020-films-social-dilemma-smurfs-1534933
[Accessed 11 01 2021].
Spiekermann, S., 2017. The Challenges of Privacy by Design. *Communications of the ACM ,* March, Volume 7, pp. 34-37.
Spiekermann, S. & Christl, W., 2016. *Networks of Control – A Report on Corporate Surveillance, Digital Tracking,* January: Facultas.
Srinivasan, R. & IlamParithi, V., 2018. A Study on Interpersonal Surveillance on Social Media Using WhatsApp. *Portrayal of Social Issues in Literature and Media,* 18(9).
Steeves, V., 2020. A dialogic analysis of Hello Barbie's conversations with children. *Big Data & Society,* 12(1).
Steeves, V. & Jones, O., 2010. Editorial: Surveillance and children. *Surveillance & Society,*.
Sticotti, P., 1931. *ARREFORIE o Erreforie.* [Online]
Available at: http://www.treccani.it/enciclopedia/arreforie-o-erreforie_(Enciclopedia-Italiana)/
[Accessed 02 02 2020].

Szakolczai, J. M., 2012. *Electronic Solitudes- BA dissertation,* Ireland: University College Cork.
Szakolczai, J. M., 2021. 'What have you caught?' Nannycams and hidden cameras as normalised surveillance of the intimate. In: M. I. B. Paul O'Connor, ed. *The Technologisation of the Social.* s.l.:Taylor & Francis, p. 14.
Takahashi, T. T., 2012. DRONES AND PRIVACY. FALL, Issue XIV.
The Economist, 2020. *Creating the coronopticon.* [Online]
Available at: https://www.economist.com/briefing/2020/03/26/countries-are-using-apps-and-data-networks-to-keep-tabs-on-the-pandemic
[Accessed 04 12 2021].
Thompson, C., 2020. Worried About Privacy at Home? There's an AI for That. *Wired,* 28 02.
TikTok, 2020. *Our Mission.* [Online]
Available at: https://www.tiktok.com/about?lang=en
[Accessed 25 2 2020].
Tokunaga, R. S., 2011. Social networking site or social surveillance site? Understanding the use of interpersonal electronic surveillance in romantic relationships. Computers in human behavior. *Computers in human behavior,* 27(2).
Touma, R., 2021. *Clubhouse app: what is it and how do you get an invite to the exclusive audio app?.* [Online]
Available at: https://www.theguardian.com/technology/2021/feb/17/clubhouse-app-invite-what-is-it-how-to-get-audio-chat-elon-musk
[Accessed 09 12 2021].
Treccani, 2021. *Vignetta.* [Online]
Available at: https://www.treccani.it/vocabolario/vignetta/
[Accessed 14 05 2021].
Triventi, M., 2007. *Segni di inciviltà sul territorio e "paura" del crimine. Un'analisi dei dati dell'Indagine sulla sicurezza dei cittadini,.* [Online]
Available at: http://www.soc.unitn.it/ais-trento2007/papers/Triventi.pdf
Trottier, S., 2015. *Social Media as Surveillance.* US: Taylor & Francis Ltd.
Truffaut, F., 1966. *Hitchcock/Truffaut.* s.l.:Simon & Schuster.
Turkle, S., 2010. *Alone Together.* s.l.:Basic Books.
Turkle, S., 2011. *Alone Together: Why We Expect More from Technology and Less from Each Other.* 3rd, 2017 ed. New York, N.Y: Basic Book.
Ulanoff, L., 2014. *Amazon Knows What You Want Before You Buy It.* [Online]
Available at: https://mashable.com/2014/01/21/amazon-anticipatory-shipping-patent/?europe=true
[Accessed 25 02 2020].
Vaidhyanathan, S., 2018. *Antisocial Media.* UK: Oxford University Press.
Vakhitova, Reynal & Townsley, 2022. Online Routine Activities and Self-Guardianship Against Cyber Abuse. *Victims and Offenders,* Volume online.
Verde, A., Fleetwood, J., SANDBERG, S. & PRESSER, L., 2022. *The Third Narrative Criminology Symposium.* Genova, s.n.
Verdery, K., 2014. *Police, Secrets and Truth: Ethnography in the Archive of Romania's Secret.* Budapest: Central European University Press.

Virilio, P., 1998. *The Information Bomb.* 2000 ed. London: Verso.
Virilio, P., 2010. *Grey Ecology.* New York: Atropos Press .
Wacquant, L., 2001. The Penalisation of Poverty and the rise of Neo-Liberalism. *European Journal on Criminal Policy and Research ,* Issue 9, pp. 401-412.
Wacquant, L., 2004. *Body & Soul.* Oxford: Oxford University Press.
Wallace, R. S., 1998. *Calvin, Geneva and the Reformation.* 1st ed. US: Wipf and Stock.
Wall, D. S., 2020. *(Reverse) Double Jeapoardy: Are Universities as Modern Complex Organisations becoming the New Target for Cybercriminals and Spies?.* [Online]
Available at: https://www.emphasis.ac.uk/2020/09/16/reverse-double-jeapoardy-are-universities-as-modern-complex-organisations-becoming-the-new-target-for-cybercriminals-and-spies/
[Accessed 26 04 2021].
Warren, S. D. & Brandeis , D. L., 1880. The Right to Privacy. *Harvard Law Review,* 4(5).
Wiener, A., 2020. *Taking Back Our Privacy.* [Online]
Available at: https://www.newyorker.com/magazine/2020/10/26/taking-back-our-privacy
[Accessed 05 03 2021].
Wilde, O., 1889. *The Decay of Lying – An Observation.* London: The Nineteenth Century.
Woodcork, J. & Graham, M., 2020. *Gig Economy.* Cambridge: Polity.
Woollacott, E., 2018. *Facebook Reveals Its Secret Rules For Censoring Posts.* [Online]
Available at: https://www.forbes.com/sites/emmawoollacott/2018/04/24/facebook-reveals-its-secret-rules-for-censoring-posts/#6d2560b056da
Wuyts, D., Vansteenkiste, M., Mabbe, E. & Soenens, B., 2017. Effects of Social Pressure and Child Failure on Parents' Use of Control: An Experimental Investigation. *Contemporary Educational Psychology,* October.
Yar, M., 2005. The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory. *European Journal of Criminology,* 2(4).
Yar, M., 2012. Recognition as the Grounds for a General Theory' of Crime a Social Harm?. In: *Recognition Theory as Social Research: Investigating the Dynamics of Social Conflict.* Basingstoke: Palgrave.
Yar, M., 2014. *The Cultural Imaginary of the Internet: Virtual Utopias and Dystopias.* UK: PALGRAVE MACMILLAN.
Yar, M., 2017. Toward a Cultural Criminology of the Internet. In: *Technocrime and Criminological Theory.* New York: Routledge.
Yeats, F. A., 1966. *The Art of Memory.* 1984 ed. London: ARK PAPERBACKS.
Zarsky, T. Z., 2016. Incompatible: The GDPR in the Age of Big Data. *Heinonline.*
Ziccardi, G., 2015. *Internet, Controllo e Libertà.* Milano: Raffaello Cortina.
Ziccardi, G., 2019. *Tecnologie per il Potere.* 1st ed. MIlano: Raffaele Cortina.
Zuboff, S., 2019. *The Age of Surveillance Capitalism.* UK: Profile Books Ltd.
Zuckerberg, M., 2018. *A Blueprint for Content Governance and Enforcement.* [Online]
Available at: https://www.facebook.com/notes/mark-zuckerberg/a-blueprint-for-content-governance-and-enforcement/10156443129621634/