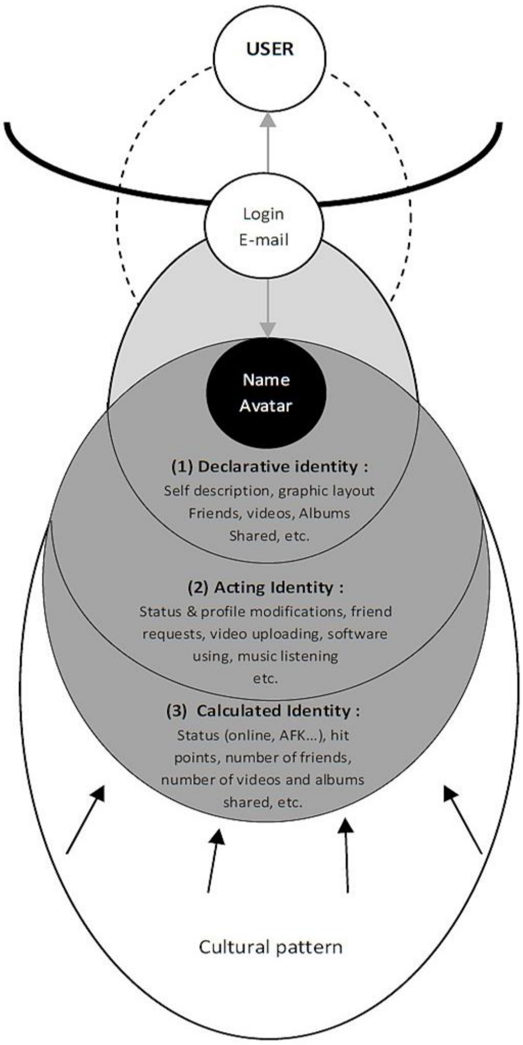
DIGITAL IDENTITY

Why to regulate?

The problem is that not all daily users are aware of the term digital identity, or in what context it is used. Some may believe that it somehow connected to some sci-fi futuristic ideas of modern world that is not influenced by their daily life and digital consumption.

Digital identity can be defined as both the collection of traces (writings, audio/video content, forum messages, sign-in details, etc.) that we leave behind us, consciously or unconsciously, as we use the platform, and the reflection of this mass of traces as it appears after being "remixed" by search engines (Ertzscheid, 2016). Alternatively, „Digital identity is a dynamic map based on the information available on the internet about a person or a brand (digital footprint), as well as the perceptions this information generates in third parties (digital reputation)" (Orihuela, 2017).

Figure 1: Digital Identity Model


USER
Login
E-mail
Name
Avatar
(1) Declarative identity :
Self description, graphic layout
Friends, videos, Albums
Shared, etc.
(2) Acting Identity :
Status & profile modifications, friend
requests, video uploading, software
using, music listening
etc.
(3) Calculated Identity :
Status (online, AFK...), hit
points, number of friends,
number of videos and albums
shared, etc.
Cultural pattern

Source: Georges, 2017

A seemingly fundamental difference between the real life identity and digital identity is that within digital identity one can choose more or less exactly how one would like to portray herself (including using real name or partially disguised /avatars, pseudonymity/ or totally concealed /anonymity, identity theft/misappropriation/ and what one decides to share with others. However, still, digital identity is imperfect. Babb (2016) suggests that we should see social media as epideictic discourse—as rhetoric that routinely constructs and displays small pieces of our digital identities. Ertzscheid (2016) identified three key features of digital identity. First, there is granularity: fragmented and piecemeal, underexposed yet over documented traces of digital identity. Second, these identity fragments, and the means by which they are accessed, are naturally porous. The different platforms where we publish fragments of our digital identity are increasingly, and ever more systematically, interconnected. Third, Ertzscheid sees there a feature of percolation. In other words, digital identities are like water droplets percolating through sand.

No wonder that Szymielewicz (2019) argues that digital identity is less a reflection of somebody than a caricature. This is so since the most valuable data about us is inferred beyond our control and without our consent.

Nonetheless, on the one hand, freedom to have to a certain degree personally adjusted digital identity can be liberating for people who may face discrimination in their everyday lives. On the other hand, organisations and individuals can also suffer from being confused with fake accounts (either spoofs or with more malicious intent) that have similar names to their own. There are some common sense recommendations how to protect ones digital identity (see Gibbons, 2018 and Orihuela, 2017).

People leave traces in digital world in similar way to those footprints the police or forensic scientists use to track down criminals (Prajapati, 2018). Almost every action one takes in a digital world leaves a set of detailed and predictive digital footprints. Obviously, digital identity may be classified as weak or strong. The weak digital identity is limited to virtual characters, avatars, or fakes, which play digital roles with no significant impact on the subjects' lives. The strong digital identity is constructed when subjects use digital technologies as a support to convey meanings that extend into the subjects' lives and reach beyond a virtual concept (Ferrer Maia and Valente, 2012).

In any case, there are digital footprints that can be used for digital surveillance. In fact, there are four main types of surveillance that occur using social media: interpersonal (the most extreme is stalking, however, Boyd /2011, in Kidd, 2017, 14/ suggests that many social media users sign up specifically so that they can be seen, ie to be surveilled, or for doing some surveillance themselves), institutional (the most common is to keep tabs on their employees), market (primarily involves keeping track of what customers buy or search for), and police (to detect criminal or otherwise targeted activity) (Trottier, 2012, in Kidd, 2017, 13).

This is what we tackle in this contribution, with reference to social platforms. Thus, we do not mean the European Union's electronic identification, authentication and trust services (eIDAS) regulation here.

The most known and most widely used programme based on digital identity is Chinese social credit system (In Mandarin Chinese, the term is more closely associated with a phrase like "public trust."). Chinese citizens are ranked on professional and personal interactions, online activity, and public appearances (Huang, 2015). The Chinese government and state media argue that the project is designed to boost public confidence and fight problems like corruption and business fraud. Critics often see social credit project instead as an intrusive surveillance apparatus for punishing dissidents and infringing on people's privacy. In fact, the system is more a patchwork of regional pilots and experimental projects, with few indications about what could be implemented at a national scale as planned for 2020 year (Matskakis, 2019).

Threats Posed

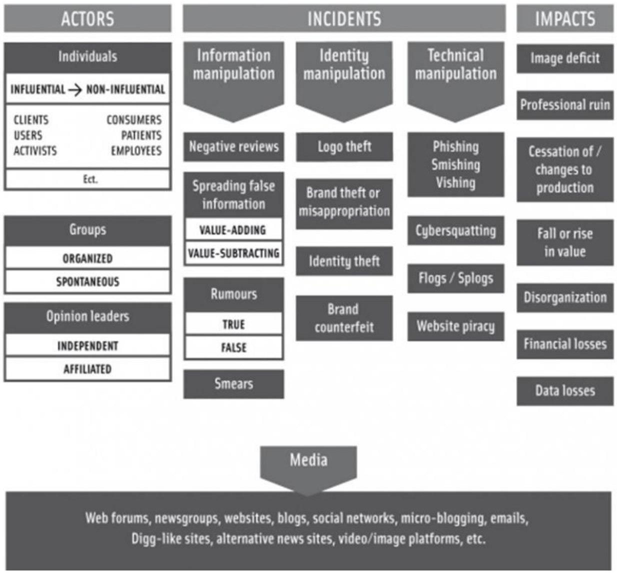
There are obviously first of all **privacy concerns**. However, as put by Ertzscheid (2016), the importance of the digital identity issue **varies from platform to platform**. The question of anonymity, for example, is absent on professional social networks such as LinkedIn, where users showcase their CVs. In general, Boyd (in Ertzscheid, 2016) defines social networks as "semi-public" spaces. She supports this argument with four features: there is persistence of our messages in time, there is searchability function, there is replicability of our messages and there are "invisible audiences".

Increasing use of virtual reality also raises concerns relating to **cyberbullying and cyber-stalking**. The age-group particularly vulnerable to these kinds of crimes include teenagers and adolescents and can have a remarkable impact on their social compass. Digital footprints left behind in VR/AR can be used by hackers to **extort money out of victims,** or worse, **forge duplicate identities with malafide intentions** (Prajapati, 2018).

Kelly (2019) predicts that digital identity theft will continue to grow rapidly in 2019. The lack of awareness of the real risks that can be associated with accepting people we do not know on social platforms, activating geolocation in applications and the "dictatorship" of "likes" as a means of acceptance and/or social recognition, are the main reasons that lead to **harassment of females** in digital environment (S2Grupo, 2018).

A graph below gives overview of perhaps all possible risks related to digital identity.

Figure 2: A typology of e-reputation risks



Source: Ertzscheid (2016), originally published in E-reputation, typologie des risques liés à la reputation, Christophe Asselin – Digimind.

Policy Solutions

WEF Report (2018) identified five equally important elements that a proper digital identity must satisfy. These elements are: Fit for purpose, inclusive, useful, offer choice and must be secure. Obviously, tensions exist between some of them.

The GDPR gives EU M.S. users the right to verify their data. Moreover, there is the right to be forgotten in addition to the right to erasure. In addition, Szymielewicz (2019) observes that people/users can take measures to control the first layer of their digital online profile (For example, users can choose not to post status updates or like pages). Prajapati (2018) also focuses at personal or the first layer of protection: Conducting background research before establishing connection with online identities of other individuals (for example - online dating), keeping digital identities private unless necessary to be shared with others and reporting fake/misleading identities as soon as possible. In effect, Ertzscheid (2016) suggests as a solution specialised training, acculturation and support that allows users to understand, analyse and circumscribe their digital identity. Such (**media literacy**) training and support should form part of most school and university curricula.

However, users can not influence much behavioural monitoring and microtargeting. The only way to regain full control over own profiles is **to change policies of platforms**. Theoretically, instead of hiding this data from users, they could become more transparent. Moreover, the platforms could ask questions and respect our answers. As mentioned, to certain degree this is covered/protected by GDPR. However, although virtually every platform or application asks for permission to use data, offered options are often too complex and simply not manageable by an average user.

Maybe as a response, some professionals believe that although there are real, life-threatening risks to sharing personal information, nevertheless, the real, tangible value we get from sharing data about ourselves usually outweighs the risks (e.g. Weigend, 2017). Weigend believes that power lies in choosing to use those data refineries which offer **tools that increase transparency and agency for users-** including tools that allow to evaluate how much benefit one can get in exchange for the data one shares. It is not quite clear what are these tools, and how feasible this option is. Kelly (2019) believes that **data security experts** should play a more important role in the discussion on regulating social media and privacy related to digital identity. Moreover, he suggests that **industry** should get more deeply involved. We have to choose between **decentralized identity system vs. centralized identity system.** If we choose the first concept (with the nick "little brother") that will protect our "self-sovereign" identity or we defeat the fragmentation of our identities and centralize them under one unique password.

The future is around the corner and they are still open question on a real interest on digital identity and its protection, and from the theory to concept to pilot and then to implementation of new regulations.

Compiled by SCM