Año 26 No. Especial 6
2021

RVG

Año 26 No. Especial 6
2021

25 ANIVERSARIO

Revista Venezolana de Gerencia

Revista Venezolana de Gerencia

UNIVERSIDAD DEL ZULIA (LUZ)
Facultad de Ciencias Económicas y Sociales
Centro de Estudios de la Empresa

ISSN 1315-9984

COMO CITAR: Tello de la Torre, C., Martí-Noguera, J. J., y Perez, V. (2021). Digital Human Assets and Psycho-digital Risks. Concept and recommendations. *Revista Venezolana de Gerencia*, *26*(Especial 6), 12-28. https://doi.org/10.52080/rvgluz.26.e6.2

Universidad del Zulia (LUZ)
Revista Venezolana de Gerencia (RVG)
Año 26 No. Especial 6 2021, 12-28
ISSN 1315-9984 / e-ISSN 2477-9423

Digital Human Assets and Psycho-digital Risks. Concept and recommendations

Tello de la Torre, Claudia*
Perez, Vanesa**
Martí-Noguera, Juan José***

Abstract

Nowadays, 60% of humanity is digitally connected, implying the generation of data and content. In this sense, the objective of this article is to discuss the relationship between the concepts of Human Digital Assets and Psycho-digital Risks. The former comprises digital information linked to a person, and the latter is conceived as the potential danger arising from the interaction of people and organizations due to interaction with networked technologies without sufficient knowledge. Through a qualitative methodological approach and a documental research design, both concepts are addressed, in order to provide their identification, evaluation, and integration in the management of human digitization processes. This paper does not intend to formulate a methodology for its quantification, but rather to motivate and raise awareness of the need to rethink digital literacy in various interest groups. The conclusions allow reflecting on considering the basic aspects of both concepts, their relationship, and recommendations to be incorporated in organizations in order to minimize the risks generated in the digital space that affect our physical life.

Key words: Human digital assets; risk; management; digital environment

Received: 17.08.21 **Accepted:** 18.10.21

* Doctora en Economía por la Universidad de Barcelona (UB), España. Maestra en Economía por la Universidad de Barcelona y Maestra en Gobierno y Asuntos Públicos por la Facultad Latinoamericana de Ciencias Sociales (FLACSO-México). Investigadora Cátedra-CONACYT Centro de Investigación en Ciencias de Información Geoespacial, CentroGeo. Cdmx, Mex. Email: ctello@centrogeo.edu.mx ORCID: https://orcid.org/0000-0002-0664-6713

** Profesora adjunta Universidad Internacional de Valencia. Candidata a doctora y Máster Universitario en Neurociencias Básicas y Aplicadas por la Universidad de Valencia. ORCID: https://orcid.org/0000-0003-0284-7304

*** Doctor por la Universidad de Valencia, España. Socio fundador de Cibersalud y Bienestar Digital. Docente Universidad Internacional de Valencia. Email: juanjomn@protonmail.ch ORCID: https://orcid.org/0000-0002-4449-8563

Activos Digitales Humanos y Riesgos psicodigitales. Conceptos y recomendaciones

Resumen

Hoy en día, el 60% de la humanidad está conectada digitalmente, lo que implica la generación de datos y contenidos. En este sentido, el objetivo de este artículo es discutir la relación entre los conceptos de Activos Digitales Humanos y Riesgos Psicodigitales. El primero comprende la información digital vinculada a una persona, y el segundo se concibe como el peligro potencial derivado de la interacción de personas y organizaciones que no tienen el conocimiento suficiente para interactuar con las tecnologías conectadas a la red. A través de un enfoque metodológico cualitativo y un diseño de investigación documental, se abordan ambos conceptos, con el fin de proporcionar su identificación, evaluación e integración en la gestión de los procesos de digitalización humana. Este trabajo no pretende formular una metodología para su cuantificación, sino motivar y sensibilizar sobre la necesidad de repensar la alfabetización digital en diversos grupos de interés. Las conclusiones permiten reflexionar sobre la consideración de los aspectos básicos de ambos conceptos, su relación, y las recomendaciones a incorporar en las organizaciones para minimizar los riesgos generados en el espacio digital que afectan a nuestra vida física.

Palabras clave: Activos digitales humanos; riesgo; gestión; entorno digital.

1. Introduction

In 2021, 60% of the world's population has access to the internet and 55% of the population is connected through social networks (Kemp, 2021). There is an accelerated growth since the confinements caused by COVID-19. As digital connectivity advances, the access gap decreases and there is an international process of obligation in the use of technologies in all areas: commercial, labor, educational, administrative, banking, leisure, among others. Mostly from the use of smartphones as an inseparable complement used by people to access the wide range of services and digital resources (Jeffrey, 2021; Harkin & Kuss, 2021).

However, there is a lack about training society for the implications of being digital, although there is an incipient concern for digital ethics and responsibility (Elliot et al, 2021; Lobschat et al, 2021). Governments and companies have focused on teaching how to use technologies, but to a lesser extent on defining and addressing the risks of digital citizenship (Buchholz et al, 2020; Pritika et al, 2020). In this sense, this article presents two concepts: Digital Human Assets, and that of psycho-digital risks derived from the conditions of a digitally interconnected social model. Methodologically, it is based on a review

of research, reports and policies (Hsieh & Shannon, 2005).

In the so-called IV Industrial Revolution, by Schwab (2016), the relationship with technologies is not only characterized by the interaction people make to communicate with each other, it also implies an evolution and integration of programs and interconnected technologies called Artificial Intelligence, or the "internet of things". In addition to the creation of programs that can handle large volumes of information, which is impossible to manage by a person, designed to learn, predict and execute actions. Interactive synergies are established between people to communicate with other people, relationships of people with programs to execute actions, novelties, interactions of programs with other programs and devices connected to the Internet.

In 2020, half of the internet traffic was given by programs that analyze and manage the information we shared, without our participation. Countless profiles, behavior patterns and even consumer preferences are created with our data (Suchacka & Iwański, 2020). It does not depend on a person to turn off the system to which your information is connected; since it is in the cloud, distributed in servers, it is outside the relative control of the person (Junjiang, et al, 2021; Tao, 2008).

Here are two examples of incorporating programs impact with artificial intelligence in our lives. The system of a smartphones can learn from our routines, process information, make predictions and decisions. If your smartphone detects that you are systematically late for daily meetings, it can decide to advance the time of our alarm clock, if it is connected to internet in the same network. It could be considered a positive factor.

On the contrary, there is the case of the use of programs for personnel selection in companies that systematically exclude them by gender, ethnic or sexual orientation, when they should focus on identifying the required competencies for a job. Systems that operate with Artificial Intelligence are not neutral in their data analysis. There is an ethical debate about its effect due to the biases of those who program them in their interpretation of reality, affecting the learning and decision-making models for which they have been designed (Ntoutsi et al, 2020; Paliwal et al, 2020; Srinivasan & Chander, 2021).

Society advances towards a coexistence in the physical and digital plane, in a hybrid and interactive way, what happens in one space can be translated into effects in the other. Digital life and its effects on a person daily life force us to think about new concepts, management, learning and evaluation methodologies in the view of integrating the digital space and artificial intelligence in the personal, social, and work sphere

Consecutively, the definition of digital identity is addressed to the context of information that we generate through our digital interaction. We define Digital Human Assets, followed by the concept of digital risks that emerge from this digital condition, and discusses some proposals for its management in organizations.

2. Identity and Human Digital Assets

Identity must be understood as an identifier of each person in a territory (Allende, 2020). An attempt has been made to define the digital territory as the information infrastructure under the

control of a state (Capurro et al, 2013; Mukerji, 2010). Regulatory frameworks on nation and citizenship, space and property in digital environments; the limits between material and moral dimension in which objects and data flow, are put into play, leading to insufficient privacy and security controls, consequently, a digital territoriality without borders (Möllers, 2021).

The digital society presents tensions in the understanding of what citizenship is. In the states, citizenships are granted to people who inhabit a territory, regulated by a legal framework. In the digital territory, there are situations of illegality because they are not contemplated in the current legislations. In this territory, relationships can happen between people and artificial intelligence systems without sharing the same country, lacking borders within the same legal framework.

The recognition of who we are when interacting digitally, in a globalized world, needs to have a digital identity that authenticates (identity) each individual in his or her relationship with cyberspace. It should be noted that the beginnings of the digital society have occurred through the convenient creation of user profiles in virtual accounts without the necessary correspondence, with physical identity. To give an example, the European Union is working to shape a certificate or digital document that unifies documents such as passport, driver's license, medical and banking data, to name a few (Berbecaru, 2019).

However, the requirement is that all online access is usually linked to an e-mail account and, increasingly, to a phone number associated with a smartphone. At this moment, e-mail or smartphone number are means that allow us to access the digital space to interact and access services; they do not depend, usually, on national governments but on international companies.

The e-mail, unlike our name or identification number, is an identity created at the user's choice. It depends on the company that validates said identity, allows access to it and stores information among other functions, as well as the company that provides the internet connection service. E-mail accounts are mostly free services, which are economically nourished by the volume of data we exchange. In this sense, there is a problem of defenselessness on the part of the population, when States require communication by digital means, without providing an e-mail that guarantees our rights and knowledge about the implications of its use. Any alteration that involves changing e-mail or telephone number, losing password, as we emphasize, linked to our gateway to the digital space; obliges us to review what services we have linked to and modify them so that they can locate us and maintain access.

To give an example, if a government forces to receive digital notifications, and the organization or person loses access to e-mail, it could be penalized for not responding to requirements to which it is obliged to, without the state being the guarantor that it will have an e-mail account and internet access to be able to respond to the requirement. Nowadays, to have and maintain a digital identity acquire a special relevance, as it is necessary to service access and not to be excluded. So how do we define and manage our digital identity?

2.1 Digital Identity

In the digital context, identity is not regulated by a country, for now. It consists of freely assigning yourself

(depending on your availability) a username for an e-mail account, social networks or registration on web pages or apps. This should not always be associated with our physical identity that gives us the registration of a state. Our digital identity, also known as digital self (Feher, 2021), has no physical border limitations because we can navigate, access, and consume content from different countries.

To own a digital identity gives us privileges access to services. The dynamics and digital relationships generate a new sociocultural typology, with effects on our behavior due to the consideration of anonymity by not making our registered physical identity explicit. It allows a different level of interaction than in person, because by avoiding physical exposure, no risk is perceived, with the consequent danger that exposure may entail (Aboujaoude, 2011; Suler, 2016).

For example, choosing a digital user like greenhorse@ / imnotdavid @ ... is not my name and surname in my identity document, I do not have the obligation to link my official ID to my e-mail account. It is my digital identity, and it serves me as my email account, social networks, user on web pages, etc.., allows me to access and interact online. In this sense, digital identity beyond a name and identity number can be defined as the set of all the information available digitally regarding an individual, regardless of its degree of validity, its form, or its accessibility, which includes direct and inferred data, or indirect (Allende, 2020). Digitization cannot be considered a parallel life, but rather our development in which we establish interconnection not only with people, but also with bots and programs with which we interact and learn from our behavior. These range from the voice assistant that waits for orders or gives us suggestions, to the system that organizes the agenda. Different studies allude to the confusion between personal / professional digital identity, and the risks posed by the lack of training, as well as the lack of research (Guraya, Guraya & Yusoff, 2021)

Digital identity is an evolving construct. It includes, the digital certificate issued by governments, our e-mail accounts, social networks, apps or web pages in which, in addition to the data we provide when creating them, our behaviors when using them in the digital space because they are recorded. Not only do people create their e-mail accounts, but also companies can create them to give us access to corporate e-mail or certain services. Unlike physical identity, digital identity is currently characterized by discretionary use and less temporality than physical identity. We can make use of a digital identity for a time (an e-mail, a profile in networks) and discard it.

However, the information we generate, associated with our digital identity (way of being, tastes, habits and records), can be stored on digital devices, published (post, tweets) or tagged (another person quotes our user). This information can be used so that other people and computer programs can identify us and attribute some traits or characteristics to us without our direct action, and this information conditions our life. We then analyze your relationship with digital assets.

2.2 The era of Digital Assets

Digital identity allows us to have digital assets, resources that exist in a digital format, and comes with the right

to use (Inozemtsev, 2021). Under this concept, a wide range of resources is considered that include elements stored on devices, USB or online files, photographs, word / excel documents, ppt, videos, cryptocurrencies, emails, instant messages, software, any email account, (the chosen username), social networks, photo sharing files, websites and domain names (Kud, 2019; Toygar et al, 2013).

Digital assets are only accessible with a suitable program and can be stored on a physical device enabled to be container (USB or memory systems), as well as in the cloud. In this case, it is required to have access to the internet, and a digital user profile, linked either to an e-mail account, or to a code to verify ownership. While digital assets are products, our digital access has a subsidiary implication. Every time, we access the digital space, either directly or indirectly, they quote us in a post, share a photo in which we appear, and a digital asset related to our digital identity is generated.

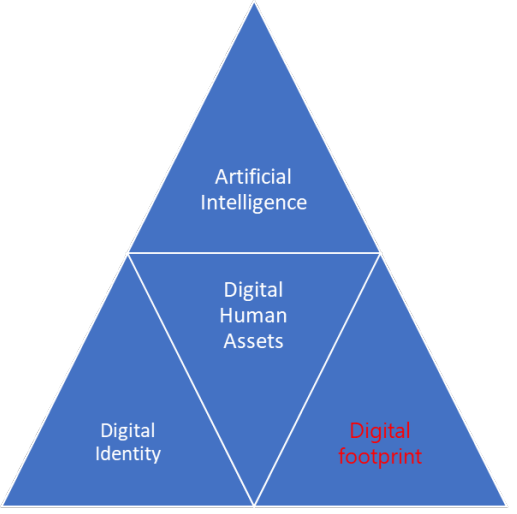
2.3. From Digital Assets to Human Digital Assets

The digitization of human activity due to the integration of connected technologies generates a new framework and concepts such as Digital Human Assets (DHA). It includes the consequence of any action, carried out directly by the person, or indirectly by another person -the tag in a publication on social networks- or system -Google organizing information about our profile- that generates structured digital data of our profile. It becomes a product, which in turn can be marketed, processed to obtain or generate information, and it acquires value. The most common example, companies that buy profile data to make certain types of ads visible to us that match the data collected from our DHAs.

Among other data, DHA can be considered: the physical place from where we connect (our travel routes when recorded using devices with *GPS* enabled), the website we visit (the time, and the content we interact more, less, or nothing), the publication of a post or product, share and rate, or comment on content. Generate an action that includes accepting the privacy and cookies policy or rejecting it. Every action, linked to a digital identity, generates a profile of our behavior, emotions, and thoughts. Those who, for different reasons, do not have a constant Internet connection, or refuse to be connected (mail, social networks, etc.), due to the fact of living in digital societies, can be filmed or photographed in public spaces by surveillance systems, or deprived by close people who have a greater digital life.

In this article, we define Human Digital Assets as digital records of a person associated with their physical, psychological or behaviors stored on the network. It has a value as they can be accessed and manipulated by the person, other people or programs. Figure 1 shows how DHAs are supported by our digital identity, it is built based on interactions on the internet (e-mail, social networks); and our fingerprint and generated by information provided by us or third parties via the web, smartphone, or wearables (behavior, thought, image, audio ...). On the top, Artificial intelligence operates on this pillar, structuring data that classify us to predict our behavior.

Figure 1
Basis of Human Digital Assets



Some features to keep in mind:

- DHAs are associated with our digital identity and belong to us insofar as the concept of digital property can be interpreted. All the information that we generate (e-mail, social networks, etc.) is our property to the extent that we know and exercise our rights as individuals. Depending on the country of nationality, pressure can be exerted in international courts to demand control measures. That is the example of the European case for the forgotten right demanded to Google (Larsen, 2020), and they remain after our physical death, generating issues associated with their property (Conway & Grattan, 2017).
- Our access to ownership of such DHAs is limited. Being stored on servers in the so-called cloud, as individuals, we do not have a *de facto* control as it is not material and can be hosted in different countries.
- They can be accessed by other people (for example, posts, that are commented on when we are not paying attention and can generate dialogues far from our control), or by artificial intelligence systems.

Examples can be posting or publishing a photo. Being our property in the digital sphere can produce reactions, comments, be copied, downloaded, edited, screenshot, etc., generating a projection of our digital identity, different from the face to face on which we have more control. Unlike the physical territory, the limits in which information is accessible in time or space, in the digital world they are diluted, which generates processes of abuse or violation that cannot be notified (Beslay and Hakala, 2007).

DHAs intervene in the construction

of identity, which we call hybrid because it occurs in the physical and digital planes. We propose its development in two dichotomous dimensions: conscious / unconscious and proactive / passive. Both factors have in common the absence of digital literacy that mostly affects unconscious use of tools, applications, and their consequences. In order to illustrate the implications, a series of examples are presented below.

1. Unconscious / passive digital identity. It is the information that can characterize a person, and it is configured by being the object of photographs, publications on social networks, e-mail content, sending of audios in messaging systems, by other people without their participation. For example, the case of photos and conversations on Instagram of a pregnancy have been normalized. An unborn person can already have data associated with their identity, even an account created in their name with comments, positive or negative. It is passive on the part of the person, for obvious reasons given that it does not intervene, and unconscious to the extent that those who post comments do not consider the consequences that may arise.

Another example, when a person referenced years later see in networks that it was a trending topic for a photo, number of “likes” and comments, positive or negative, by someone who did not know him. This situation applies to any person, who even if they do not participate digitally, can be photographed / filmed and an online discussion could be started about them.

2. Proactive / unconscious digital identity. The information we share with other people becomes proactive but unconscious. It happens when an underage person begins to share information by enabling an e-mail account, or the use of a connected device. She/He does not have enough knowledge to know the effects that the shared information may have without the supervision of an adult. Although the most frequent is that the web programs themselves detect age and impose restrictions (for example, YouTube channel, if it identifies minors, it limits access to comments and other functionalities).

An example of the construction of a proactive - unconscious digital is when without understanding the consequences, the digital profiles that we create such as user accounts to visit morally ill-considered pages. Or, for example, to make comments under another identity, without considering the consequences they may cause in the absence of a moral filter that gives the feeling of anonymity. By generating digital identities with names, other than physical identity, responsibility for actions is dissociated but, if they are carried out with the account registered on a device or smartphone, they are geolocated, they can be associated by facial and relationship recognition that the person maintains, facilitating their identification. The fallacy of feeling that I am not the one who says my physical identity, recognized by a state, by using a different name or nickname, increasingly lacks foundation and legal implications.

3. The passive and conscious digital identity. It happens when we integrate connected devices into our routine, such as a smartphone or smartwatch. Without an intention to record or communicate our behavior, it maps the path of each person and generates information on how

much we have walked, where we have been, where we have eaten, interacted (going to the movies, trips, etc.). We generate information just by carrying a device, even if we do not interact with it. We are aware, or we can be, to the extent that a large part of the apps provides the information they collect from our behavior and we have the option to disable certain records.

4. Active and consciuous digital identity is any activity we establish with the purpose of communicating with people or web systems (for example, completing forms in exchange for access to information). All information that we do not delete (post, cookies, photo, account, etc.). While it would not be feasible to claim that we have full control of the information we share, it may refer to a higher level of awareness about what we share.

On the physical plane, our own identity and the social construct that defines us were limited to the interpretation and memory that people had of the interactions that we carried out in a given space. In the digital society, without space-time borders, information can be public and largely accessible by different people and artificial intelligence systems. On the digital level, the interactions we make, those that other people comment, those that collect pages we visit and those that we do not visit are recorded. This information of ours can be interacted with by people, without the participation of the protagonist. It also generates a series of data that is stored on different devices, user accounts and cloud platforms.

As indicated above, programs based on Artificial Intelligence integrate available information from data, can develop individual profiles on their characteristics, predict and influence behaviors and attitudes. Recognizing the DHA as the information generated in our interaction within the digital society, it becomes essential at a time when organizations run a large part of their processes using artificial intelligence.

The analysis of information that is carried out on the internet about our fingerprint, if not controlled, can affect our life. Issues as decisive as the analysis of our profile in job selection processes, previously commented, or the decision to grant us health insurance, depending on the analyses carried out by programs with our DHAs, could be affected by the information shared. Some examples of information present in the digital plane that affect our physical life:

1. Could a health insurer refuse to assist us if our devices show that we do very little physical exercise, we order high-fat food through apps and we have shared in a profile that we have family members with health problems?
2. In the selection of personnel, reviewing the information accessible in networks of people who choose a job or new position provides more information than a curriculum that we prepare. All our information, the DHAs available on the network, define and allow us to predict our behavior in the future, and is of interest to organizations. A company, instead of evaluating our profile by a summary that we present to it of our experience, may prefer to access our digital information and establish a prediction about what we would contribute to decide to hire us.

Faced with this situation, the question should be asked about the impacts derived from the lack of

control and knowledge over our digital information. We then deal with Psycho-Digital Risks and their management.

3. From risks due to digital stress to Psycho-Digital Risks

One of the main changes, experienced between the 20th century and this century, in the man-technology relationship is that the first digital technologies ended their influence in our lives by turning off the button. Much of the information was printed and had no major impact on a day to day. Even so, the integration of technologies in human activity requires a learning period. In the 1980s, technostress was defined as "an adaptive disease caused by the lack of ability to deal with new computer technologies in a healthy way" (Brod, 1984). The conceptualization of the discomfort arising from the integration of technologies in our lives has received great interest since then, although with more theoretical than applied studies (Cuervo et al, 2018).

At present, we not only refer to technostress from using computers, smartphones and programs as tools or means for a work purpose; digitization makes us receive information from people by mail, instant messaging and different social networks (Facebook, Instagram, twitter, among others). In addition, as has been presented, programs interact with people and demand attention. On the smartphone, with assistants such as Alexa, Siri, wearables, google home ... they monitor our activities, and run programs to ask us for information, or make proposals. This situation surpasses any other past technology with which a relationship has been previously maintained, generating new risks to our health and well-being.

3.1 The integration of technology in the absence of training.

The COVID-19 pandemic, for all intents and purposes, has been a point of disruption in the digitization of society, increasing its sphere of use. Weaknesses have been demonstrated in the adoption of technologies and the transfer of analogue to digital processes with risks that affect privacy and an increase in digital insecurity (Faraj et al, 2021). As mentioned above, the main reason is the absence of a regulatory framework and training in digital skills both in professional and personal aspects (Milenkova & Lendzhova, 2021).

The key point is who is responsible for training in the use of digital technologies. The private sector provides connectivity and the development of devices, as well as programs, but does not regulate their use. A function that would correspond to government institutions. Faced with this lack of assumption of responsibility, those who are teachers at different levels of education, from basic to university, have limited knowledge about the implications of incorporating connected technologies in the classroom. Technology has been integrated, without designing the mechanism to train teachers and prevent derived risks.

In the family sphere, with digital skilled parents / adults, connected devices (smartphones, tablets, computers, etc.) are given to minors as tools of entertainment, repeatedly infringing access to content up to a certain age. From access to unsuitable content to contacts with people or programs

(it is not known, they are only digital identities), which among other problems allows a digital profile of minors to be built without explicit knowledge. Several studies point to an increase in internet addiction. A problem on the rise and difficult to avoid although many apps report the time we dedicate to its use (Cash et al, 2012; Zimmermann, 2021).

In short, being digital is a condition for an increasing population, and given the lack of training it requires a risk analysis.

3.2 Psycho-digital risks

Starting from the DHA, do you imagine that a person has access to all the information generated since having an e-mail, social networks, or messaging systems? It would be difficult to store all that information even when much of it has been deleted or remains on devices that are no longer in use.

Do you know how many times you have been tagged, mentioned in a post, or featured in a photo taken by other people? Once we publish a photo, or a post, there may be people talking about that digital asset, without already having a direct link. Without having intervened or carried out any other activity that could have given rise to register comments.

In this way, we define psycho-digital risks as the real or potential damages that the management of their DHA can cause to a person. Following the hybrid identity scheme according to DHA, psycho-digital risks occur in the continuum of proactive dimensions - passive, conscious and unconscious.

- Conscious - unconscious. They are given in a conscious way, to the extent that there is knowledge of the impact of each action we carry out in a digital context. We can consciously publish a post, send audios whose information outside the original sender - receiver channel can be reinterpreted, biased, and used to give a negative image of us. Unconscious refers to the consideration of keeping anonymity in networks by not making use of our physical identity data. Visiting web pages for searching information generates a pattern of behavior, which due to ignorance may be assumed that other people will not have access to it.
- Proactive - Passive Mode. They are carried out by the same individuals through actions with digital tools, or originated through data manipulation by other individuals or by artificial intelligence systems. In a pro-active way, we broadcast information in each virtual interaction. In the same way that passively happens when carrying a smartphone, geolocated information of the places through which our moves are recorded.

The intersection of both dimensions facilitates four measurement scenarios, which, when properly structured, allow the elaboration of a risk map and the taking of measures that, based on digital literacy, mitigate their impacts.

The recognition of areas in which psycho-digital risks may occur is key to avoiding problems with a negative effect. Identifying the spaces for digital interaction is a necessary first step to have information on possible risks and measures to be taken. We put two examples, to facilitate understanding.

Media such as YouTube have developed platforms for sharing videos at convenience subtitled, with the purpose to become viral. Not necessarily being negative, the fact that millions of views are produced may cause the content

to be commented on, or modified in its sense, without the author and original messages having any relation to what happens later. This is the case of a young man who in 2008 was interviewed by a journalist. In the year 2021, the interview with him is subtitled with references to any other topic under the generic name of "Dimitri realizes ...". The protagonist was not named Dimitri, and what is known is that due to the pressure caused by the use of his image, he abandoned all social networks (Russian News Clip, 2008 Dimitri Finds Out | Know Your Meme). In this case, both the interviewer and the interviewee were not aware of what could be derived from this fact.

Another recent case is that of a lawyer from a county in Texas, USA, during an online connection to hold a trial. The computer was previously used by another person, and in its interaction for connecting to the trial via zoom, it appears with a filter that superimposes a cat on its image. Before the audience, what appears is a cat speaking, and after expressing his ignorance of how to remove the filter, he manages to express "I'm not a cat". Judge Roy Ferguson (February 9, 2021), awares of the impact it would have on him, shares the recording on social networks. Within a few hours, the lawyer receives hundreds of calls, his image is used to make thousands of memes, t-shirts and have an ephemeral international digital life.

The videos become DHA, a digital part of their lives, decontextualized and out of control of their actors. You can cause personal harm in the digital plane by overexposing your image, comments and mockery; also in the physical world in their personal and professional environment to be recognized and questioned as the involuntary author of a fact considered comic. Both videos continue to generate views, comments and reinterpretations.

3.3. Psycho-digital risks in organizations.

This last point refers to a particular area. Organizations, public and private, that, for the most part, have interpreted digital transformation as the acquisition of technology and programs to be competitive, more efficient, reduce costs or respond to market demands (Kamaljeet, 2021). However, there are still few studies on psychosocial risks in digitization (Williams, 2020).

Various investigations address digital fatigue, or burnout, produced by person - device or program interaction, and the consequent anxiety, frustration or exhaustion in learning how to use it. In addition to the time of using computer screens or smartphones (Leonardi, 2020). Although the devices themselves integrate more and more applications that allow us to know the time, we dedicate our attention to interacting (Zimmermann, 2021). Without an adequate evaluation of the human factor, a series of primary risks such as technostress have been assumed, facilitating errors that affect cybersecurity, or cyber scams, whose consequences translate into negative effects and high costs for organizations. The high incidence of human error cannot hold people exclusively responsible, given that they have not been adequately prepared (Agazzi, 2020; Cains et al, 2021; Hijji & Alam, 2021; Neigel et al, 2020; Sánchez-Teruel, 2016).

In this regard and referring to psycho-digital risks, this article goes beyond the so-called psychosocial risks. It focuses on the digital identity and DHA of each person who is part of

an organization. When hiring a person or incorporating digital technology, all the available information of each person, accessible or stored on the network, presents an organizational risk by interconnecting with the personal baggage of each member of the organization. From social and personal networks such as Facebook or Twitter, professionals such as LinkedIn, and in the use of corporate e-mail for professional or personal purposes, etc. Delimiting personal / professional aspects in the digital space does not currently have a model. It usually tries to save itself by including notes such as "the opinions expressed in this account are personal."

The problem is that the information, generated by the person as DHAs are also associated with the organization, and vice versa. An organization can be criticized for the digital behavior of a member, such as a person cataloged for working in a certain company. Risks increase in intangible aspects (reputational risk), as well as tangible ones (cybersecurity risks and the reaction of interest groups).

Analyzing the DHA of each member and evaluating their psycho-digital risks allow organizationally to identify, evaluate, and integrate them into the management strategy through concrete and measurable actions. The definition of an organization's digital strategy cannot be limited to integrating technology and training in its use, but also to identifying its individual consequences and collateral effects.

4. Conclusions

According to what has been developed in this article, the impacts derived from the digital condition generated by the DHAs, exceed the individual capacity to manage them, and implicitly carries on psycho-digital risks. Due to the complexity they present, we point out the urgency of defining a governance model, with an emphasis on analyzing DHA, describing and evaluating risks, as well as designing the means for managing the digital condition.

Regarding the objective of this paper, it can be clarified that it is not intended to be exhaustive on the subject, but to contribute both to the discussion of the causes and effects, as well as to the assessment of the risks of the different digital environments. In this sense, promoting the understanding and study of DHA and its relationship with pre-existing vulnerabilities put at the center the analysis of new processes of interaction and interrelation of individuals with digital technology and their identity beyond legal, historical and philosophical structures.

To finalize this first conceptual approach, we formulate a question: What are your DHAs and what risks do they present? And we recommend considering three aspects for your individual or organizational implementation:

1. Identify DHAs related to you. If it is a company, with each person related to the organization. Structure the information in a matrix.
2. Establish indicators for monitoring and control DHAs in relation to the risks they can cause in order to be identified.
3. Include a digital scoreboard that makes it easier for the person to monitor the evolution of their DHA, facilitating the organizations with whom the associated risk management is linked.

It is necessary to design training, according to the implications of digitizing ourselves, as human society and organizations, defining those responsible

for digital transformation, aimed at the people who are part of the organization, as well as its stakeholders.

The new etiquette that defines us is not how we dress, or what neighborhood we live in. It is how we build and manage our DHAs.

References

Aboujaoude, E. (2011). *Virtually you: The dangerous powers of the e-personality*. W.W. Norton.

Agazzi, A. E. (2020). *Business email compromise (bec) and cyberpsychology. Department of Computing and Informatics*. https://arxiv.org/abs/2007.02415

Allende López, M. (2020). Self-Sovereign Identity: The Future Identity: Self-Sovereignity, Digtal Wallets, and Blockchain (en inglés). https://doi.org/10.18235/0002635

Berbecaru, D., Lioy, A., & Cameroni, C. (2019). Providing digital identity and academic attributes through European eID infrastructures: Results achieved, limitations, and future steps. *Software: Pract. Exper.*, *49*(11), 1643–1662. https://doi.org/10.1002/spe.2738

Beslay, L., & Hakala, H. (2007). Digital territory: Bubbles. In P. Kid (ed.). *European visions for the knowledge age: A quest for new horizons in the information society*. UK: Cheshire Henbury

Brod, C. (1984). *Technostress : the human cost of the computer revolution*. Addison-Wesley.

Buchholz, B.A., DeHart, J., and Moorman, G. (2020). Digital citizenship during a global pandemic: moving beyond digital literacy. *Journal of adolescent & adult literacy: a journal from the international reading association*, *64*(1), 11–17.

Cains, M.G.; Flora L., Taber D., King, Z., Henshel, D.S. (2021). Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation. Risk Analysis: an Official Publication of the Society for Risk Analysis. https://doi.org/10.1111/risa.13687

Capurro, R., Eldred, M., y Nagel, D. (2013). *Digital whoness: identity, privacy and freedom in the cyberworld*. Walter de Gruyter.

Cash, H., Rae, C. D., Steel, A. H., & Winkler, A. (2012). Internet Addiction: A Brief Summary of Research and Practice. *Current Psychiatry Reviews*, 8, 292-298. https://doi.org/10.2174/157340012803520513

Conway, H. & Grattan, S. (2017) The 'New' New Property: Dealing with Digital Assets on Death, en Conway and Hickey (eds), Modern Studies in Property Law, 9, Hart Publishing, pp 99-115. SSRN: https://ssrn.com/abstract=3289171

Cuervo Carabel, T., Orviz Martínez, N., Arce García, S., & Fernández Suárez, I. (2018). Tecnoestrés en la Sociedad de la Tecnología y la Comunicación: revisión bibliográfica a partir de la Web of Science. *Archivos de Prevención de Riesgos Laborales*, *21*(1), 18-25. https://dx.doi.org/10.12961/aprl.2018.21.01.4

Elliott, K., Price, R., Shaw, P. et al. Towards an Equitable Digital Society: Artificial Intelligence (AI) and Corporate Digital Responsibility (CDR). *Society*, *58*, 179–188. https://doi.org/10.1007/s12115-021-00594-8

Faraj, S., Renno, W. & Bhardwaj, A. (2021) Unto the breach: what the COVID-19 pandemic exposes about digitalization.

Information and Organization, *31*(1). https://doi.org/10.1016/j.infoandorg.2021.100337

Feher, K. (2021). Digital identity and the online self: Footprint strategies – An exploratory and comparative research study. *Journal of Information Science*, *47*(2), 192–205. https://doi.org/10.1177/0165551519879702

Ferguson, R. [@judgefergusontx] (9 de febrero, 2021) Judge Roy Ferguson on Twitter: "IMPORTANT ZOOM TIP: If a child used your computer, before you join a virtual hearing check the Zoom Video Options to be sure filters are off. This kitten just made a formal announcement on a case in the 394th (sound on). [Tweet]. Twitter. https://bit.ly/2ZkYhh5

Fernández-Prados JS, Lozano-Díaz A, Ainz-Galende A. (2021). Measuring Digital Citizenship: A Comparative Analysis. *Informatics, 8*(1), 18. https://doi.org/10.3390/informatics8010018

Guraya, S.S., Guraya, S. & Yusoff, M.S.B. (2021). Preserving professional identities, behaviors, and values in digital professionalism using social networking sites; a systematic review. *BMC Medical Education*, *21*, 381 https://doi.org/10.1186/s12909-021-02802-9

Guraya, S.S., Guraya, S., & Yusoff, M.S.B. (2021). Preserving professional identities, behaviors, and values in digital professionalism using social networking sites; a systematic review. *BMC Medical Education*, *21*, 381 https://doi.org/10.1186/s12909-021-02802-9

Harkin, L. J., & Kuss, D. (2021). "My smartphone is an extension of myself": A holistic qualitative exploration of the impact of using a smartphone. *Psychology of Popular Media*, *10*(1), 28–38. https://doi.org/10.1037/ppm0000278

Hijji, M. & Alam, G. (2021). A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats During the COVID-19 Pandemic: Challenges and Prospective Solutions. *IEEE Access*, *9*, 7152-7169. https://doi.org/10.1109/ACCESS.2020.3048839

Hsieh, H.-F., & Shannon, S.E. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research*, *15*(9), 1277-1288

Inozemtsev M.I. (2021) Digital Assets in the United States: Legal Aspects. In: Ashmarina S., Mantulenko V., Vochozka M. (eds) Engineering Economics: Decisions and Solutions from Eurasian Perspective. Engineering economics week 2020. Lecture Notes in Networks and Systems, vol 139. Springer, Cham. https://doi.org/10.1007/978-3-030-53277-2_61

Jeffrey, J. (2021). Confronting the scarcity of digital skills among the poor in developing countries. *Development Policy Review*, *39*(2), 324-339. https://doi.org/10.1111/dpr.12479

Junjiang, H., Tao L., Beibei L., Xiaolong L., Zhiyong L., & Yunpeng W. (2021). An immune-based risk assessment method for digital virtual assets. *Computers & Security*, *102*, 102134.

Kamaljeet, S. (2021). *Emerging Challenges, Solutions, and Best Practices for Digital Enterprise Transformation*. Advances in Business Strategy and Competitive Advantage. IGI Global. https://doi.org/10.4018/978-1-7998-8587-0.ch004

Kemp, S. (2021) Digital 2021: The latest insights into the "state of digital". https://datareportal.com/reports/digital-2021-global-overview-report

Kud, A. A. (2019). Substantiation of the Term "Digital Asset": Economic and Legal Aspects. *International Journal of Education and Science*, *2*(1), 41–52. https://doi.org/10.26697/ijes.2019.1.06

Larsen, R. (2020). Mapping Right to be Forgotten frames: Reflexivity and empirical payoffs at the intersection of network discourse and mixed network methods. *New Media & Society*, *22*(7), 1245–1265. https://doi.org/10.1177/1461444820912534

Leonardi, P. M. (2020). COVID-19 and the New Technologies of Organizing: Digital Exhaust, Digital Footprints, and Artificial Intelligence in the Wake of Remote Work. *Journal of Management Studies*, *10*. https://doi.org/10.1111/joms.12648

Lobschat, L., Mueller, B., Eggers, F., Brandimarte, L., Diefenbach, S., Kroschke, M., y Wirtz, J. (2021) Corporate digital responsibility, *Journal of Business Research, 122*, 875-888, https://doi.org/10.1016/j.jbusres.2019.10.006

Milenkova, V., & Lendzhova, V. (2021). Digital Citizenship and Digital Literacy in the Conditions of Social Crisis. *Computers, 10*(4), http://dx.doi.org/10.3390/computers10040040

Möllers, N. (2021). Making Digital Territory: Cybersecurity, Techno-nationalism, and the Moral Boundaries of the State. *Science, Technology, & Human Values*, *46*(1), 112-138. https://doi.org/10.1177/0162243920904436

Mukerji, C. (2010) The Territorial State as a Figured World of Power: Strategics, Logistics, and Impersonal Rule. *Sociological Theory*, *28*(4), 402-24.

Neigel, A.R., Claypoole, V.L., Waldfogle, G.E., Acharya, S., Hancock, G.M. (2020) Holistic cyber hygiene education: accounting for the human factors. *Computers & Security*, *92*, https://doi.org/10.1016/j.cose.2020.101731

Ntoutsi, E., et al. (2020). Bias in data-driven artificial intelligence systems—An introductory survey. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, *10*(6). https://doi.org/10.1002/widm.1356

Paliwal S., Bharti V., Mishra A.K. (2020) Ai Chatbots: Transforming the Digital World. In: Balas V., Kumar R., Srivastava R. (eds) *Recent Trends and Advances in Artificial Intelligence and Internet of Things. Intelligent Systems Reference Library*, vol 172. Springer, Cham. https://doi.org/10.1007/978-3-030-32644-9_34

Pritika, R., Bibhya S. N. & Kaylash C. (2020). Digital Literacy: a review of literature. *International Journal of Technoethics*, *11*(2). 65-94. https://doi.org/10.4018/IJT.20200701.oa1

Ruan, B., Yilmaz, Y., Lu, D., Lee, M., y Chan, T. M. (2020). Defining the Digital Self: A Qualitative Study to Explore the Digital Component of Professional Identity in the Health Professions. *J Med Internet Res*. *22*(9), e21416.

Russian News Clip (2008, 11 de octubre). *Dimitri Finds Out* https://knowyourmeme.com/memes/dimitri-finds-out

Sánchez-Teruel, D., & Robles-Bello, M. A. (2016). Riesgos y potencialidades de la era digital para la infancia y la adolescencia. *Educación y Humanismo*, *18*(31), 186-204.

Schwab, K. (2016). *La Cuarta revolución industrial*. Debate.

Srinivasan R. & Chander, A. (2021). Biases in AI systems. Commun.

ACM, *64*(8),44–49. https://doi.org/10.1145/3464903

Suchacka G., Iwański J. (2020) Identifying legitimate Web users and bots with different traffic profiles – an Information Bottleneck approach, *Knowlegde-Based Systems*, 197. https://doi.org/10.1016/j.knosys.2020.105875

Suler, J. R. (2016). Psychology of the Digital Age: Humans Become Electric Cambridge University Press. https://doi.org/10.1017/CBO9781316424070

Tao, L. (2008). Dynamic detection for computer virus based on immune system. *Science in China Series F: Information Sciences*, *51*(10), 1475-1486.

Toygar, A., Rohm, T., and Zhu, J. (2013). A New Asset Type: Digital Assets, *Journal of International Technology and Information Management*, *22*(4), https://scholarworks.lib.csusb.edu/jitim/vol22/iss4/7

Williams Jiménez, I. (2020) El contexto cambiante de los riesgos psicosociales. Riesgos emergentes y el impacto de la tecnología. En: Correa Carrasco, Manuel; Quintero Lima, María Gema (coord.). *Los nuevos retos del trabajo decente: la salud mental y los riesgos psicosociales (Objetivos de Desarrollo Sostenible 3,5,8,10)*. Getafe; Universidad Carlos III de Madrid, pp. 112-126. https://e-archivo.uc3m.es/handle/10016/29766

Zimmermann, L. (2021), "Your Screen-Time App Is Keeping Track: Consumers Are Happy to Monitor but Unlikely to Reduce Smartphone Usage," *Journal of the Association for Consumer Research*, *6* (3), https://doi.org/10.1086/714365