Information protection in the digital age: A shared responsibility

Jorge Arturo López Arias, Hugo del Ángel Delgado, Víctor Manuel Arias Peregrino,
Dulce María León de la O, Clemente Hernández Arias

Tecnológico Nacional de México - Campus Villahermosa/Instituto Tecnológico de Villahermosa, División de Estudios de Posgrado e Investigación

Abstract

Information security is a set of proactive and reactive measures backed by multiple regulations worldwide, which are constantly changing due to various events where the misuse of personal data has shown that it can be used for malicious purposes with questionable outcomes. In an interconnected world where nothing is inherently private, where benefits are not free, and where the duality of business-government is not immune to technical flaws or immoral conduct, information security becomes a key component for the protection of our data, and where it is the responsibility of the user to be aware of how, when, and under what conditions to share their information.

Resumen

La seguridad de la información es un conjunto de medidas proactivas y reactivas que tiene respaldo de múltiples regulaciones en el mundo, las cuales se mantienen en constantes cambios a causa de diversos eventos en los que el uso indebido de los datos personales a demostrado que pueden ser utilizados con fines maliciosos y con resultados cuestionables; en un mundo interconectado donde nada es privado en sí mismo, donde los beneficios no son gratuitos y donde la dualidad empresa-gobierno no es ineludible a defectos técnicos o a conductas amorales, la seguridad de la información se convierte en un componente clave para la protección de nuestros datos y donde al usuario le corresponde hacer conciencia en el cómo, cuándo y en qué condiciones ceder su información.

Keywords: Panóptico, Data Survillance, Psychographics Operations, Cambrindge Analytica
Palabras Clave: Panóptico, Vigilancia de datos, Psicografía, Operaciones psicológicas, Cambridge Analytica

1. INTRODUCTION

In the digital age, full of inventions and technological developments in data processing, one of the most important topics to consider is information security and its most sensitive aspects such as privacy and the security of personal data. With the vast amount of information generated daily, concern for its protection is increasingly greater. Day by day, people face the exposure, manipulation, or loss of data since, due to the rapid development of technology, monitoring online user activity has become a common practice. Companies and governments can collect information about users, including their interests, political preferences, behaviors, and more. In this article, we will explore concepts such as the Panopticon, Personality Tests, Data Surveillance, and mention the notable case of Cambridge Analytica.

2. THE PANOPTICON: THE ALL-SEEING EYE

At the end of the 18th century, prisons began to fill up due to the American War of Independence in 1776, followed by the French Revolution in 1789, and the replacement of corporal punishment with loss of liberty as a penalty. This was the reason to structure a formula that would accelerate the release of detainees from prisons, and that each one would be successfully reintegrated into society.

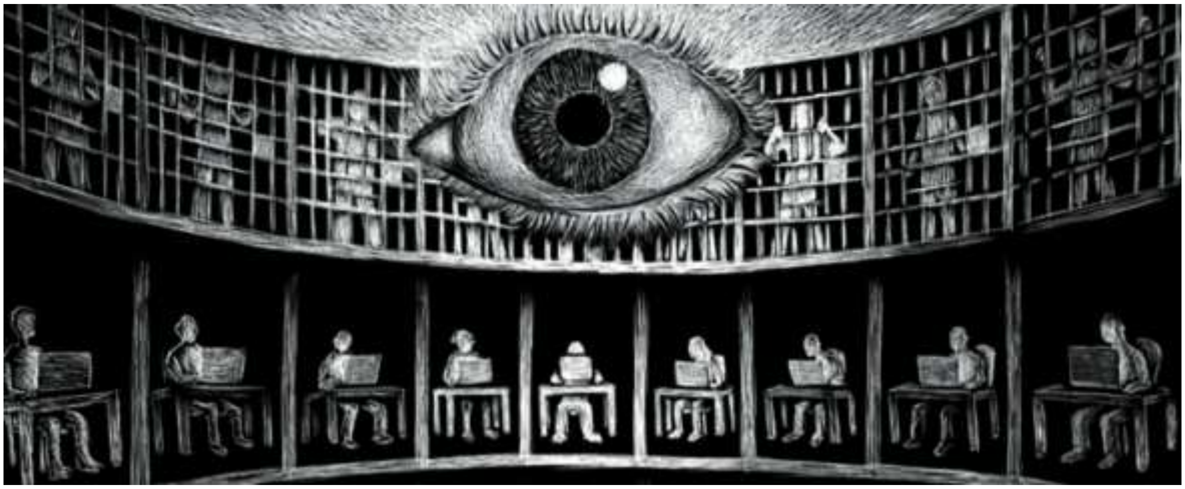

Figure 1. "The panopticon is a machine for dissociating the see-being seen pair" (Foucault Michael, 1980)

One of the most approved proposals was that of the philosopher and economist Jeremy Bentham: the panopticon (from the Greek root "to see everything" (pan-opticon), whose most elementary explanation is: a circular prison with cells on the perimeter, which are easily visible from the center of the building's floor plan, where a tower is erected, and from its interior, guards monitor detainees 24/7. And what is the notable advantage of this idea? The detainees will not know when they are being watched. As the detainee is aware of being watched, he or she is forced to behave, a self-monitoring in conformity with the law, or by habit. This results in an inner monologue driven by the paranoia of surveillance by the invisible guard. The detainee becomes aware of their crime and understands the behavior expected of a person in a civilized society with legal precepts (Foucault Michael, 1980).

Bentham's model did not succeed, although several prisons were built with that idea. The loss of interest in the system was due to human instrumentalization, given the mental burden caused by continuous observation.
"I have no doubt that we live within a digital panopticon" Miren Gutiérrez, (Rouco, 2020), who is the Director of the Postgraduate Program "Analysis, Research, and Data Communication" and a Professor of Communication at the University of Deusto in the Basque Country. The way we give up our information when requesting to be a user of a website or an application is no longer a subject of reflection. We just enter, fill out the form, and continue with our day, without thinking about whether that service really needs to know the vast majority of the personal information it requests.

The concept of the observed person still persists today, aware of their surveillance but not knowing where or when. This situation arises due to the frequent use of technological platforms (email, mobile applications, Google, YouTube, Instagram, Twitter, WhatsApp, Facebook, etc.) since with each interaction with these services, the associated behavior is saved and never deleted. This creates a digital footprint of the user with which the vast universe of collected data can be identified, known, used, and dominated, transforming them into personality models.

3. DATA SURVILLANCE

The panopticon is limited because the observed and observer must coincide in time and space, unlike the panspectrum (Rouco, 2020) (a term coined by Sandra Braman) in which the watcher can do their job even if the watched is hundreds of kilometers away or on the other side of the world; this ability to monitor is called data surveillance (dataveillance), which involves tracking the digital footprint through the collection and monitoring of online data generated in different types of services (electronic banking, shopping sites, phone calls, GPS tracking, geolocated photographs, opinion forums), collected in real-time, allowing for the identification of social and political preferences. In general, all everyday tasks carried out on the internet provide data that is considered private and, once obtained, needs to be converted into useful information, so algorithms are designed using big data and artificial intelligence, which are subsequently used to compete for individuals' attention with content specifically crafted to influence behavior in a subtle but effective way for their purposes. (Hawthorne, Steven, n.d.)

"The surveillance and intelligence have always been an important part for governments, for better or for worse," as stated by Miren Gutierrez (Rouco, 2020). This premise considers that the government should be informed about the needs of the citizens in order to govern with certainty and direct efforts towards the common good. However, when surveillance is exercised through the corporate-governmental amalgam, detailed plans within a legal framework must be established to avoid transgressing users' rights. Data surveillance has been a subject of controversy in many countries as many people consider it to violate users' privacy, and the duality of corporate-government should be more transparent regarding data collection and use (Rouco, 2020).

Some governments have implemented laws to protect users' privacy online; the law governing personal data protection varies by country and region.

Here are some examples:

- In the European Union, the General Data Protection Regulation (GDPR) sets the rules for the protection of personal data of European citizens. The GDPR applies to all companies that process personal data of European citizens, regardless of where the company is located.
- In the United States, the California Consumer Privacy Act (CCPA) sets rules for the collection, use, and disclosure of personal information of California residents. Additionally, the California Privacy Rights Act of 2018 (CPRA), also known as Proposition 24, is a broader privacy law that took effect in 2023 and expands the privacy protections established by the CCPA.
- In Mexico, the Federal Law on Protection of Personal Data Held by Private Parties establishes the rules for the protection of personal data held by private companies and organizations.

4. PERSONALITY AND BIG DATA: SHOULD WE BE WORRIED?

In a social interaction environment, the correspondence of roles is modeled primarily by the family nucleus, followed by the state structure, and ending with religion. This social framework brings with it the obligation to shape our behavior to what society expects of each individual, and this is where psychology takes an active role in understanding human behavior using descriptive models such as the Big Five test (Costa & McCrae, 1992), which allows scoring of the 5 main personality traits: Openness to experience, Conscientiousness, Extraversion, Agreeableness, and Emotional stability. This method was developed and refined with the collaboration of psychologists and researchers such as Lewis Goldberg, Warren Norman, Paul Costa, and Robert McCrae, which serves to categorize personality, which is defined as a set of thoughts, feelings, and behaviors. These behavior patterns are currently manifested significantly in the use of technology.

The digital psych politics fueled by Big Data and Machine Learning is consolidating as the digital big brother. It is for this reason that the term digital panopticon is becoming relevant today, being essentially the first almost immaterial system that leans more and more towards the invisible as its dominion is transferred to digital media that influence our psyche, magnifying the central idea of seeing and not being seen.

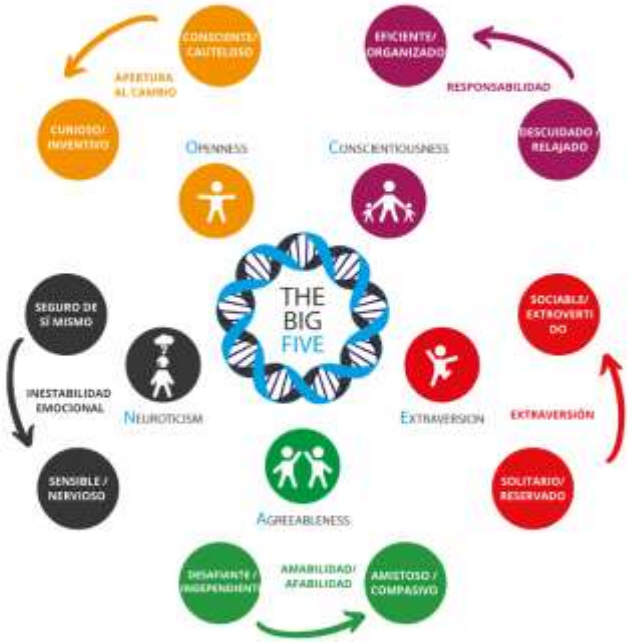

Figure 2. Big Five traits - Openness, Conscientiousness, Extraversion, Agreeableness, Neuroticism

Private companies and governments collect a large amount of data about online users, this information can be used for advertising purposes but it can also be used for darker purposes such as spying or political manipulation through the application of artificial intelligence algorithms that seek to understand how to direct people and subtly redirect their interests; in other words, it is the most effective way to show desired information and obtain approval based on empathy as emotional contagion.

5. CAMBRIDGE ANALYTICA: APPLIED PSYCHOLOGICAL OPERATIONS.

Currently, advertising or ads are only allowed to reach people based on the tracking data that reveals interests (favorite movies or music, favorite characters, sites of interest, etc.), but if we combine the following ingredients: mathematics, psychology, innovation, technology, and the human being with their participation, either unconsciously or consciously, in a network created to unite and strengthen ties in this globalized world, what could go wrong?

Scenario: 2016 United States presidential election, with the Republican Party's formula with their candidates Donald Trump and Mike Pence against the Democratic Party's duo with their representatives Hillary Clinton and Tim Kaine.

Advisory company: SCL Elections and Cambridge Analytica, the latter dedicated to data mining and analysis, companies that had Alexander Nix as CEO in common.

Actors: GSR - Prof. Aleksandr Kogan, belonging to the University of Cambridge and also serving as an associate professor at the University of St. Petersburg, Steve Bannon, Vice President of Cambridge Analytica and former White House Chief Strategist, and Robert Mercer, hedge fund magnate in the US.

Social network: Facebook - Mark Zuckerberg, co-founder, and CEO.

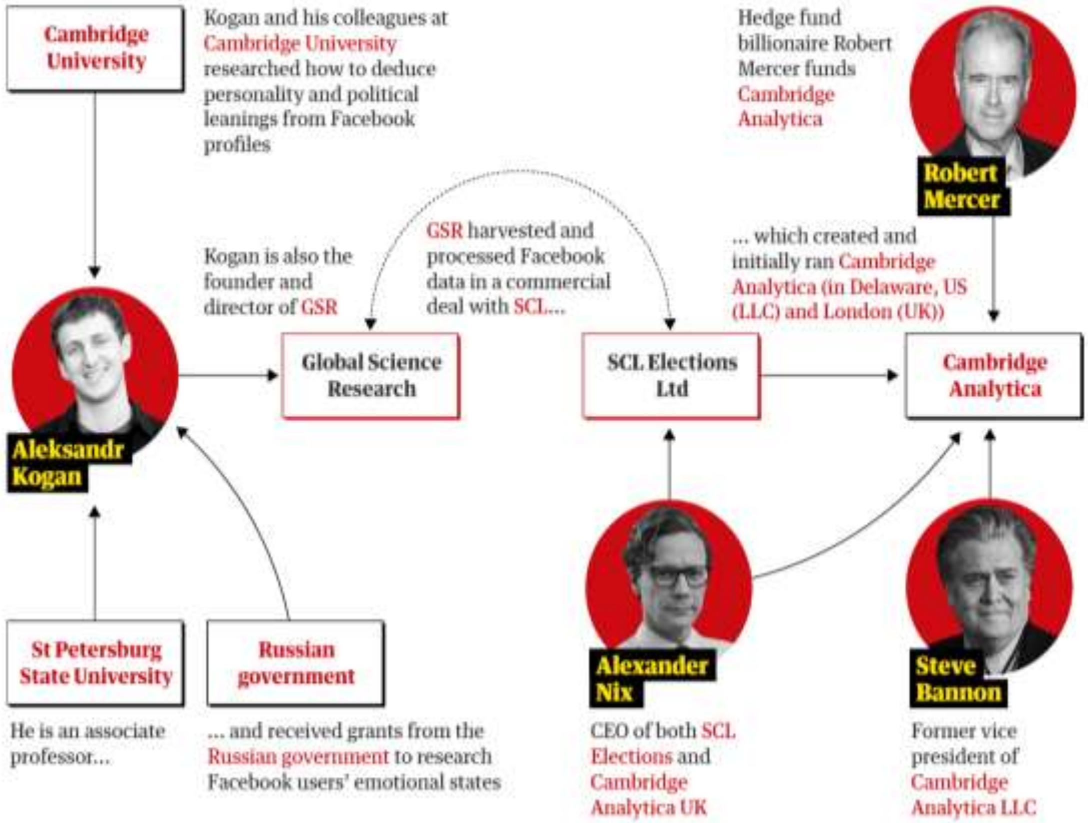
Cambridge University
Kogan and his colleagues at Cambridge University researched how to deduce personality and political leanings from Facebook profiles
Hedge fund billionaire Robert Mercer funds Cambridge Analytica
Robert Mercer
Kogan is also the founder and director of GSR
GSR harvested and processed Facebook data in a commercial deal with SCL...
... which created and initially ran Cambridge Analytica (in Delaware, US (LLC) and London (UK))
Aleksandr Kogan
Global Science Research
SCL Elections Ltd
Cambridge Analytica
St Petersburg State University
Russian government
Alexander Nix
Steve Bannon
He is an associate professor...
... and received grants from the Russian government to research Facebook users' emotional states
CEO of both SCL Elections and Cambridge Analytica UK
Former vice president of Cambridge Analytica LLC

Figure 3. Cambridge Analytics: How the key players are linked. (Guardian graphic)

5.1 Exposing the Cambridge Analytica case to public scrutiny

The first public denunciation of personal data harvesting by the Cambridge Analytica (CA) case happened at the end of 2015 by Harry Davies (Ted Cruz campaign using firm that harvested data on millions of unwitting Facebook users | US news | The Guardian, n.d.), a journalist for The Guardian, who declared the use of this data in Ted Cruz's campaign. This was followed by McKenzie Funk, a reporter for The New York Times Sunday Review, in November 2016 and Carole Cadwalladr for The Guardian in February 2017, but the highest point was when a former CA employee appeared on the scene and took on the role of whistleblower, Christopher Wylie. His approach to Carole Cadwalladr (Cadwalladr & Graham-Harrison, 2018), a reporter for The Observer and The Guardian, led to a series of exclusive interviews that exposed the way in which CA provided its services since 2014. Subsequently, a journalist from UK Channel 4 News (n.d.) conducted an undercover investigation and held a meeting with Cambridge Analytica executives, represented by Alexander Nix, the CEO of the company, Mark Turnbull, and Alex Tayler, the Head of Data Services. In this meeting, their involvement in multiple elections and consensuses was evidenced, mentioning in particular Brexit and the US election campaign. The following statements were taken from the video of the meeting:

"We did all the research, all the data, all the analytics, all the targeting, we ran all the digital campaign, the television campaign and our data informed all the strategy," Nix told the undercover reporter (Neuman, 2018).

"We just put information into the bloodstream of the internet and then watch it grow, give it a little push every now and again... like a remote control. It has to happen without anyone thinking, 'that's propaganda,' because the moment you think 'that's propaganda,' the next question is, 'who's put that out?'" he said. "So we have to be very subtle" (Neuman, 2018).

5.2 Reconstructing the events

The strategy of CA began with the activities of GSR (Global Science Research) which, in a commercial agreement with CA, carried out paid advertising campaigns on Facebook in 2014 to encourage users to take a personality test through an application called ThisIsMyDigitalLife. This application had permission to operate within the social network for data collection for academic purposes. The operation was simple, claiming academic purposes, they paid the user to answer the survey and requested permission to access their profile to provide the test result. However, the respondent did not know that they were also granting access to their friends' network and information without them needing to enter the survey. Subsequently, using an algorithm based on the Big Five personality traits (Stillwell & Kosinski, n.d.), they structured the personality of each user who installed that application and that of their friends. The collected data formed psychographic profiles and with this, the strategy to create personalized messages achieving behavioral micro-targeting to redirect information and influence millions of users about their vote in the US elections. It is worth mentioning that the number of personality study participants was 270,000 users, but when linked to the network of contacts, this number reached 50 million users. Facebook became aware of this situation in 2015 thanks to the investigation carried out by Harry Davies, a reporter for The Guardian, providing a more precise figure of approximately 87 million users whose data was compromised.

What is alarming is that the commercial agreement to purchase the data of 87 million US Facebook users was illegal, and CA, who used the information for questionable purposes, is no longer considered a data mining and analysis company but rather a company that profits from the use of behavioral microtargeting (Cadwalladr, 2018) in the electoral environment, applying PsyOps (psychological operations) («Psy-Ops de oferta», 2018) for behavioral control using fake news, discrediting, and a mercenary propaganda agency.

On the other hand, in August 2016, shortly before the US elections and two years after the data extraction took place, Facebook sent an email to CA informing them that the data had been obtained illegally and that GSR was not accredited to share or sell any data collected by ThisIsMyDigitalLife. In such case, the data had to be deleted entirely, and CA's response was to select a checkbox, sign it, and return it, without Facebook taking any further action to retrieve the data.

Since the 1990s, CA has participated in communication warfare applying PsyOps during elections held in Argentina 2015, Malaysia 2013, Kenya 2013, Italy 2012, Colombia 2011, India 2010, Trinidad and Tobago 2009, Ukraine 2004, Thailand 1997, South Africa 1994, and once they perfected their data modeling, it was used in Great Britain for Brexit 2016 and the United States during the 2016 elections (Jehane Noujaim, Karim Amer, 2019).

5.3 Consequences for the parties involved

Cambridge Analytica was the subject of investigations on both sides of the Atlantic, with a total of three investigations, two in the UK: The Electoral Commission, regarding the company's possible role in the EU referendum, and the Information Commissioner's Office, regarding the analysis of data for political purposes; and one in the US conducted by special counsel Robert Mueller on the collusion between Trump and Russia to influence the 2016 elections. In May 2018, Cambridge Analytica declared bankruptcy in an attempt to stop the investigations.

Mark Zuckerberg spoke before US and UK authorities, and these are his most notable statements (It was my mistake and I'm sorry, 2018):

- "In retrospect, it was clearly a mistake" to think that Cambridge Analytica had deleted the data without verifying it.
- He doesn't "feel" that Facebook is a monopoly.
- "There will always be a free version" of Facebook.
- Managing hate speech automatically has "a higher error rate than I would like."
- Zuckerberg expressed personal concern about the possibility of his company having a political bias.

As for Facebook, in July 2019, the US Federal Trade Commission (FTC) ordered the company to pay a $5 billion fine for its mishandling of user data security, and forced the creation of an independent committee for privacy data regulation. Following this announcement, the company's reputation was damaged, and investors' reactions were not long in coming, as the social network suffered an 8% drop in its shares, resulting in a monetary loss of $46 billion in the company's value. Likewise, the ICO, the body responsible for enforcing data protection rules, stated that Facebook allowed the violation of legislation by enabling and not limiting access to its users' data in the UK without "clear consent," resulting in a fine of €565,000 in October 2019.

6 CONCLUSION

"When a product is free, you are the product."

Currently, there are multiple platforms that provide quick, easy and free means for sharing ideas and thoughts. On these sites, behaviors and actions leave traces that do not disappear and, without one knowing, feed an industry that perceives billions of dollars per year. In the digital world, it is very easy to install applications on smartphones or navigate sites of interest; however, one forgets to read the terms and conditions (a section that indicates the purpose of the site or application, as well as the rules of use) in such a way that the individual ceases to be a consumer of the product and becomes the product itself.

The value of companies like Google and Facebook lies in the fact that they are the ones who store, organize, segment, and suggest products and services based on individual preferences. These organizations constantly observe the information of millions of people around the world, which leads to the urgent need for global legislative improvements where individuals own their data as a property and this becomes a fundamental human right for the sake of privacy. It is important to note that, regardless of the specific law that is applied, the protection of personal data is an important and sensitive issue that affects everyone, and appropriate safeguards must be established to ensure the privacy and freedom that are the genuine basis of human development to ensure compliance with democracy and prevent crimes (fraud, identity theft, etc.).

As individuals, we can limit the flow of data that we expose through various means, but there is no way to hide. Consequently, it is imperative to understand that data in the wrong hands can affect daily life. Therefore, each individual must assume the responsibility of conscious analysis and choice of what they want to see, hear, know, and share.

REFERENCES

[1] Cadwalladr, C. (2018, marzo 18). 'I made Steve Bannon's psychological warfare tool': Meet the data war whistleblower. The Guardian. https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump

[2] Cadwalladr, C., & Graham-Harrison, E. (2018, marzo 17). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

[3] Channel 4 News (Director). (s. f.). Cambridge Analytica: Undercover Secrets of Trump's Data Firm—YouTube (Vol. 335) [Reportaje de investigación]. Channel 4. Recuperado 27 de febrero de 2023, de https://www.youtube.com/watch?v=cy-9iciNF1A

[4] Costa, & McCrae. (1992). Four ways five factors are basic. Personality and Individual differences.

[5] Foucault Michael. (1980). Vigilar y Castigar (1ra ed.). Siglo veintiuno editores Argentina s. a.

[6] «Fue mi error y lo siento»: Mark Zuckerberg comparece ante el Congreso de EE.UU. por el escándalo de Cambridge Analytica. (2018, abril 10). BBC News Mundo. https://www.bbc.com/mundo/noticias-internacional-43720004

[7] Hawthorne,Steven. (s. f.). MCF, modelo de los cinco grandes factores de la personalidad: OCEAN (PSICOLOGÍA).

[8] Jehane Noujaim, Karim Amer (Director). (2019). The Great Hack [Documental]. Netflix, The Othrs. https://www.netflix.com/mx/title/80117542

[9] Neuman, S. (2018, marzo 21). In Hidden-Camera Exposé, Cambridge Analytica Executives Boast Of Role In Trump Win. NPR. https://www.npr.org/sections/thetwo-way/2018/03/21/595470164/in-hidden-camera-expose-cambridge-analytica-executives-boast-of-role-in-trump-wi

[10] Psy-Ops de oferta: Cambridge Analytica es lo que sucede cuando se Privatiza lo Militar. (2018, abril 15). Kaos en la red. https://archivo.kaosenlared.net/psy-ops-de-oferta-cambridge-analytica-es-lo-que-sucede-cuando-se-privatiza-lo-militar/index.html

[11] Rouco, F. (2020, enero 21). El panóptico digital, el gran temor distópico que acecha tras la revolución de los datos, la inteligencia artificial y la «dataveillance». Xataka. https://www.xataka.com/privacidad/panoptico-digital-gran-temor-distopico-que-acecha-revolucion-datos-inteligencia-artificial-dataveillance

[12] Stillwell, D. J., & Kosinski, M. (s. f.). myPersonality project: Example of successful utilization of online social networks for large-scale social research.

[13] Ted Cruz campaign using firm that harvested data on millions of unwitting Facebook users | US news | The Guardian. (s. f.). Recuperado 27 de febrero de 2023, de https://web.archive.org/web/20160216175150/http://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data

Corresponding Author: ***jalopezarias78@gmail.com***