

# Who Stands to Blame? Digital Platforms as Enablers of Insidious Acts

Bruno Luis Avila Freischlag<sup>1</sup> , Bruno Anicet Bittencourt<sup>1</sup> 

<sup>1</sup>Universidade do Vale do Rio dos Sinos, Porto Alegre, RS, Brazil

**How to cite:** Freischlag, B. L. A., & Bittencourt, B. A. (2024). Who stands to blame? Digital platforms as enablers of insidious acts. *BAR-Brazilian Administration Review*, 21(4), e230124.

**DOI:** <https://doi.org/10.1590/1807-7692bar2024230124>

## Keywords:

dark side; digitalization; social media

## JEL Code:

M14

## Received:

October 31, 2023.

This paper was with the author for one revision.

## Accepted:

April 20, 2024.


## Publication date:

June 25, 2024.


## Corresponding author:


Bruno Luis Avila Freischlag  
Universidade do Vale do Rio dos Sinos  
Av. Dr. Nilo Peçanha, n. 1600, Boa Vista, CEP 91330-002,  
Porto Alegre, RS, Brazil


## Editor-in-Chief:

Ivan Lapuente Garrido   
(Universidade do Vale do Rio dos Sinos, Brazil)

## Guest Editors:


Amarolinda Zanela Klein   
(Universidade do Vale do Rio dos Sinos, Brazil)

Cristiane Pedron   
(Universidade Nove de Julho, Brazil)


Silvia Elaluf-Calderwood   
(Florida International University, USA)

Winnie Ng Picoto   
(Universidade de Lisboa, ISEG, Portugal)

## Associate Editor:

Minelle Silva   
(University of Manitoba, Canada)

## Reviewers:

Edvan Cruz Aguiar   
(Universidade Federal de Campina Grande, Brazil).  
and one anonymous reviewer.

## Editorial assistants:

Eduarda Anastacio and Simone Rafael  
(ANPAD, Maringá, Brazil).

## ABSTRACT

**Objective:** Understand how digital platforms can be used to render insidious acts, and what roles each actor plays within such ecosystem. **Methods:** We conducted a non-participant observation of 32 videos and thousands of comments on the YouTube platform on the context of digital predation of minors. Data were codified through thematic analysis. **Results:** We ended up unraveling six major enablers – i.e., (1) frailty, (2) burdening, (3) ineffective oversight, (4) unaccountability, (5) sense of impunity, and (6) digital naivety, at three levels: organizational, institutional, and individual. **Conclusions:** This research complements the theory of the digital platforms ecosystem by framing the ‘dark’ side of interactions and illustrating six building blocks that surround the insidious acts occurring within social media platforms. The proposed framework helps us understand how each of these actors facilitates the occurrence of insidious acts through the so-called enablers. Practical and social contributions were also provided.



**Data Availability:** Freischlag, Bruno; Bittencourt, Bruno (2024), "Data for: Who stands to blame? Digital Platforms as enablers of insidious acts, published by BAR - Brazilian Administration Review", Mendeley Data, V1, doi: [10.17632/9mkrw3vbn1](https://doi.org/10.17632/9mkrw3vbn1)  
BAR – Brazilian Administration Review encourages data sharing but, in compliance with ethical principles, it does not demand the disclosure of any means of identifying research subjects.

**Plagiarism Check:** BAR maintains the practice of submitting all documents received to the plagiarism check, using specific tools, e.g.: iThenticate.

**Peer review:** is responsible for acknowledging an article's potential contribution to the frontiers of scholarly knowledge on business or public administration. The authors are the ultimate responsible for the consistency of the theoretical references, the accurate report of empirical data, the personal perspectives, and the use of copyrighted material. This content was evaluated using the double-blind peer review process. The disclosure of the reviewers' information on the first page is made only after concluding the evaluation process, and with the voluntary consent of the respective reviewers.

**Copyright:** The authors retain the copyright relating to their article and grant the journal BAR – Brazilian Administration Review, the right of first publication, with the work simultaneously licensed under the Creative Commons Attribution 4.0 International license (CC BY 4.0) The authors also retain their moral rights to the article, including the right to be identified as the authors whenever the article is used in any form.

## INTRODUCTION

No one can deny the benefits that digitalization brought to our daily lives. The widespread use of the internet revolutionized the way that we humans interact with each other. Through bits and bytes, we now convey information nearly at the speed of light and in a ubiquitous fashion. One in South America can now communicate and share a virtuality of experiences with another in New Zealand. Just by having a device connected to the internet, no place seems too far away. At an exponential pace, we are now blurring every border that once kept us away from each other. In fact, we may be on the very brink of Zweig's dream; a *bona fide* borderless world. Nevertheless, one can be very easily bewitched by such wonders. When this pace becomes exponential, it also runs the risk of being unbridled. With the digitalization as our Icarus' wings, we might be flying directly toward the sun, heedless of the very menaces that lurk behind its blinding lights. These so-called menaces are also referred to in the academic world as the 'dark side of digitalization' and have been under inquiry for quite some time.

One of the most recent dark implications of digitalization is privacy. Nowadays we do have a pressing concern with who has access to our data and, perhaps most unsettling, what is done with it. Zuboff (2015) christened the term 'surveillance capitalism' to describe this very aspect of digitalization. In a borderless world, how can one ensure their privacy? This question proved to be a delicate matter, involving individual, organizational, and institutional actors. Big tech companies such as Google play a major role in such a conundrum. In fact, every digital platform where information is often shared between users has a prominent role in understanding this phenomenon.

Almost paradoxically, while the majority of the discussion revolves around the topic of privacy, or the lack thereof, some actors seem to disregard the idea of a surveillance mechanism altogether. That is the case of those who use these digital platforms to commit insidious acts. Insidious acts come from behaviors that generate real and serious negative repercussions in the life of one or more of the actors involved. Indeed, social media can also be used for irresponsible, criminal, and hateful ends (Müller & Schwarz, 2021; Whelan et al., 2013). From the diffusion of fake news and hate speech toward minority groups to the sharing and selling of illegal products such as drugs and child pornography, each of the aforementioned can have harmful psychological and physical effects on users (Müller & Schwarz, 2023; Trittin-Ulbrich et al., 2021).

Despite that, we have little to no knowledge whatsoever on why we allow such insidious acts to happen

in the first place — or better yet, what may enable them. By questioning what factors contribute to the occurrence of insidious acts within digital platforms, this article aims to identify these factors (i.e., the enablers) and to link them to the actors within an ecosystem of digital platforms. To achieve this, we dove into the context of digital predation of minors and the sharing of child pornography. Through a non-participant observation of 32 videos and thousands of comments on YouTube, we uncovered six major enablers — i.e., (1) frailty, (2) burdening, (3) ineffective oversight, (4) unaccountability, (5) sense of impunity, and (6) digital naivety — at three levels: (1) organizational, (2) institutional, and (3) individual.

This study complements existing research on digital platforms and its dark implications by framing the bad side of the interactions between the actors in an ecosystem. We also explore how these interactions could potentially extrapolate from digital space to harmful real-world implications. Following the Kietzmann et al.'s (2011) proposal of a honeycomb-shaped framework, we propose six building blocks that enable insidious acts within social media platforms. The proposed framework helps us understand how each of these three actors facilitates the occurrence of insidious acts through the so-called enablers. We also discuss approaches at both the managerial and governmental level that could deal with this problem on both ends. Lastly, we also highlight the study's potential for social change, as it brings light to this dark side and calls for pressing changes in both organizations and institutions to make the virtual environment safer for every one of its users.

The paper is structured as follows: (1) the theoretical background, which brings the concept of digital platforms and ecosystems, as well as the actors that takes part in this ecosystem and their roles within; (2) the research design, which brings and justifies the methodological choices and procedures, such as data collection and data analysis; (3) the findings, in which the evidence is compiled and contrasted with the literature; (4) the discussion; which brings the framework and possible approaches on how to mitigate the incidence of insidious acts within digital platforms; and (5) the final remarks, that explain the theoretical, practical, and social contributions, talk about the avenue for future studies, and discuss the research's limitations.

## THEORETICAL BACKGROUND

### Digital platforms and the digital ecosystem

Digital platforms certainly do not lack in definitions. Some derive from their economic or functional aspects (e.g., Rossotto et al., 2018), technical (e.g., Sedera et al.,

2016), or sociotechnical aspects (e.g., [De Reuver et al., 2018](#)). Regardless, digital platforms are usually technologically mediated, enable interactions between users, and allow users to render a particular intent ([Koskinen et al., 2019](#)). In addition, digital platforms can be defined based on their use, as in the case of social media or networks (e.g., [De Reuver et al., 2018](#)) — software-based platforms that offer an interface through which individuals interact ([Tiwana et al., 2010](#)). Following this perspective, we define digital platforms simply as cyber or virtual environments through which individuals interact with each other.

Digital platforms are therefore not an isolated phenomenon. Their use and very existence are in fact influenced by a set of economic, organizational, institutional, and spatial forces ([Bonina et al., 2021](#)). Consequently, digital platforms are seen as enablers of new ecosystem innovations ([Gawer & Cusumano, 2014](#)), such as the digital ecosystem; “a self-organizing, scalable and sustainable system composed of heterogeneous digital entities and their interrelations focusing on interactions among entities to promote information sharing” ([Li et al., 2012](#), p. 119). A digital ecosystem is composed of two parts: one static, represented by the digital technologies and people, and one dynamic, defined by the interactions that together form the behavior of the ecosystem ([Elia et al., 2020](#), p. 150).

### The actors of a digital ecosystem

In this tenet, the digital platform ecosystem consists of “a platform owner that implements governance mechanisms to facilitate value creating mechanisms on a digital platform between the platform owner and an ecosystem of autonomous complementors and consumers” ([Hein et al., 2020](#), p. 90). Such ownership is under the domain of organizations — namely social media organizations (SMOs). These organizations are the ones within the digital ecosystem that retain the rights (i.e., governance) to mold the rules of such platforms at their own will, often to monetize the users’ interactions and profit from it. Consequently, their power distribution is highly centralized, giving little to no autonomy to their users ([Hein et al., 2020](#)) — those who represent the demand side.

Users can be defined as anyone who interacts with technology. They play a pivotal role in multisided platform businesses as SMOs since such organizations rely entirely on user-generated content from which they draw the majority of their revenue ([Sussan & Acs, 2017](#)). There is also the role of institutions. Deemed a fundamental pillar within the ecosystem, institutions are simply known as ‘the rules of the game.’ Here, we refer to the institutions more explicitly as the governmen-

tal rules that facilitate or hinder the interactions within the ecosystem. It is therefore the legal aspects that the actors (i.e., the organizations and users) assent to in order to co-participate in a digital environment ([Sussan & Acs, 2017](#)). While platform owners rule over the interactions within their platform, the latter may also be subject to wider institutional forces through regulatory action ([Bonina et al., 2021](#)).

We understand a digital ecosystem of platforms as a virtual environment consisting of organization(s)-institution(s)-individual(s) interactions through a digital(s) platform(s). Organizations are seen as businesses that utilize the platforms as a means of personal exploitation. Institutions are the policymakers, which do or do not allow the platforms to be exploited. Finally, individuals are the end-users, who allow themselves to be exploited through the platforms. The theoretical lens of the digital platform ecosystem allows us to understand the actors involved and their roles in a systematic way.

### RESEARCH DESIGN

We applied a qualitative exploratory approach through netnography — an internet, cyber-, virtual ethnography is the most common instrument to research virtual social environments with traditional eutrophics standards ([Hine, 2008](#)). Among its many advantages, netnography allows for rich data collection otherwise impossible in a non-virtual environment, along with the implementation of several data collection instruments ([Lopez-Rocha, 2010](#)). Moreover, when analyzing the social media phenomenon and its dark implications, contemporary methodologies such as netnography are considered most suitable for understanding social interactions in a social media context ([Baccarella et al., 2018](#)).

We chose to study the exposure of children online to ‘Category A’ pictures, the most severe level of child abuse material online. Category A material has more than doubled from 2018 to 2022, and the number of reports suspected of containing Category A material already stands at 375.000 images ([Internet Watch Foundation, 2023](#)). This denotes that our current solutions are not sufficient to deal with such problems as they deserve. Exposure to child abuse materials can have several harmful and long lasting consequences for children and adolescents, including psychological damage, self-harm tendencies, and even suicidal behavior ([Chang et al., 2021](#)). This denotes a pressing need to understand how children experience abuse and exposure online, who is most vulnerable, who are the perpetrators, and if our current generation is armed with the right knowledge to deal with this hostile environment ([Bantourakis & Manojlovic, 2023](#)).

## Data collection

The data collection was conducted through non-participant observations, an instrument where researchers insert themselves into social systems to observe behaviors and interactions within a given culture in order to gain an understanding of phenomena in their natural settings without interacting with it (Liu & Maitlis, 2010). Some particular situations do not give room from direct participation through involvement. However, researchers can still gather data and draw conclusions from it through non-participant methods (Spradley, 1980).

Such is the case here. Gathering data from observational participation is impractical for this subject, considering that the 'dark side' of the topic often consists of information that can compromise or incur in psychological harm to the source itself. Moreover, it is assumed that many would not be so keen to share such sensitive information to an unverified third-party (i.e., the researcher), if not in specific contexts that cannot be reproduced by the researcher due to limitations, such as knowledge, professional license, and lack of financial resources. On the other hand, the internet offers a great deal of data from points of view other than that of the researcher, which can overcome most of these limitations without necessarily compromising the data's reliability.

We choose the YouTube platform as a field of research, or as Netnography space. YouTube is one the largest video sharing platforms, holding a digital archive of more than 800 million videos, 144 million active YouTube channels and 2.6 billion of active users monthly (Hayes, 2023), and thus has huge potential as a data source (Sui et al., 2022). In addition, the YouTube's material does not need to be subject to human subjects guidelines nor to consent since YouTube is a public forum where all uploaders agreed with its guidelines (Berger, 2012). As a matter of fact, other research studies have already used the YouTube platform to carry out this type of thematic analysis (e.g., Ratwatte & Mattacola, 2019). Nevertheless, we took care not to disclose any type of personal information that could identify those directly involved in the videos.

We followed the Sui et al.'s (2022) five steps framework for conducting research in YouTube. On the YouTube platform, we used the search strings 'digital predator,' 'online predator,' and 'online grooming' on the search bar in an incognito tab in order to avoid algorithmic bias (Sui et al., 2022). However, the latter string was later disregarded due to video redundancy. The search was sorted by 'relevance' and no other filters were applied. The researchers thoroughly

reviewed the content of each video to determine if it matches the research problem. We had 21 valid recurrences directly from the both strings, and 11 valid recurrences from the recommendation tab of each video, following the snowball technique (see Table 1).

**Table 1.** Search strings and the total of valid recurrences.

String	Recurrences
Digital predator	15
Online predator	7
Recommendation <sup>1</sup>	11
Unique videos	32

**Note.** <sup>1</sup> Videos resulting from the suggestion sidebar. Source: Author's elaboration.

At the end, we reached a total of 32 unique videos, totaling almost 10 hours of content and 170 thousand comments. We also collected supplement data such as numbers of viewers, channel's number of subscribers, and verified status to ensure the findings' reliability.

## Data analysis

The data thematic analysis used both oral evidences extracted from the videos, as well as written statements from the comments sections, following the six phases proposed by Braun and Clark (2006), which are: (1) familiarization and immersion through the reading and re-reading the data to identify potential codes; (2) coding the evidence using these codes; (3) collating the codes into themes; (4) reviewing the themes; (5) defining and naming each theme; (6) providing an example of each code through the excerpts from the data. The data gathered were deemed sufficient following the Merriam and Tisdel's (2015) saturation and redundancy criteria when further observations did not add any new knowledge whatsoever. Such evidence was then compiled (see Table 2). We reached 59 pieces of evidence, six codes and three themes.

## FINDINGS

Using the ecosystem lens, we were able to identify six enablers for each of its actors. We found that institutional forces often suffer from inadequate legal and operational capacity to exert efficient power over digital platforms. Organizations' ineffective oversight and lack of accountability for what happens within their digital platforms can also contribute to the emergence of insidious acts within. Lastly, at the individual level, perpetrators of such acts enjoy a sense of impunity while the victims seem to suffer from digital naivety. Table 2 comprises our codification through the ecosystem lens based on gathered evidence.

**Table 2.** Themes, codes, definitions, and evidences.

Theme	Code	Definition	Evidence
Institutional Enablers	Frailty	Regulations and policymakers exert little to no influence on SMOs.	"Alice's suit is likely to be one, if not the first time a tech platform is put on trial for the way it's built" (a reporter).
	Burdening	Institutional forces as law enforcement cannot follow the exponential pace that insidious acts occur within digital platforms.	"Our job became increasingly more difficult with the amount of data that is available" (FBI agent).
Organizational Enablers	Ineffective Oversight	SMOs are falling in, or do not have the intent, to tackle illegal and harmful content from their online platform.	"The site is moderated, but... (negation onomatopoeia) They don't really know what's going on half of the time, to be honest" (an influencer).
	Unaccountability	SMOs do not hold themselves responsible for insidious acts within their platforms whatsoever.	"People are solely responsible for their behavior while using the website" (owner of a social media platform).
Individual Enablers	Sense of Impunity	The explicit exposure of perpetrators suggest that they are also moved by impunity.	"They have the feeling that they would not get caught, and live their fantasies online" (a detective inspector).
	Digital Naivety	Victims and parents alike often do not perceive social media as capable of real world harm.	"Many parents today worry more about physical danger of their children than they do online" (a pediatric).

Note. Source: Author's elaboration.

In the next subsections, we dive into the role of each of the three actors and by how they enable these insidious acts in greater depth.

### Institutional enablers: Frailty

Most of the regulatory body worldwide is yet not ready to deal effectively with problems regarding social media usage. Digital platforms are indeed poorly regulated in several countries. Scandals such as the 2014's Facebook CEO trial regarding data leaking and selling was a milestone on privacy related topics and the role of policymakers in it. Consequently, the 'platformization' of the internet raises questions of whether such an environment should be more meticulously regulated.

Digitalization often develops faster than the regulation or social structures (Organisation for Economic Co-operation and Development [OECD], 2019). The Uber application, for instance, has been banned in several countries already due to inability or unwillingness of governments to regulate it (Trittin-Ulbrich et al., 2021). Quite the contrary, big tech companies such as Google seem to have a significant hegemonic power over institutions to foment and align regulations with their own business interests (Whelan, 2019). Indeed, social media can contribute to the decentralization of power away from governments, whilst also centralizing the power in the hands of the organization that owns them (Whelan et al., 2013). Consequently, platforms alone do have the power to challenge the prevailing institutional logic by replacing it altogether (Bonina et al., 2021).

Needless to say, this so-called frailty can lead to huge institutional holes that could be, and indeed are, thoroughly exploited by these organizations to soci-

ety's detriment. One of such perceived holes is not how an organization exploits its users per se, but rather how it is built in the first place. As the evidence suggests, new lawsuits have been filed against corporations regarding how such platforms are inherently built as an enabler of these acts. This is called product liability – i.e., responsibility for harm or loss due to a product's, in this case the platform's, defectiveness, which can be in its flawed design or misleading advertisements (Matthews-EI, 2023). One prominent example is that of Omegle; a very popular virtual chatroom in which by the time that was online its website's frontpage said: "you are paired randomly with another person to talk one-on-one". Now, after 14 years online, Omegle has finally been shut down after several lawsuits alleging grooming and predation of minors on the platform, one alone totaling \$22 million in damages (Loffhagen, 2023). "It is a hunting ground for predators ... and quite literally encourages them (children) to 'talk with strangers'" (an attorney).

Laws on what can be perceived as a product liability differ drastically depending on the local regulations. Usually, most of these cases fall under the negligence category (Matthews-EI, 2023). However, this type of lawsuit is yet not popular against companies that hold social platforms, and those filed against are usually due to the platforms propensity to addiction and hindrances such as the diffusion of dangerous challenges and other forms of noxious influences (Furman, 2022), rather than how these platforms actually facilitate the interaction between minors and ill-intended individuals. Other regulatory concerns are about what the law considers to be child sexual abuse materials (CSAM), the lack of fines to companies that perpetuate the sharing of such materials, and the unsupervised usage

of social media by repeat offenders in crimes involving CSAM selling or consumption.

### **Institutional enablers: Burdening**

The ubiquitousness of the internet made the state machine to be stressed out to the point of almost collapse. This is what we call ‘institutional burdening’ – the governments are now helpless at following the exponential pace by which new cases come forth to develop and deploy effective countermeasures.

As the findings suggest, public entities such as the law enforcement do not have enough infrastructure to keep up with the coming cases. Such burdening is aggravated by two main factors: (1) human and (2) technology. Human concerns the understaffing of law enforcement, whereas technology refers to its lack, such as sophisticated pieces of software and hardware. Staff shortage is indeed a concern nationwide in America, as increasingly more people are not interested in pursuing such a vocation or they are not qualified enough (Klemko, 2023). Consequently, this shortage can be overwhelming for active-duty police officers, which would shift their attention toward more pressing and feasible-solved crimes.

The lack of technological instruments was also perceived as aggravating. Traditionally, law enforcement had a quite unfriendly relationship with technology, and are usually more keeping to traditional and age-old methods (Fatih & Bekir, 2015). However, the digitization of crimes starts to unavoidably shift this reality, which does not come without obstacles. The most perceived ones are: (1) the non-availability of technology; (2) the lack of notion about technologies available; (3) the unfriendliness of technologies; and (4) the inefficiency of technology (Custers, 2012). Another obstacle for technology adoption is that of cost, which requires significant funding (Dekker et al., 2020). Lastly, even in the cases where the technology is employed, some lack the proper training to use it.

### **Organizational enablers: Ineffective oversight**

At the very least, organizations are failing to tackle illegal and harmful content from their online platforms. The findings suggest that pornographic content as a whole, which should be illegal following the guidelines of most of these digital platforms, are in fact being shared at an unprecedented pace. The most critical tool by which organizations deal with such problems is moderation – i.e., a set of measures destined to first identify and further filter the content that do not follow a given platform’s guidelines and it is being exposed to the wide audience.

Nowadays, part of such moderation comes from human eyes. However, there are often low-paid jobs and dreadfully emotional taxing, as they require constant exposure to gruesome violence and disturbing sexual content (Stackpole, 2022). Many big tech companies also quite so often declare that they are constantly applying advanced machine learning algorithms as moderators in order to deter such harmful content from being shared. They seem to fail to be effective, all the same.

The level of complexity that the digitalization brought to social platforms suggests that it is somewhat unfeasible to organizations to oversee every bit of information, despite their best efforts. One could outright assume that organizations are not willing to spend that much on scrapping every bit of harmful content within their platforms. Nonetheless, moderator tools do not only play a role in avoiding shocking exposure for their audience but are also a vital tool for ad-driven platforms, since, logically, not a company would like to have its brand associated with such content (Stackpole, 2022).

### **Organizational enablers: Unaccountability**

The evidence suggests that most of the organizations that hold the domain of these digital platforms are not and often do not feel accountable for the wrongdoings within their virtual environment. It is not uncommon for corporations to refrain from any kind of social responsibility whatsoever (Trittin-Ulbrich et al., 2021). In fact, some reject the idea that organizations should be responsible for any social harm resulting from digitalization (Grigore et al., 2021). While practically every organization has user’s guidelines that condemns the use of their platforms in harmful ways, activists state that few to none actually commits to their policies and act thoroughly upon it (United Nations, 2023). Quite the contrary, they may even be inadvertently condoning it.

Most of these companies allow inflammatory advertisements to be published in their platforms, such as electoral disinformation, conspiracy theories, and hate speech (United Nations, 2023). Proposedly, environments where such practices are condoned might lead to a sense of legitimacy by the perpetrators, consequently increasing the occurrence of insidious acts within the platform and in the real world. The problem seems to lie not on what the users may post, but rather how the platforms deal with such content (Eisenstat, 2021).

This unaccountability seems not to be something intrinsic to the SMOs, but also somewhat condoned by policymakers. Section 230 of the 1996 Communications Decency Act, known as “the rule that shaped today’s

internet,” states that “no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider” (Brannon & Holmes, 2024, p. 2). Such a statement has indeed shielded the SMOs to be held accountable from countless lawsuits for many years now (Ortutay, 2023).

### Individual enablers: Sense of impunity

It also seems that these digital predators often benefit from impunity. This suggests that most of them are not held accountable for their online wrongdoings. While some prefer a more subtle approach toward their victim, others would outright explicit themselves without any fear of repercussion. Indeed, digital predators are not subject to code or social conventions since their activities are not observable in the real world in which they would otherwise be stigmatized (Bjelajac & Filipovic, 2022). Now in complete anonymity, predators found on the internet almost a risk-free environment. In fact, it is estimated that 85% of online predators are never identified by authorities (SBS Dateline, 2019). Proposedly, this sense of impunity can aggravate the occurrence of insidious acts within digital spaces as social media platforms.

### Individual enablers: Digital naivety

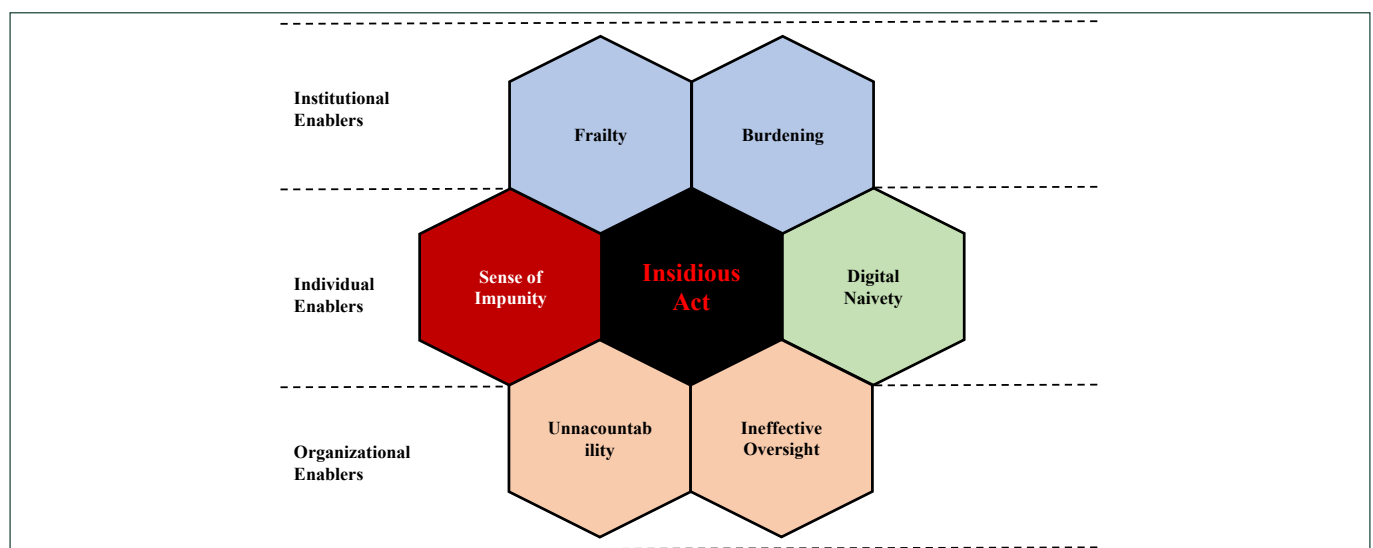
There is an explicit naivety when it comes to the danger that might lurk with social networking of victims and parents alike. Such naivety might derive from a false sense of security, or yet the empowerment that digitalization may bring outside the real world. Girls in particular are the most targeted by digital predators. In fact, digital spaces are now commonplace for adolescents to explore their budding sexuality. In such a digital environment, young girls are more likely to ascend into positions of social authority than boys (Cassell & Cramer,

2008). Proposedly, such a sense of authority could lead to a faint perception of control. Predators would then parsimoniously fuel such perception until they find the victim most vulnerable, as most of them are persistent in building a relationship (Bjelajac, 2020). This could be particularly worrying since the boundaries between the digital and the real world are often blurred, and thus behavior that may be in one domain could be easily consummate in another.

Digital naivety is also related to a dubious sense of digital prowess. Many parents might simply assume that their children, by ‘being born with their heads inside a screen,’ would intrinsically know how to properly behave in such environments. Part of that might come from an ignorance that most of the dangers from the real world may not apply in the digital one. The other side may have to do with the role of authority within a household. As parents are the final voice regarding real-life situations, parents would not dare to interfere in their online lives. This lack of interference may be due to privacy-related concerns, or as aforementioned, just plain ignorance.

## DISCUSSION

Kietzmann et al. (2011) proposed a honeycomb framework to fathom how individuals, organizations, and communities use social media through the illustration of building blocks, which unpacks the core social media functionalities to that end. Instead of particularly using it for the purpose of functionality, the honeycomb framework can also be used to understand and examine different aspects of the dark side of social media (Baccarella et al., 2018). Using the ecosystem lens, Figure 1 illustrates, at the three proposed levels (i.e., institutional, organizational, and individual), the building blocks (i.e., the enablers) surrounding the insidious acts within social media.



Source: Author's elaboration.

**Figure 1.** The building blocks surrounding insidious acts within social media at three levels.

Although we used the context of grooming and predation of minors, we believe that our framework is comprehensive enough to be used in other contexts. What follows is a discussion about what can be done to address these enablers.

### Promoting awareness

Due to these dangers of social media, many parents would outright prohibit the use of it by their children or strictly monitor their every online step. Although some might differ about what may be the best approach depending on one's age, it is the consent of the experts that privacy is indeed essential for adolescents to gain autonomy, self-assuring, independence, and develop responsibility (Witmer, 2022). Restricting online freedom can prove to have a significant backfiring effect, as now social media have a significant role on adolescents' daily lives (Yang, 2016). Is through it that they bond with other individuals outside their families, explore alternative identities, and mature sexually (Cassell & Cramer, 2008). Therefore, education has proven to be the best approach to effectively reduce the chance of unwanted or harmful interaction with strangers (Chan et al., 2016).

A good way is to teach them how to recognize the modus operandi and the personal traits of online predators in order for children to develop self-defense mechanisms against it. Digital predators are very manipulative. They first identify the victims' needs and then proceed to slowly earn their trust with praises, money, video games etc. Once the victim provides their demands, they trap them in a vicious cycle of harassment and intimidation (Bjelajac & Filipovic, 2022). "First and foremost, they look for someone who's vulnerable. They look for someone who's susceptible to being praised or looking to fill some sort of void. And what the strategies generally consist of is flattery, grooming. This grooming will consist of doing a number of things to gain the child's trust; befriend the child; a lot of compliments: 'you're amazing, you're beautiful,' and look to draw this child into where they trust this individual" (an FBI agent).

It is imperative that parents be present in the lives of their children and have an open dialogue channel with them in which they can express their anguish without fear of being judged, but with the expectation of being understood. As for kids and adolescents, they must understand that the usage of social media implies its risks and that they should not discard their parents' concerns. The same approach can also be useful in other contexts such as hate speech, trolling, and many other aspects of cyberbullying that one may suffer or help disseminate (see Quayyum et al., 2021).

### Rethinking social media organizations as we know

There are those who argue that a firmer government intervention through policies is needed. At the very least, Americans are now pressing changes on Section 230 to better portray the current state of social media. If SMOs were to be stripped from such immunity, chances are that they would not take the risk of legal liability from published content and would then proceed to moderate such content more thoroughly, possibly removing it altogether (Ortutay, 2023). If not, there are some who prefer to take a more subtle approach. Instead of disregarding the Section 230 altogether, one way might be to redefine the role of SMOs as not completely unaccountable, but rather see it as a kind of 'digital curator,' whose algorithms decide the fate of the content, and by that demanding transparency (Eisenstat, 2021).

Under the pretext of a safer internet, countries have also started their regulatory moves. Brazil's National Congress is discussing the implementation of a bill (PL 2,630/20), also known as the 'Fake News Bill,' whose proposal is to create measures to combat the dissemination of false content on social networks. In practice, the bill would reduce the SMOs' moderation power in some categories (Tomaz, 2023). The bill, however, did not fall in anyone's favor. The common people, most of all, outright expressed their utter dissatisfaction by naming it as 'PL da Censura' (i.e., Law of Censorship). Censorship is yet a delicate topic amongst Brazil's population, since until recently, the country suffered with dreadful dictatorial periods, with the democratic state as we know today being implemented only in the 80s.

Inevitably, it seems that any attempt to regulate such environments usually falls under the discussion whether or not such measures violate basic rights such as freedom of speech. However, regulation may be not so utterly needed if SMOs started to be more mindful regarding the state of their own business model. The problem may not be the actual self-regulating nature of SMOs, but how their CEOs perceive their platforms as purely profit-centric, and how their profit over the sharing of harmful content. Corporations that shift to a more responsible approach can have a significant increase of their market value, as well as a reduction in systematic risk, staff turnover, and cost of debt (Rochlin et al., 2015).

### Foresting the cooperation between the actors

Many social media companies are already obliged by law to provide cybertips to the local law enforcement in certain places when they find obscene images. The National Center for Missing and Exploited Children



(NCMEC) works with law enforcement to identify children in that kind of material, provided by companies like Google and Yahoo through algorithms detection. Cybertips like these can constitute about 50% of all cases investigated in certain states of USA (PBS NewsHour, 2018). In 2017 alone, Facebook made over 18 million reports to NCMEC (Dupnack, 2021).

Tools such as the Child Protection System, projected to help law enforcement triage child pornography cases online by identifying those who download and share such material, is an optimal example of how the third sector and government agencies can work together to tackle this issue. Developed by the non-profit organization Child Rescue Coalition, it has been now used in more than 95 countries free of charge. Mindful of the potential of its tool, the NGO is now pursuing partnership with the big techs such as Google and Facebook. Many of these consumer-focused companies, however, are still reluctant to adopt technologies like this due to the number of false positives that the tool can present as well as other privacy-related concerns (Solon, 2020).

### The role of artificial intelligence

It seems that the current state of technology does not allow us meaningful changes on how we deal with the proliferation of insidious activities within digital platforms. Regarding content moderation, the use of machine learning tools only goes so far (Uduba et al., 2023). Their usefulness is usually attributed to spam jobs and other previous acknowledged content already in a database. The limitation of machines in such a context is due to linguistic and cultural competencies that can be only attributed to humans (Stackpole, 2022).

The insurgency of artificial intelligence (AI) is now being perceived as a game changer in a myriad of contexts, and against crime is no exception. Incidentally, AI can have its uses for organizations and institutions alike. AI-powered systems can help SMOs through the scalable handling of data in real time and fully automatize the content filtering, all of that by relieving human moderation of exposure to harmful content (Darbinyan, 2022).

Likewise, institutions can make use of AI-powered systems to develop solutions to tackle virtual crimes. New efforts have been made to identify child abuse and grooming behavior in the online environment. The Chat Analysis Triage Tool (CATT) is one of such solutions that through natural language processing technique is capable of analyzing conversations between minors and predators and determine the likelihood of real-word contact (Miller, 2018). Another

AI-powered solution can match the pattern of veins in one's hands to help identify or exclude a person's involvement with child abuse material (VICE, 2022). Proposedly, public-private partnerships are deemed as a promising way for governments to alleviate their institutional burden while bringing more efficiency in the tackling process.

### Know when to reintegrate and to punish

One can pursue the consumption of CSAM for various reasons. In the case of digital predators, it is difficult to pinpoint exactly what are the motivations for one to pursue such intent. However, four are believed to be the main reasons: (1) the sexual interest in prepubescent children (pedophiles) or young adolescents (hebephiles), who use child-pornography images for sexual fantasy; (2) sexual indiscrimination; those that are constantly looking for new and different sexual stimuli; (3) plain curiosity; and (4) for profiting by selling images (Wolak et al., 2005).

Understanding the underlying motivation of such behavior is critical to better provide countermeasures on how to address each particular case. For example, the pedophilia disorder — i.e., “a sexual affinity disorder mostly found in adults who have expressed sexual fantasies and a tendency to enter the sexual relations with children of the same or the opposite sex” (Bjelajac & Filipovic, 2022, p. 1), it is not in fact a common denominator amongst those who use digital spaces to this very end. There are those who are limited to fantasy, but also those who actively pursue real sexual relationships. In fact, it is estimated that about one in two online offenders that only consumed such material actually engaged in sexual abuse at a certain point (Seto et al., 2011). “There is a very strong possibility that those lead to actual physical sexual abuse of children. Like any addiction, you will get to a certain point where you can't get anymore, and you now need to manipulate others to get what you want. And is there where the grooming offensives came in, from grooming you are arranging to meet, and once you arrange to meet, you are pretty much doing so to commit a physical sexual abuse offence” (detective inspector).

However, no one becomes a predator overnight. In fact, it is estimated that for the most convicted abusers, there is a 10-year delay between first fantasizing about children and then actually abusing them, often as a result of pornography consumption (SBS Dateline, 2023). “They are mostly a little or a lot different from what you are imagining (pedophiles). The estimates across the globe are that about 1% of the adult male population are essentially pedophilic in their sex interest. But what we have been seeing online is sig-

nificantly different. Most of the people that we have worked with have journeyed through adult pornography consumption to looking at teenage images, looking at the next age down, to at the next age down. Some realized the shock of what they have done, and will not return” (director of Stop it Now!).

Helplines such as Stop it Now! is a clever way to prevent cases of child abuse not just through the conventional reporting method, but through a confidential hotline for those who are struggling with sexual thoughts and behaviors toward children. This helpline was established in 2002, but it was only in the Covid-19 pandemic that the numbers reached its peak of over 12.000 contacts so far. Right now, Stop it Now! helped prevent several potential cases of child abuse by talking through the issues, helping callers clarify their concerns, exploring any immediate child protection considerations, providing information and support to help callers make sense of their situation, think about next steps and referring to another agency or their own follow-up services among many other approaches (Stop it Now!, n.d.)

Alternatively, predatory behavior toward minors can be a way of profiting for some. The commercial sexual exploitation of children (CSEC) is the sexual exploitation of a child through production and/or sale of child pornography that occurs at least in part for the monetary or nonmonetary benefit of a particular party (Mitchell et al., 2011). In 2022 alone, both the distribution of child sexual abuse material and grooming practices in the online environment has reached a historical peak of 32 million of suspects (Negreiro, 2023), and about 500,000 online predators actively pursuing minors in social media daily (Nikolovska, 2023).

## FINAL REMARKS

Who stands to blame? A purely rhetorical question that does not have by any means to point out a culprit, but rather urge the discussion on what could be the possible enablers of each one of the actors. Through non-participant observation of 32 videos and thousands of comments in the YouTube platform, we ended up unraveling six major enablers – i.e., (1) frailty, (2) burdening, (3) ineffective oversight, (4) unaccountability, (5) sense of impunity, and (6) digital naivety, within organizational, institutional, and individual levels, that when interacting together are the ultimate formula for insidious acts to happen from within digital platform potentially to the real world.

What follows are the main contributions, a research agenda for pertinent future studies, and finally, the study’s limitations.

## Contributions: theoretical, practical, and social

Most studies on ecosystems tend to focus on how competition arouses amongst the actors or how they collaborate to create value. However, this research complements the theory of the digital platforms ecosystem by framing not the ‘good’ side of interaction, but the bad one, and how these interactions could potentially extrapolate the digital space to harmful real-world implications. Following the Kietzmann et al.’s (2011) proposal of a honeycomb-shaped framework, we proposed six building blocks that surround the insidious acts within social media platforms. The proposed framework helps us understand how each of these actors facilitates the occurrence of insidious acts through the enablers. Future studies are encouraged to measure the influence of each enabler on each other and the occurrence of insidious acts through quantitative data. Likewise, we could also benefit from a mix of theoretical lenses that help us shed light on potential behaviors on social media that could lead to insidious outcomes. Lastly, future studies could also assess what behaviors on social media actually lead to insidious real-world implications and what form they take.

This study also brings contributions at a managerial level. We intend to conscientize the SMOs and other tech companies whose attributions are intimately related to third-party activities within digital platforms that they may be unwittingly supporting insidious acts within their own platforms. In that regard, they could benefit from a more socially responsible attitude, bearing the responsibility for what happens within their platforms and seeking a more sustainable monetization model. To that end, SMOs could team up with other organizations in order to provide AI-powered solutions in the fight against the sharing of harmful content. Furthermore, policymakers and government bodies alike could also benefit from public-private corporations in order to mitigate, and hopefully avoid altogether, that insidious acts that originate in virtual spaces come to the real world.

Lastly, this study also offers pertinent social contributions. Discussing something as harmful as child abuse makes it clear the necessity of actions that can somewhat change this reality. The evidence shows us that the problem is contemporary, complex, harmful, and huge in scope. Consequently, by bringing this dark side to light, we can see that we have an ample avenue for social change, one that can only be fostered by all the actors working together. If anything, this study calls for pressing changes in both organizations and institutions to make the virtual environment safer for each of its users.

## Some insights for future research

Digital predation of minors and the sharing of child pornographic is one of many insidious acts that can occur within a digital platform. Interpersonal cyber-crimes such as cyberbullying and cyber abuse (intimate or domestic) are also contexts worthy of attention (Clevenger et al., 2018). In face of these, we are indeed in a dire need of solutions to deal effectively with these enablers. Here, we were concerned with highlighting the most perceived and practical solutions. Besides exploring the aforementioned contexts, future studies are encouraged to 'think outside the box' and thus scrutinize how we can address these problems properly.

More on that, this study also brought the role of AI in all this dark side. Should we surrender ourselves to AI? Such a question is not without critique. There are some who disregard the idea that AI should be the answer for content moderation altogether, since there is not a 'universal value system' that a machine could assimilate; quite on the contrary, our values are not a definitive consensus, but are under constant and legitimate reconsideration, essential and without an end (Gillespie, 2020). Consequently, we would benefit from studies regarding specifically the ethical implications of AI on content moderation in digital platforms. Furthermore, rather than seeing it as a solution, future studies should also be concerned about how AI can empower child grooming behavior and other harmful ends (see Butler, 2023), and what institutional gaps may arise from the indiscriminate use of AI.

Lastly, future studies are encouraged to formulate hypotheses and test these enablers statistically. For instance, they could assess whether they have any correlation or a direct relationship with the occurrence of insidious acts. This also includes the formulation of scales that could help us measure these reliably and bring forth empirical validation. Likewise, the testing of moderation and mediation effects as age, gender, and socioeconomic status is heavily appreciated to further understand what might enhance or explain it. Finally, we suggest that this phenomenon could be analyzed through other theoretical lenses than the digital platform ecosystem.

## Limitations

No research is without limitations. We must highlight the role of bias. The majority of the videos were from channels that had the verification badge attached to it, which helps distinguish official channels from any impersonators. Part of such videos was from huge news channels such as BBC, NBC, and PBC, whose credibility are taken for granted. The other ones were from inde-

pendent creators that do not necessarily follow journalistic standards of integrity, but rather had entertainment purposes. Therefore, there is no way to precisely certify which of the videos may be deceiving, if not only by the research perception and the overall state of the comment section. We also need to point out the triangulation aspect. Although our findings could be backed up with the literature and other secondary sources, ideally, future research studies are encouraged to also triangulate their findings with primary data from interviews with different stakeholders representative of each enabler, such as marketing managers, policymakers, families, organizations and whatnot.

## REFERENCES

- Baccarella, C. V., Wagner, T. F., Kietzmann, J. H., & McCarthy, I. P. (2018). Social media? It's serious! Understanding the dark side of social media. *European Management Journal*, 36(4), 431-438. <https://doi.org/10.1016/j.emj.2018.07.002>
- Bantourakis, M., & Manojlovic, M. (2023). Why data is key to protecting kids online and ensuring the digital future we deserve. <https://www.weforum.org/agenda/2023/03/why-data-is-key-to-safeguarding-children-online-and-ensuring-the-digital-future-we-deserve/#:~:text=Currently%2C%20there%20is%20limited%20understanding,recognize%20and%20report%20online%20abuse>
- Berger, I. (2012). YouTube as a source of data. *The British Psychological Society*, 83. <https://doi.org/10.53841/bpspag.2012.1.83.9>
- Bjelajac, Ž. (2020). Phenomenological and etiological attributes of pedophilia. *Kultura Polisa*, 17(1), 11-28. <https://kpolisa.com/index.php/kp/article/view/253>
- Bjelajac, Ž., & Filipovic, A. M. (2022). Profiling of online pedophiles. *Law Theory & Prac.*, 39, 30. <https://doi.org/10.5937/ptp2204030B>
- Bonina, C., Koskinen, K., Eaton, B., & Gawer, A. (2021). Digital platforms for development: Foundations and research agenda. *Information Systems Journal*, 31(6), 869-902. <https://doi.org/10.1111/isj.12326>
- Brannon, V. C., & Holmes, E. N. (2024). Section 230: An overview. Congressional Research Service. <https://crsreports.congress.gov/product/pdf/R/R46751>
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77-101. <https://doi.org/10.1191/1478088706qp0630a>
- Butler, J. (2023). AI tools could be used by predators to 'automate child grooming'; eSafety commissioner warns. *The Guardian*. <https://www.theguardian.com/technology/2023/may/20/ai-tools-could-be-used-by-predators-to-automate-child-grooming-esafety-commissioner-warns>
- Cassell, J., & Cramer, M. (2008). *High tech or high risk: Moral panics about girls online*. MacArthur Foundation Digital Media and Learning Initiative.
- Chan, E. J., McNiel, D. E., & Binder, R. L. (2016). Sex offenders in the digital age. *Journal of the American Academy of Psychiatry and the Law Online*, 44(3), 368-375. <https://jaapl.org/content/44/3/368>
- Chang, Q., Xing, J., Chang, R., Ip, P., Fong, D. Y. T., Fan, S., Ho, R. T. H., & Yip, P. S. (2021). Online sexual exposure, cyberbullying victimization and suicidal ideation among Hong Kong adolescents: Moderating effects of gender and sexual orientation. *Psychiatry Research Communications*, 1(2), 100003. <https://doi.org/10.1016/j.psycom.2021.100003>
- Clevenger, S. L., Navarro, J. N., & Gilliam, M. (2018). Technology and the endless 'cat and mouse' game: A review of the interpersonal cybervictimization literature. *Sociology Compass*, 12(12), e12639. <https://doi.org/10.1111/soc4.12639>
- Custers, B. (2012). Technology in policing: Experiences, obstacles and police needs. *Computer law & security review*, 28(1), 62-68. <https://doi.org/10.1016/j.clsr.2011.11.009>
- Darbinyan, R. (2022). The growing role of ai in content moderation. *Forbes*. <https://www.forbes.com/sites/forbestechcouncil/2022/06/14/the-growing-role-of-ai-in-content-moderation/?sh=42874c064a17>
- Dekker, R., van den Brink, P., & Meijer, A. (2020). Social media adoption in the police: Barriers and strategies. *Government Information Quarterly*, 37(2), 101441. <https://doi.org/10.1016/j.giq.2019.101441>
- De Reuver, M., Sørensen, C., & Basole, R. C. (2018). The digital platform: A research agenda. *Journal of Information Technology*, 33(2), 124-135. <https://doi.org/10.1057/s41265-016-0033-3>

- Dupnack, J. (2021). *How police catch child porn creeps - and the support available for the victims*. <https://www.fox2detroit.com/news/how-police-catch-child-porn-creeps-and-the-support-available-for-the-victims>
- Elia, G., Margherita, A., & Passiante, G. (2020). Digital entrepreneurship ecosystem: How digital technologies and collective intelligence are reshaping the entrepreneurial process. *Technological forecasting and social change*, 150, 119791. <https://doi.org/10.1016/j.techfore.2019.119791>
- Eisenstat, Y. (2021). *How to hold social media accountable for undermining democracy*. <https://hbr.org/2021/01/how-to-hold-social-media-accountable-for-undermining-democracy>
- Fatih, T., & Bekir, C. (2015). Police use of technology to fight against crime. *European Scientific Journal*, 11(10). <https://www.eujournal.org/index.php/esj/article/view/5426>
- Furman, A. (2022). *Attorneys say products liability is emerging as a key tool in fight to hold social media companies accountable*. <https://www.law.com/legaltechnews/2022/07/14/attorneys-say-products-liability-is-emerging-as-a-key-tool-in-fight-to-hold-social-media-companies-accountable/?slretu m=20230612105127>
- Gawer, A., & Cusumano, M. A. (2014). Industry platforms and ecosystem innovation. *Journal of Product Innovation Management*, 31(3), 417-433. <https://doi.org/10.1111/jpim.12105>
- Gillespie, T. (2020). Content moderation, AI, and the question of scale. *Big Data & Society*, 7(2). <https://doi.org/10.1177/2053951720943234>
- Grigore, G., Molesworth, M., Miles, C., & Glozer, S. (2021). (Un) resolving digital technology paradoxes through the rhetoric of balance. *Organization*, 28(1), 186-207.
- Hayes, A. (2023). *YouTube stats: Everything you need to know in 2023!*. <https://www.wyzowl.com/youtube-stats/#:~:text=There%20are%20at%20least%20800,content%20is%20being%20uploaded%20constantly>
- Hein, A., Schrieck, M., Riasanow, T., Setzke, D. S., Wiesche, M., Böhm, M., & Krcmar, H. (2020). Digital platform ecosystems. *Electronic Markets*, 30, 87-98. <https://doi.org/10.1007/s12525-019-00377-4>
- Hine, C. (2008). *Virtual ethnography: Modes, varieties, affordances*. In N. G. Fielding, R. M. Lee, & G. Blank, *Handbook of Online Research Methods* (pp. 257-270). Sage.
- Internet Watch Foundation. (2023). *IWF Annual Report 2022*. <https://www.iwf.org.uk/about-us/who-we-are/annual-report-2022/>
- Kietzmann, J. H., Hermkens, K., McCarthy, I. P., & Silvestre, B. S. (2011). Social media? Get serious! Understanding the functional building blocks of social media. *Business Horizons*, 54(3), 241-251. <https://doi.org/10.1016/j.bushor.2011.01.005>
- Klemko, R. (2023). Police agencies are desperate to hire. But they say few want the job. *The Washington Post*. <https://www.washingtonpost.com/national-security/2023/05/27/police-vacancies-hiring-recruiting-reform/>
- Koskinen, K., Bonina, C., & Eaton, B. (2019). Digital platforms in the global south: Foundations and research agenda. In *Information and Communication Technologies for Development. Strengthening Southern-Driven Cooperation as a Catalyst for ICT4D: 15th IFIP WG 9.4 International Conference on Social Implications of Computers in Developing Countries*, 15, 319-330.
- Li, W., Badr, Y., & Biennier, F. (2012). Digital ecosystems: Challenges and prospects. In *Proceedings of The International Conference on Management of Emergent Digital EcoSystem*, pp. 117-122. <https://doi.org/10.1145/2457276.2457297>
- Liu, F., & Maitlis, S. (2010). Non-participant observation. In A. J. Mills, E. Wiebe, & G. Durepos (Eds.), *Encyclopedia of Case Study Research*. (pp. 609-611). SAGE.
- Loffhagen, A. (2023). Goodbye Omegle: How the anonymous chatroom traumatized our teen years. *The Guardian*. <https://www.theguardian.com/media/2023/nov/15/omegle-closing-random-video-chat>
- Lopez-Rocha, S. (2010). Netnography in context: Methodological and practical implications of virtual ethnography. *International Journal of Interdisciplinary Social Sciences*, 5(4). <https://doi.org/10.18848/1833-1882/CGP/v05i04/51693>
- Matthews-El, T. (2023). *Product Liability Lawsuit Guide (2023)*. <https://www.forbes.com/advisor/legal/personal-injury/product-liability-lawsuit/#:~:text=Product%20liability%20refers%20to%20responsibility,designed%2C%20manufactured%2C%20or%20marketed>
- Merriam, S. B., & Tisdell, E. J. (2015). *Qualitative research: A guide to design and implementation*. John Wiley & Sons.
- Miller, A. (2018). *Purdue team using artificial intelligence to catch online predators*. <https://www.purdue.edu/dawnordoom/news/News%202018/180810-Online-Predators.html>
- Mitchell, K. J., Jones, L. M., Finkelhor, D., & Wolak, J. (2011). Internet-facilitated commercial sexual exploitation of children: Findings from a nationally representative sample of law enforcement agencies in the United States. *Sexual Abuse*, 23(1), 43-71. <https://doi.org/10.1177/1079063210374347>
- Müller, K., & Schwarz, C. (2021). Fanning the flames of hate: Social media and hate crime. *Journal of the European Economic Association*, 19(4), 2131-2167. <https://doi.org/10.1093/jeea/jvaa045>
- Müller, K., & Schwarz, C. (2023). From hashtag to hate crime: Twitter and antimorality sentiment. *American Economic Journal: Applied Economics*, 15(3), 270-312. <http://doi.org/10.2139/ssrn.3149103>
- Negreiro, M. (2023). Combating child sexual abuse online. *European Parliament*. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/738224/EPRS\\_BRI\(2022\)738224\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/738224/EPRS_BRI(2022)738224_EN.pdf)
- Nikolovska, H. (2023). *Online Predator Statistics [2023 Update]*. <https://screenandreveal.com/online-predators-statistics/>
- Organisation for Economic Co-operation and Development. (2019). *Going digital: Shaping policies, improving lives*. <https://www.oecd.org/digital/going-digital-synthesis-summary.pdf>
- Ortutay, B. (2023). *What you should know about Section 230, the rule that shaped today's internet*. <https://www.pbs.org/newshour/politics/what-you-should-know-about-section-230-the-rule-that-shaped-todays-internet>
- PBS NewsHour. (2018). *How the FBI tracks down child pornography predators*. <https://www.pbs.org/newshour/show/how-the-fbi-tracks-down-child-pornography-predators>
- Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, 30, 100343. <https://doi.org/10.1016/j.ijcci.2021.100343>
- Ratwatte, P., & Mattacola, E. (2021). An exploration of 'fitspiration' content on YouTube and its impacts on consumers. *Journal of Health Psychology*, 26(6), 935-946. <https://doi.org/10.1177/1359105319854168>
- Rochlin, S., Bliss, R., Jordan, S., & Kiser, C. (2015). Defining the competitive and financial advantages of corporate responsibility and sustainability. *IO Sustainability*. <https://www.ywcasandiego.org/wp-content/uploads/Project-ROI-Report-Impact-ROI.pdf>
- Rossotto, C. M., Lal Das, P., Gasol Ramos, E., Clemente Miranda, E., Badran, M. F., Martinez Licetti, M., & Miralles Murciego, G. (2018). Digital platforms: A literature review and policy implications for development. *Competition and Regulation in Network Industries*, 19(1-2), 93-109. <https://doi.org/10.1177/1783591718809485>
- SBS Dateline. (2019, March 17). *Digital Predators | Full Episode | Dateline [Video]*. Youtube. <https://www.youtube.com/watch?v=RnKlo0EjAqc&t=1s>
- SBS Dateline. (2023, July 16). *The UK's fight against child sexual abuse online | SBS Dateline [Video]*. Youtube. <https://www.youtube.com/watch?v=iF75rooxoB0&t=2s>
- Sedera, D., Lokuge, S., Grover, V., Sarker, S., & Sarker, S. (2016). Innovating with enterprise systems and digital platforms: A contingent resource-based theory view. *Information & Management*, 53(3), 366-379. <https://doi.org/10.1016/j.im.2016.01.00>
- Seto, M. C., Karl Hanson, R., & Babchishin, K. M. (2011). Contact sexual offending by men with online sexual offenses. *Sexual Abuse*, 23(1), 124-145. <https://doi.org/10.1177/1079063210369013>
- Solon, O. (2020). *Inside the surveillance software tracking child porn offenders across the globe*. <https://www.nbcnews.com/tech/internet/inside-surveillance-software-tracking-child-porn-offenders-across-globe-n1234019>
- Spradley, J. P. (1980). *Doing participant observation*. In J. P. Spradley (Ed.), *Participant observation* (pp. 53-84). Holt, Rinehart and Winston.
- Stackpole, T. (2022). *Content moderation is terrible by design. A conversation about how to fix the front lines of the internet*. <https://hbr.org/2022/11/content-moderation-is-terrible-by-design>
- Stop it Now. (n.d.). *The stop it now! UK and Ireland helpline*. <https://www.stopitnow.org.uk/helpline/>
- Sui, W., Sui, A., & Rhodes, R. E. (2022). What to watch: Practical considerations and strategies for using YouTube for research. *Digital Health*, 8, 20552076221123707. <https://doi.org/10.1177/20552076221123707>
- Sussan, F., & Acs, Z. J. (2017). The digital entrepreneurial ecosystem. *Small Business Economics*, 49, 55-73. <https://doi.org/10.1007/s11187-017-9867-5>
- Tiwana, A., Konsynski, B., & Bush, A. A. (2010). Research commentary—Platform evolution: Coevolution of platform architecture, governance, and environmental dynamics. *Information Systems Research*, 21(4), 675-687. <https://doi.org/10.1287/isre.1100.0323>
- Tomaz, T. (2023). *Brazilian fake news bill: Strong content moderation accountability but limited hold on platform market power*. *Javnost-The Public*, 30(2), 253-267. <https://doi.org/10.1080/13183222.2023.2201801>
- Trittnit-Ulbrich, H., Scherer, A. G., Munro, I., & Whelan, G. (2021). Exploring the dark and unexpected sides of digitalization: Toward a critical agenda. *Organization*, 28(1), 8-25. <https://doi.org/10.1177/1350508420968184>
- Uduga, S., Maronikolakis, A., & Wisioerek, A. (2023). Ethical scaling for content moderation: Extreme speech and the (in) significance of artificial intelligence. *Big Data & Society*, 10(1). <https://doi.org/10.1177/20539517231172424>
- United Nations. (2023). *Freedom of speech is not freedom to spread racial hatred on social media: UN experts*. <https://www.ohchr.org/en/statements/2023/01/freedom-speech-not-freedom-spread-racial-hatred-social-media-un-experts>

Vice. (2022). Catching Pedophiles Using AI. *VICE Video*. [https://video.vice.com/en\\_uk/video/catching-pedophiles-using-ai/61841b788b2e171ec133e54b7latest=1](https://video.vice.com/en_uk/video/catching-pedophiles-using-ai/61841b788b2e171ec133e54b7latest=1)

Whelan, G. (2019). Born political: A dispositive analysis of Google and copyright. *Business & Society*, 58(1), 42-73. <https://doi.org/10.1177/0007650317717701>

Whelan, G., Moon, J., & Grant, B. (2013). Corporations and citizenship arenas in the age of social media. *Journal of Business Ethics*, 118, 777-790. <https://doi.org/10.1007/s10551-013-1960-3>

Witmer, D. (2022). *Why teens need privacy from their parents*. <https://www.verywellfamily.com/why-does-my-teen-need-privacy-2609615>

Wolak, J., Finkelhor, D., & Mitchell, K. J. (2005). *Child-pornography possessors arrested in internet-related crimes: Findings from the national juvenile online victimization study*. National Center for Missing & Exploited Children. Alexandria, VA.

Yang, L. K. (2016). Protecting youth from dangerous media: Online predators. In R. Levesque (Ed.), *Adolescents, rapid social change, and the law: The transforming nature of protection* (pp. 75-92). Springer. [https://doi.org/10.1007/978-3-319-41535-2\\_4](https://doi.org/10.1007/978-3-319-41535-2_4)

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of information technology*, 30(1), 75-89. <https://doi.org/10.1057/jit.2015.5>

## Authors

**Bruno Luis Avila Freischlag** 

Universidade do Vale do Rio dos Sinos

Av. Dr. Nilo Peçanha, n. 1600, Boa Vista, CEP 91330-002, Porto Alegre, RS, Brazil  
brunoavila98@hotmail.com

**Bruno Anicet Bittencourt** 

Universidade do Vale do Rio dos Sinos

Av. Dr. Nilo Peçanha, n. 1600, Boa Vista, CEP 91330-002, Porto Alegre, RS, Brazil  
banicet@unisisinos.br

## Authors' contributions

**1<sup>st</sup> author:** conceptualization (lead), data curation (lead), formal analysis (lead), investigation (lead), methodology (lead), writing – original draft (lead), writing – review & editing (lead).

**2<sup>nd</sup> author:** conceptualization (supporting), data curation (supporting), formal analysis (supporting), investigation (supporting), methodology (supporting), supervision (lead), validation (supporting), writing – original draft (supporting), writing – review & editing (supporting).