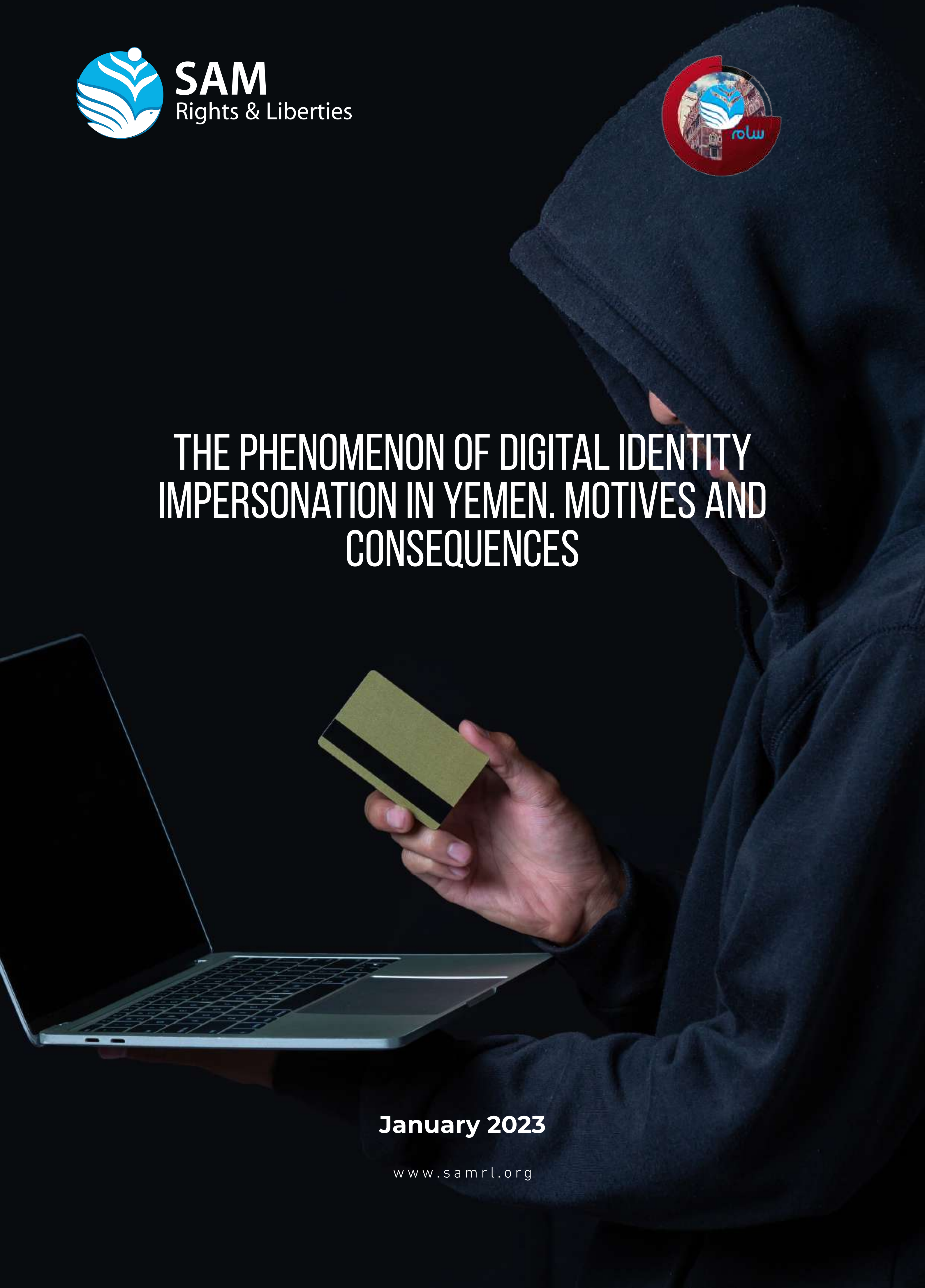
SAM
Rights & Liberties



THE PHENOMENON OF DIGITAL IDENTITY IMPERSONATION IN YEMEN. MOTIVES AND CONSEQUENCES

January 2023

www.samrl.org

THE PHENOMENON OF DIGITAL IDENTITY IMPERSONATION IN YEMEN. MOTIVES AND CONSEQUENCES

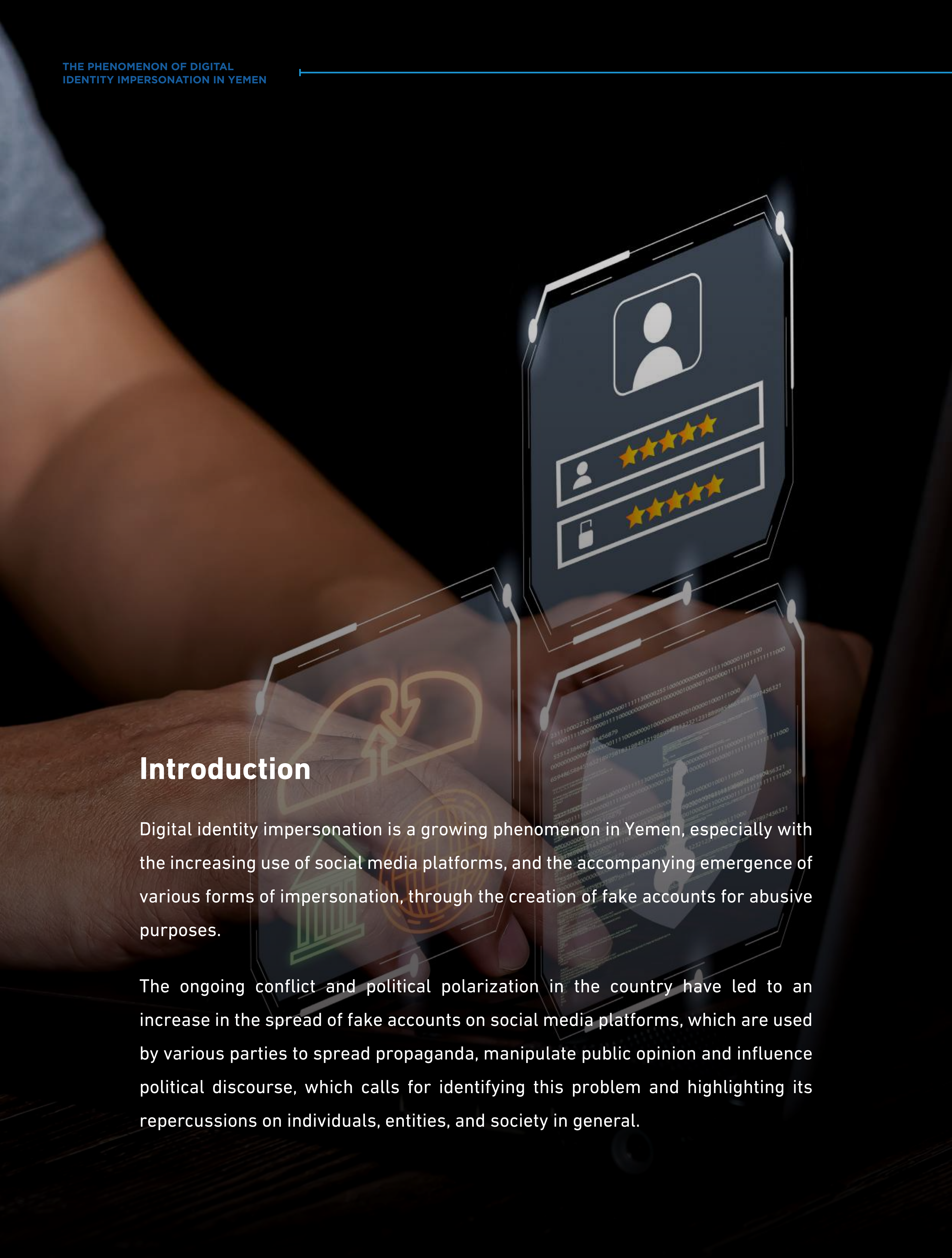
January 2023

SAM
Rights & Liberties

Digital Rights Project

A non-profit human rights window affiliated with SAM Organization, with the support of Internews, aims to introduce digital rights and monitor digital violations against users of the digital space, as it works to advocate for the digital rights of Yemenis, with the aim of reaching a safe, fair and free digital space. The window allows reporting digital violations, documenting them and creating a database about them. She publishes studies and research on digital activism, digital rights and digital security, in addition to planning and managing local and international advocacy campaigns.

violations@samrl.org



Introduction

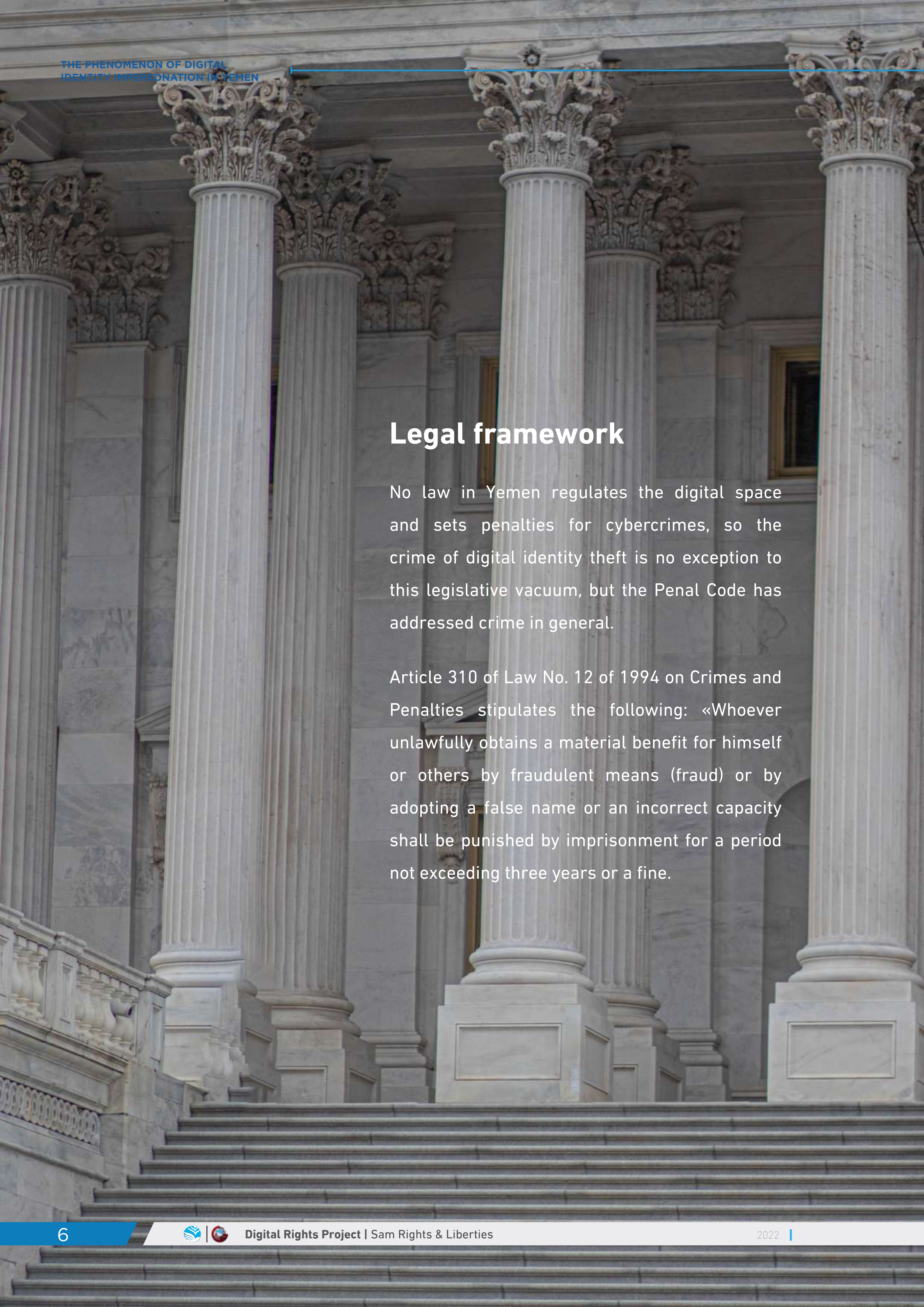
Digital identity impersonation is a growing phenomenon in Yemen, especially with the increasing use of social media platforms, and the accompanying emergence of various forms of impersonation, through the creation of fake accounts for abusive purposes.

The ongoing conflict and political polarization in the country have led to an increase in the spread of fake accounts on social media platforms, which are used by various parties to spread propaganda, manipulate public opinion and influence political discourse, which calls for identifying this problem and highlighting its repercussions on individuals, entities, and society in general.

Conceptual framework

Digital identity impersonation is a form of identity theft to commit fraud or deception where someone pretends to be someone else by assuming that person›s identity, usually to access resources or obtain data, and other benefits in that person›s name and fame, or to use that identity to defame, discredit and damage the impersonator. Cyber Crime Chambers

Impersonating real people on social media falls into a larger category of social engineering, a series of tactics that rely on psychological manipulation and deceiving victims. Bit Defender



Legal framework

No law in Yemen regulates the digital space and sets penalties for cybercrimes, so the crime of digital identity theft is no exception to this legislative vacuum, but the Penal Code has addressed crime in general.

Article 310 of Law No. 12 of 1994 on Crimes and Penalties stipulates the following: «Whoever unlawfully obtains a material benefit for himself or others by fraudulent means (fraud) or by adopting a false name or an incorrect capacity shall be punished by imprisonment for a period not exceeding three years or a fine.

Researcher and legal advisor Abdul Rahman Al-Zabib said that Yemen suffers from weak mechanisms for dealing with cybercrimes, and if cybercrime occurs, it is difficult to prove, investigate and prosecute its perpetrators, due to the lack of an anti-cybercrime law so far, and the lack of harmonization of the national legal system with ratified international conventions. (Adengad - June 2021).

If we take an example of how an Arab country deals with the crime of electronic plagiarism, and other crimes that ensue - to draw inspiration from the experience and benefit from it - We find that the UAE, for example, has defined the penalty, as Article (11) of the Anti-Cybercrime Law stipulates that «Whoever unlawfully seizes for himself or others movable property or benefit or a bond or signs such a bond, using any fraudulent method or by adopting a false name or impersonation, shall be punished by imprisonment for a period of not less than one year and a fine of not less than two hundred and fifty thousand dirhams and not exceeding one million dirhams, or by either of these two penalties. an incorrect description through the computer network, an electronic information system, or one of the means of information technology.»

The general context of the phenomenon

The ongoing conflict and political polarization in Yemen have increased the proliferation of fake accounts on social media platforms, which various parties use to spread propaganda, manipulate public opinion and influence political discourse.

Since 2011, Yemenis› use of social networking sites has escalated significantly, and it has become one of the most important means of mobilization and political polarization in the country, and for this reason organized political factions began to create fake accounts, some of which show their pseudonymous nature through the name of the non-personal account, and some of which are the names of accounts that appear personal and sometimes with personal photos and have a remarkable activity, and with time users discover that it is an account of fake characters. (Al-Madania website - April 2020)

In light of intense polarization and political tug-of-war, «high levels of coordinated fake accounts are being published in Yemen and Iraq – many linked to political or jihadist reasons – that spread disinformation and provoke local violence, often between warring groups.» According to an investigation prepared by journalist «Mark Scott» for the American newspaper «Politico» and published in October 2021.

Although our focus is on fake accounts with malicious intent, there are pseudonymous accounts created without the intention of harming others, according to a report by Yemen Future, «many women, girls, and activists were initially entering social media platforms expressing their opinions freely, but they were recently forced to change their names under pseudonyms, due to harassment, verbal violence and bullying. (Yemen Future - September 2021)

Given that Yemeni society is a closed patriarchal society – with some exceptions – fake nicknames and accounts are rife on Facebook, with some boys and girls creating pseudonyms for fun, to avoid any social restrictions, and others creating fake accounts to trick their friends into thinking they are talking to girls. Al-Monitor - October 2013

Types of plagiarism that are popular in the Yemeni digital space

- Real impersonation

There are thousands of accounts and pages that impersonate politicians, military leaders, social figures, media professionals, journalists, and celebrities, as a prominent example of this type of plagiarism, there are more than 30 pages and accounts, on Facebook, and like them on Twitter, impersonating the President of the Presidential Council, Rashad Al-Elaimy.

- Fake impersonation

There are thousands of fake accounts and pages, pretending to represent real characters, in reality, appearing with familiar names, data, and qualities, For example, Dr. Hussein Al-Yafei, a Twitter account with more than 112,000 followers, describes himself as the head of the Southern National Movement, and claims to be an assistant professor of political science at the University of Aden, often attacks the STC and spreads completely false information, but an in-depth investigation prepared by the Yemeni Sadaq platform, dated October 2021, revealed the falsity of the account, with evidence, and it turned out that it was registered in the name of a media person before it was changed to the current name.

- Impersonation of institutions and entities

Many accounts and pages have been monitored – which cannot be mentioned – that impersonate (ministries and government institutions, organizations operating in Yemen, media and news entities, commercial companies, and private institutions).

- Aliases

Aliases are widely spread on the Yemeni digital space, some of which were created for innocent motives, such as social sensitivity and escape from harassment, but the vast majority of these accounts have bad intentions.

- Theft of personal accounts

In Yemen, it is common for someone›s social media account to be hacked and later the hacker speaks on behalf of the victim, for example in September 2022, three former ministers in the internationally recognized government (Marwan Dammaj, Abdel Raqib Fatah, and Salem Al-

Hurayzi) warned that unknown people are using their old personal accounts on Facebook, after they hacked them years ago, and asking contacts to transfer money, considering that the ministers are requesting financial assistance.

Motives for digital identity impersonation

- Manipulation of public opinion

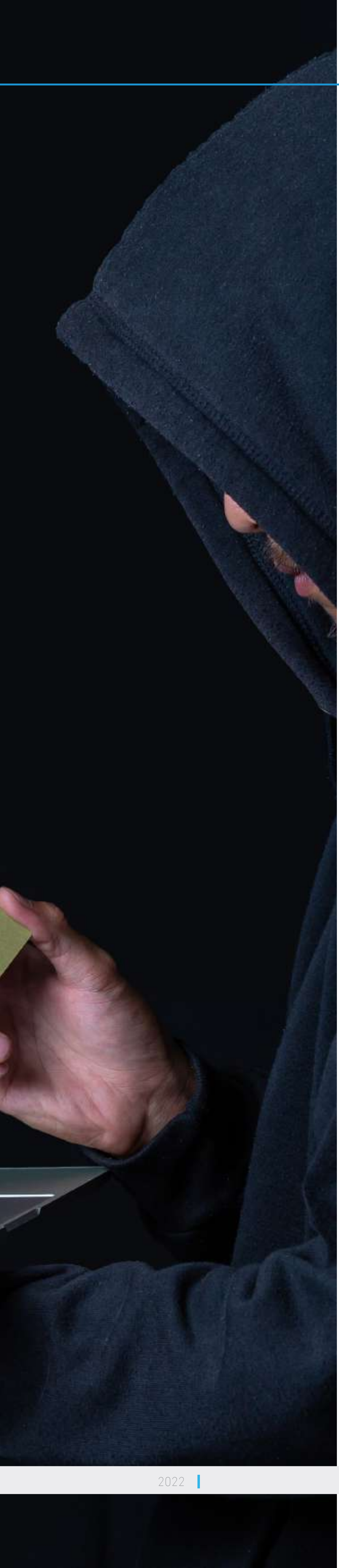
The frequency of targeted use of social networking sites has increased significantly with the events of the Arab Spring since 2011, as members of political groups and parties have become practicing the role of propaganda and counter-propaganda, spreading the scandals of the opposing party and trapping it, in addition to spreading intolerant ideas that sometimes lead to increasing the pace of social division and intellectual and regional alignment, which have negative effects that have begun to reflect on reality. Al-Monitor - October 2013

After a political event, for example, accounts and profiles emerge that impersonate the central figures of that event and fabricate statements and opinions to achieve bad ends.

The parties to the conflict in Yemen use fake accounts on social media to manipulate public opinion to spread biased narratives that amplify certain events and points of view by posing as real people or impersonating opposition parties, to publish information and statements to cause division among those parties.

- Spreading rumors and defamation

Fake accounts on social media platforms are used as a tool to spread rumors and share misinformation, and deliver it to a wide audience of followers, who are trapped by piles of lies, at all levels, not only at the political level.



Perhaps the most prominent example of this motive is that one of the accounts on the Twitter platform, which bore the name «Somaya Al-Khoulani», published information in April 2022 that it said revealed the existence of corruption and exploitation of girls by relief organizations, which was picked up by news sites, without thought, so they retweeted that account intensively, in addition to that social media activists launched a fierce campaign against organizations, against the background of the information published by the aforementioned account, without providing single evidence for its claims, to make it clear Later that the account is completely fake.

- Carry out phishing attacks

Phishing attacks in the Yemeni digital space have increased steadily, as unknown people usually use fake accounts to trap their victims, either by sending malicious links – which are usually accompanied by tempting messages such as getting help from an organization, or financial prizes, internet credit… etc- or recording account access data through fake Facebook pages, created to hack the target's account and obtain his data, or sending messages from fake accounts requesting personal information, or posting links to fake sites, and then blackmailing him with money or fulfilling immoral desires.

For example, funded ads have appeared on social media, to attract the largest number of victims, through fictional offers offered in advertising to job seekers. This process is based on impersonating the names of major companies through fake pages on «Facebook» or «WhatsApp», the advertisement includes the need for these companies for young men and women to work for them, and this is accompanied by a link to fill in the applicant›s data, so the applicants are surprised by a fake link, or «hacker», and thus the blackmail process begins, according to a report issued by Daraj Media (dated December 2021).

- Extortion

Fake accounts on social media are often used to carry out extortion, by contacting the victim and demanding either payment (for not sharing information or personal photos), responding to immoral demands, after the information and images are obtained through hacking or phishing, or creating fake content to blackmail the victim.

As an example of this type of motive, the activist in the protection and security of information, Mukhtar Abdel Moez, revealed in June 2022 that three girls were subjected to blackmail, after they were lured by a Yemeni fraudster who created a fake account on Facebook, and impersonated a Gulf businessman, pointing out that the blackmailer threatened the girls, if they did not respond to his demands and pay a sum of money he will tell their families.

- Practicing financial fraud

Fraudsters hide behind the guise of fake accounts and pages to carry out fraud, by contacting the victim and demanding payment for the provision of a particular service or to access exclusive information and opportunities, and the fraudster may claim to represent a government institution or a legitimate company and request sensitive information.

In July 2022, YouTuber «Ahmed Ghazi» revealed a «financial fraud» targeting Yemeni expatriates in Saudi

Arabia, through dating and marriage applications, and pointed out that individuals fell victim to fake engagements and marriages that were documented with forged marriage contracts, under which they paid sums of money to Yemeni fraudsters, who impersonated girls, noting that professional gangs are behind this fraud.

In mid-January 2023, the Yemeni Sadaq platform said that it had closed - in cooperation with Meta - a group of accounts (33 accounts) on the Facebook platform that carried fake names, mostly posting pictures of veiled women, and publishing the same videos in which poor families appear to solicit people, defraud them, and take money from them.

This is not the first time that the platform has closed accounts of this type after reporting Meta, in June 2020 the platform closed a network of fraudulent accounts that carry several names with the same number and ask for money as assistance to those in need, and exploit an old video of a real medical condition, which he had taken care of in 2017.

In October 2022, activists revealed incidents of financial fraud, which several people were subjected to by a fake Facebook account called «Shatha Al-Mikhlafi» - claiming to be a media and human rights activist residing in America - who robbed the victims of sums of money ranging from 30,000 to 40,000 dollars, to obtain residency in America.

Effects of plagiarism

Max Heinmeier, director of threat tracking at Darktrace (a US-British IT company specializing in cyber defense), says that the threat of fake accounts on social media platforms is real, and it is a big problem, as they can be used for many evil things, including creating spam, carrying out fraud, inciting violence, organizing terrorism or other behavior. (Protocol - May 2020)

There is no doubt that fake accounts on social media contribute significantly to the creation of a hostile environment on the Internet, by spreading hate speech and inciting violence, harassing and bullying others, slandering and defaming them, promoting divisive and polarizing ideologies, not to mention using these accounts to amplify extremist views, all of which makes the online environment toxic and hostile.

Fake accounts also cause severe damage to individuals and entities, at all levels, (psychologically, socially, financially... etc.), for example: «The ease of obtaining a fake character using an email on social networking pages helps blackmailers to continue to hunt their victims and practice all kinds of blackmail, which may lead some to carry out their threats and publish photos of the victim on the fake account on Facebook without revealing their identity or even tracking them.» (Dakkah platform - December 2022).

In this context, activist Mukhtar Abdel Moez warns – in a Facebook post (March 2022) – against being dragged behind fake accounts, and believes that they were created specifically to abuse people, noting that one of the fake accounts caused the imprisonment of more than one activist in Ibb governorate, including journalist Majed Yassin.

These accounts can undermine societal cohesion by spreading misinformation and biasing, creating a crowd of hostile content, fueling tensions and conflicts, and undermining trust between different parties, thereby weakening social ties and exacerbating existing divisions. In addition, the use of fake accounts to manipulate public opinion produces a distorted view of reality, where individuals are exposed to one point of view, and the other visions are absent.

The role of local authorities in combating plagiarism

In general, "the government's role entrusted with implementing the monitoring and control measures that are supposed to be adopted to pursue cybercrime in Yemen is absent, due to the disintegration of the state and the multiplicity of ruling authorities in the country due to the conflict crisis," according to a report published by the Post in October 2022.

In the absence of explicit provisions governing cybercrimes in Yemen, the judge is forced to subject and criminalize acts by the general rules of the criminal law, which certainly fall short of including all aspects of cybercriminal activity, its complexities, and developments, not to mention the lack of experience of the security and judicial system in technical matters," lawyer and human rights activist Mazen Salam told Dakkah (December 2022).

Here, the role of fact-checking platforms in combating fake accounts and overthrowing their creators emerges, and as a model, the Yemeni Sadaq platform tracks these accounts, exposes the parties/people behind them, and in cooperation with Meta, many fake accounts and pages on Facebook are closed.

Activists and specialists also play a prominent role in addressing the phenomenon of plagiarism, such as digital security experts Fahmy Al-Bahith, Mokhtar Abdel Moez, and Ahmed Ghazi. "Al-Bahith says... If I encounter violent content or I am informed of a fake account that practices any kind of violation, I send an email to the specialized team on Facebook to report with an explanation of the reason. But the real problem, according to Engineer Nour Khaled, who works at YUDDIT, one of the organizations also accredited to submit reports, lies in the cultural barrier between a conservative country such as Yemen and the Facebook team that references reports. "We usually have difficulty convincing the team of the specificity of our culture towards the spread of images of women, and we do not find interaction or restriction measures from the team because they consider the image to be non-infringing content," Noor said. (Dakkah platform - December 2022).

The role of social media platforms

From time to time, social media platforms shut down a network of fake accounts and pages for engaging in coordinated inauthentic behavior and impersonating indigenous community figures. For example, in July 2020, Meta removed 69 accounts, 28 pages, 15 Facebook groups, and 10 Instagram accounts in Yemen impersonating government ministries in Saudi Arabia, including the Ministry of Finance and the Ministry of Labor, targeting Yemenis and sharing narratives critical of the Houthis.

In January 2019, Meta removed 783 pages, collections, and accounts for engaging in inauthentic coordinated behavior associated with Iran and conducting multiple sets of activities related to indigenous communities in several countries, including Yemen. Page managers and account owners typically represented themselves as local citizens, using fake accounts.

In July and August 2022, Twitter and Meta, which owns Facebook, removed two overlapping groups of Pentagon-linked accounts, which carried out deception and disinformation campaigns to promote the official US version of important political events and developments in Washington›s interests. The report identified multiple instances of accounts sharing content and displaying coordinated posting patterns on Facebook, Instagram, and Twitter, for example, on September 23, 2021, a Facebook profile using a fake persona and a page on the site called «Here Is Yemen» posted a video with identical comments about alleged mass executions planned by Houthi leaders in Yemen, shared from other fake accounts in just two minutes. (Al Jazeera Net - September 2022)

But this is not enough, as there are huge numbers of fake accounts and pages that share offensive and divisive content, and the platform›s management (Facebook or Twitter) has not taken any action on them, despite the reporting campaigns on those accounts.

One of the weaknesses in Facebook›s response mechanism and its handling of fake accounts and the content it publishes lies in the platform›s reliance on its user community to report such content, and the delay in responding until it reaches a certain level of popularity, while it is easier to use artificial intelligence to monitor text content in real-time. (Edited: Brookings - April 2019)

This strategy is more efficient and cost-effective for social media companies, and it also means that the more attention a fake account gains, the more likely it is to be tagged, for a closer look.

New York Times - December 2020

In addition, «social media channels have very few commercial incentives to get rid of fake accounts, as the entire advertising model is based on the average monthly number of users, especially when these fake accounts generate interaction via likes and clicks and retweets that affect the algorithm of popular content displayed to users.» Forbes - December 2020

Ways to detect fake accounts

Impersonators are getting smarter and they are making tracking fake social media accounts more difficult these days. However, if an account is fake, there is always a mark or a few signs, as every online action leaves a digital fingerprint, and when this fingerprint is not expertly hidden or the perpetrator becomes lagging in covering its traces, social media investigators can track and detect it. (Bosco Legal - October 2022)

By following these steps, you can tell if an account is fake or real:

- Find mutual

Use search engines to check if the person mentioned is on other social networks that use the same name. Check if the profile pictures used are similar, also check if the profile biographies, contact details, and location match, and check if the accounts share similar content, so if you can detect a significant degree of overlap, you›re most likely dealing with a real account. You can also study profile pictures for tips, by using the reverse image search method — a service offered by Google, Bing, and Yandex — to see if the photo used in the profile depicts someone other than the claimant, or if the photo appears elsewhere online. But keep in mind that these are keys, not hard evidence, to measure whether a calculation is correct or not. (DW - July 2022)

- Online behavior

Pay attention to when the social media profile was created. If it was created and remained active for years, it could be real. However, this is not a sure way to measure credibility... Also, study the type of content posted by the account. Also, if someone constantly changes their position, this should be surprising, unless the individual works as a travel blogger or in a similar position. (DW - July 2022)

-Interests

Be aware of and be skeptical of your favorite trolls› issues. They may be more interested in making a mess, but they also show clear preferences on certain issues. (The Conversation - June 2020)

- Also check the following indicators:

- If there are many updates and content posted but few conversations and interactions with friends.
- If you receive a request to transfer money or disclose sensitive information, this is a tactic used by fraudsters.
- If they send a random link, share the same link repeatedly in a short period, or provide misleading information about the destination of the link. (Europol - December 2021).

What should be done?

- For the public:

Fake accounts gain momentum with the help of followers themselves, by interacting with their content, re-posting, and commenting on it, all of which leads to an increase in the rate of accounts reaching a wide audience and gaining new followers, and therefore, the first step to dealing with any fake or suspicious account is to refrain from following or interacting with it in any way, and report it immediately, and be careful not to respond to requests for money transfers sent by anonymous persons, and refrain from revealing any personal information, or clicking on any attached link, under any circumstances. As a follower «You should use social media sparingly, like any addictive toxic substance, and invest in more real-life discussions, listening to real people, real stories and real opinions.» (The Conversation - June 2020)

- For media and press institutions:

The media, journalists, media professionals, and activists should not derive information or news material from fake accounts, or circulate their content, except in the context of alerting, and should play an awareness-raising role in detecting fake accounts and exposing their creators, and informing the public about the tactics and means used by trolls in practicing cybercrime through fake identity impersonation.

- For donor organizations and institutions:

Investing in supporting platforms concerned with «combating cybercrime» and providing them with the necessary capabilities, especially «initiatives» to verify the information and detect disinformation.

- For the parties to the conflict:

The parties to the conflict should not engage in a cyber conflict that lacks ethics and value practices, nor resort to the use of fake accounts to spread their propaganda, enhance their perceptions of the situation, and distort the other party.

- For social media platforms:

Take a proactive approach to detecting and removing fake accounts by implementing automated detection and reporting systems, using human intermediaries to review and remove fake accounts, and taking audit requests seriously and responsibly. In addition to partnering with local «fact-checking» initiatives, working with local organizations to promote awareness of the problem, and providing education and training to users on how to identify and report fake accounts.

- For the authorities:

Work on the issuance of the «Cybercrime Law», provided that the matter is subject to in-depth discussions with various stakeholders so that the provisions of the law are specific, clear, accurate and relevant, and in a way that does not contribute to restricting freedom of opinion and expression or leading to violating the privacy of individuals and harming them, and it is also necessary to push for the establishment of a national center to respond to cyber incidents, and the use of experts and specialists in this field, as well as the rehabilitation and training of judges, investigators and all persons concerned with dealing with cybercrime.

Conclusion

The phenomenon of digital impersonation in Yemen is a growing concern that requires immediate attention from stakeholders, which contributes to mitigating the damage caused by these fraudulent activities, by following the recommended guidelines and taking proactive measures to protect our online presence.

SAM

Rights & Liberties

The phenomenon of digital identity impersonation in Yemen

Digital Rights |

Today, Sunday, the Digital Rights Project issued a report on the phenomenon of digital identity impersonation in Yemen, and its risks and consequences that cast a shadow on individuals and society as a whole.

The report, entitled The phenomenon of digital identity impersonation in Yemen, Motives and consequences – said Digital identity impersonation is a growing phenomenon in Yemen, especially with the increasing use of social media platforms, and the accompanying emergence of various forms of plagiarism, through the creation of fake accounts for abusive purposes.

The report argued that the ongoing conflict and political polarization in the country have led to an increase in the spread of fake accounts on social media platforms, which are used by various parties to spread propaganda, manipulate public opinion, and influence political discourse, which calls for identifying this problem, and highlighting its repercussions on individuals, entities, and society in general.

The report added that the parties to the conflict in Yemen use fake accounts on social media to spread biased narratives, which amplify certain events and points of view, by pretending as real people, or impersonating characters from the opposition parties, to publish information and statements to cause division in the ranks of those parties.

The report (The Phenomenon of Digital Impersonation) considered that fake accounts on social media contribute significantly to the creation of a hostile environment on the Internet, by spreading hate speech and inciting violence, harassing and bullying others, slandering and defaming them, and promoting divisive and polarizing ideologies, not to mention the use of these accounts to amplify extremist views, all of which, makes the Internet environment a toxic and hostile environment.

It pointed out that these accounts undermine societal cohesion, by spreading misleading and tendentious information, creating a crowd of hostile content, in addition to fueling tensions and disputes, and undermining trust between different parties, thus weakening social ties and exacerbating existing divisions. The use of fake accounts to manipulate public opinion also produces a distorted view of reality, where individuals are exposed to one point of view, and different other visions are absent.

On the role of official authorities in addressing the phenomenon of plagiarism, the report pointed to the absence of an official role in combating cybercrime in general, and the lack of procedures supposed to be followed in monitoring and controlling to pursue of criminals, as well as the absence of a law regulating the digital space. In this vacuum, fact-checking platforms and activists have emerged in combating fake accounts and ousting their creators.

The report criticized the role of social platform companies in combating fake accounts, saying that the efforts and procedures they follow to address the phenomenon of plagiarism are not enough, noting that there are huge numbers of fake accounts and pages that share offensive and divisive content, without the management of the platforms - Facebook or Twitter - taking any action about them.

The report explained that one of the weaknesses in Facebook's response mechanism and its handling of fake accounts, and the content it publishes, lies in the platform's reliance on its user community to report such content, and the delay in responding until it reaches a certain level of popularity, while it is easier to use artificial intelligence to monitor text content in real-time.

The report issued by the Digital Rights Project in Yemen added that social media channels have very few commercial incentives to get rid of fake accounts, as the entire advertising model depends on the average number of monthly users, especially when these fake accounts generate interaction via likes and retweets that affect the algorithm of popular content displayed to users.

These days, impersonators are savvier at camouflaging and complicating the task of tracking fake accounts. However, any action on the Internet leaves digital fingerprints that allow social media investigators to track and detect the perpetrator. In addition, some procedures can be followed to find out if an account is fake or real, such as using search engines to check if the said person is on other social networks that use the same name, using the reverse image search method, in addition to observing the person's interests and behavior online, the date the profile was created, etc.

The report advised the public to refrain from following or interacting with fake accounts in any way, and to report them immediately, as a first step to addressing the phenomenon of plagiarism, warning users not to respond to requests for money transfers sent by anonymous persons, disclose personal information, or click on any attached link.

The report called on the media, journalists, media professionals and activists not to circulate the content of fake accounts, and instead to play an awareness role in exposing these accounts and exposing their creators and informing the public of the tactics and means used by trolls in practicing cybercrime through fake impersonation.

The Digital Rights Team also called on donor organizations and institutions to invest in supporting platforms concerned with "combating cybercrime" and providing them with the necessary capabilities, especially "initiatives" to verify the information and detect disinformation.

The authors of the report recommended that the parties to the conflict not engage in an electronic conflict that lacks ethics and value practices, or resort to the use of fake accounts to spread their propaganda, enhance their perceptions of the situation, and distort the other party.

The report stressed the need to work on the issuance of the "Cybercrime Law", provided that the matter is subject to in-depth discussions with various stakeholders, so that the provisions of the law are specific, clear, accurate and relevant, and in a way that does not contribute to restricting freedom of opinion and expression or leading to violating the privacy of individuals and harming them. It also stressed the importance of pushing for the establishment of a national center to respond to cyber incidents, and the use of experts and specialists in this field, as well as the rehabilitation and training of judges, investigators, and all persons concerned with dealing with cybercrime.

The report suggested on social media platforms to take a proactive approach to detect and remove fake accounts by implementing automated detection and reporting systems, using human intermediaries to review and remove fake accounts, and dealing with audit requests seriously and responsibly. In addition to partnering with local "fact-checking" initiatives, working with local organizations to promote awareness of the problem, and providing education and training to users on how to identify and report fake accounts.

It is worth noting that the report (The Phenomenon of Digital Identity Impersonation in Yemen.. Motives and Consequences) is the ninth within the digital rights project, which is implemented by SAM with the support of Internews, with the aim of advocating for digital rights issues for Yemenis, leading to a free and safe digital space.

DIGITAL SECURITY IN YEMEN. REALITY AND THREATS

December 2022

violations@samrl.org
www.dg.samrl.org

Digital.Rights.Yemen
@SamDigitalRight

SAM
Rights & Liberties

www.samrl.org
info@samrl.org