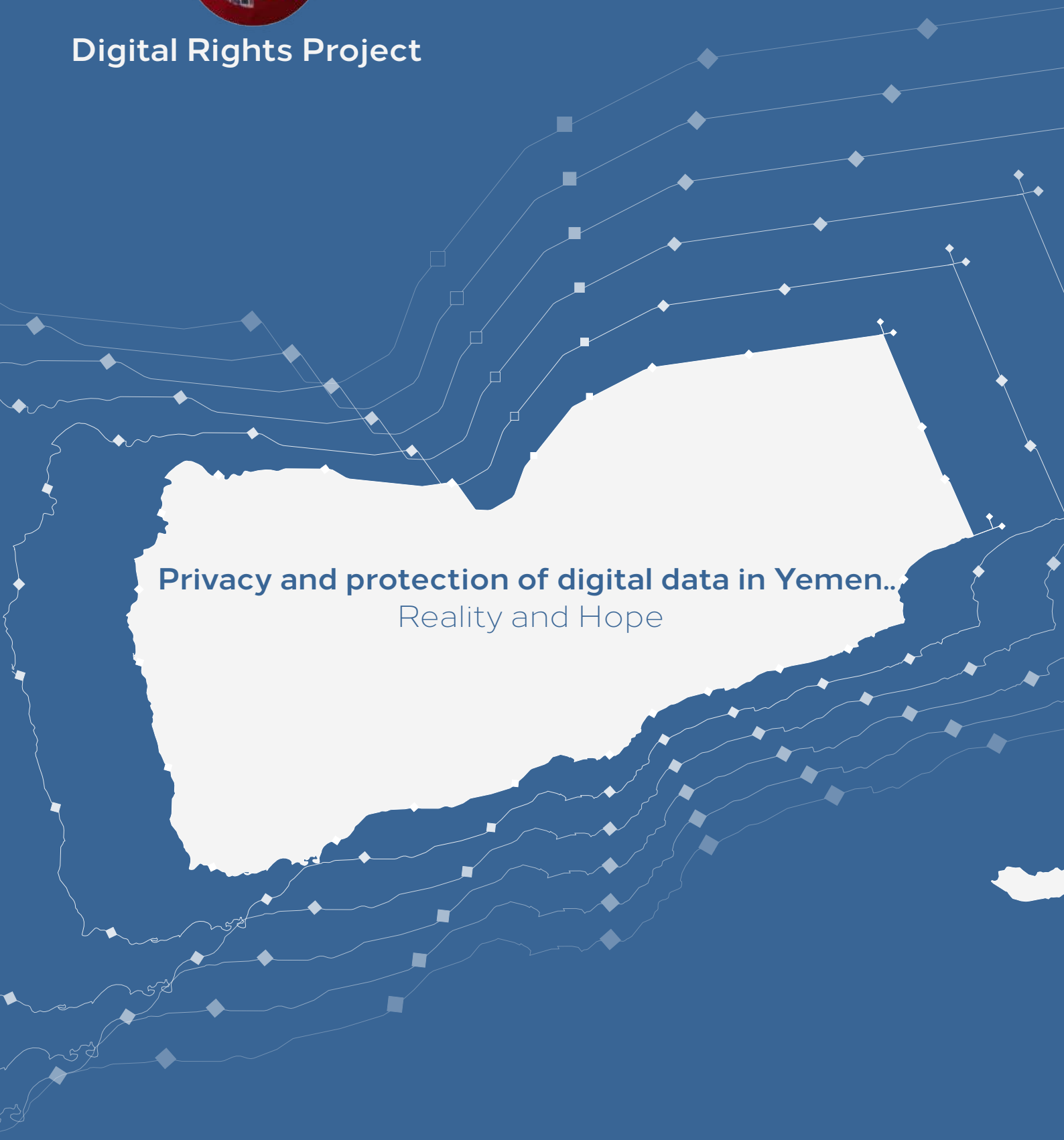
Digital Rights Project

Privacy and protection of digital data in Yemen..
Reality and Hope



https://dg.samrl.org | October 2022


SAM
Rights & Liberties

Digital Rights Project

A non-profit human rights window affiliated with SAM, with the support of Internews, aims to introduce digital rights and monitor digital violations against users of the digital space, where 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 the submission of reports of digital violations, as well as contributing to their documentation and the formation of a database about them. It produces studies and research on digital activism, digital rights and digital security, as well as planning and managing local and internatio-.nal advocacy campaigns

Introduction

With the development of technology and the expansion of the Internet revolution, a state of justified concern has emerged about privacy and digital personal data, as the possibility of storing and sharing data via the Internet, makes it vulnerable to violation, manipulation, and abuse.

The data of Internet users could be compromised, with vulnerabilities in the Internet, as well as the proliferation of smart technologies and software, which facilitate the penetration of the hard wall of privacy and make the presence of individuals in virtual space a risky adventure.

There are many forms of privacy violations in Yemen, from censorship and espionage, through hacking websites and hacking into social media accounts, to malware attacks, and obtaining and disseminating citizens' data without their will, which represents a serious breach of their digital privacy.

"The great risks we face daily online are inextricably linked to the capitalist economic model (digital surveillance economy) in which we live. At the heart of this new form of business model that relies on acquiring, integrating and exploiting very large amounts of personal data to target ads, and manipulating consumer behavior, users are bribed and urged to make their data available at the lowest possible cost to marketers." According to United, the European Anti-Discrimination Network.

The absence of a Yemeni law to protect digital data is one of the causes/-factors of the spread of cybercrime, and the enactment of such a law is the first step towards regulating the turbulent digital landscape and the violations that occur in it that affect digital rights, including the right to privacy.

Conceptual framework

Internet privacy refers to a wide range of technologies, protocols, and concepts related to giving individual users or third parties more privacy protection in their use of the Global Internet. Internet privacy takes many forms, including mandatory privacy statements on websites, data sharing controls, data transparency initiatives and more. Tech Opedia

Digital Privacy

According to Micro Analytics (a company involved in analytics, digital privacy and online security) Digital privacy can be divided into three main categories, (all of which lead to the same path; securing private information from unauthorized access), as follows:

Privacy of communications

It means that individuals have to communicate digitally while their communications and correspondence remain secure and confidential, so that the intended recipient can only access them. Communication privacy is about protecting communications from messages and calls to online meetings.

Privacy of Information

Sharing information without leaking it to unwanted individuals, which is the relationship between how data is collected and disseminated among entities. Information privacy is intended to protect data shared online from malicious access.

Individual privacy

Individual privacy is about ensuring that individual information remains private. This may include health, financial or even location information.

Data Protection

The set of processes and procedures that protect data from damage, exposure or loss. Data protection includes access to data for authorized purposes only, compliance with applicable legal or regulatory requirements, and protected data must be available when needed and can be used for its intended purpose. SNIA

The terms data protection and data privacy are often used interchangeably, but there is an important difference between the two.

Data privacy determines who can access data, while data protection provides tools and policies to effectively restrict access to data. Compliance regulations help ensure that companies implement user privacy requests, and companies have a responsibility to take measures to protect users' private data. Cloudian

Legislative status

Yemen is one of the countries that lacks privacy and data protection law, but, however, there are legal texts that have touched on the subject of privacy and data protection, where articles (15-18) of the Yemeni Telecommunications Law state the following:

15. The right of the public to freely use communications and to ensure their confidentiality is guaranteed in accordance with the Constitution and the law.

16. In case of emergency or other cases specified in the law, the Minister may, after the issuance of permission from the competent judicial authority, monitor conversations and messages through the telecommunication services and communicate their content to the legally authorized authority to request such control.

17. Any control over communications shall be by order issued directly by the Minister or his authorized person to do so.

18. In no case may conversations and communications be monitored without the prior written authorization of the judiciary, in accordance with the provisions of the Code of Criminal Procedure and by the Minister.

In addition, draft Law No. 13 of 2012 on the right to information (not implemented) contains legal provisions on the protection of information and the protection of privacy, (from articles 44 to 57).

Regulatory Policy

Regulatory policy sets out the range of actions authorities take to protect information technology and computer systems, and to manage online risks. The general policies for information security in government agencies (issued by Sana'a Government Resolution No. 59 of 2020) included procedures on the data privacy policy, and the policy of developing and maintaining systems and applications, as follows:

Data Privacy Policy

Employees must not disclose to anyone any information, the nature and location of the information systems nor the control systems used, and privacy must be taken into account when handling personal data.

System Development and Maintenance Policy

There must be a guarantee for any application or testing of information systems, and documents and lists of systems and applications must be properly maintained, while maintaining their integrity. When developing/acquiring any new information systems they must be tested.

Data Usage

The use of real data in use when testing systems is not allowed before special controls are put in place to control the security and integrity of such data and information, and it must be ensured that updates are applied, and the security risks of the systems are assessed.

Privacy Policy of Digital Service Providers

The Privacy Policy sets out the mechanism by which user information is collected, used, shared and the circumstances of its disclosure to third parties. Looking at the privacy policy of digital service providers in Yemen, it is clear how deficient it is, as it is often, brief, and not clearly defined, as well as that some providers do not have a written privacy policy, such as (Yemeni-Omani United Telecommunications YOU) TeleYemen, Y Telecommunications Company, and Aden Net,.

It should be noted that the Privacy Policy does not specify the way in which Yemeni telecommunications companies deal with subscriber data, in communication and Internet services, as much as it specifies the mechanism for collecting information from website users of these companies, and this Privacy Policy is dominated by the omission of the user rights aspect, such as (right to object, right to erasure).

Moreover, the majority of Yemeni websites (governmental, news, commercial... etc) does not have a privacy policy, and if any, it is just mostly copied speech, which means that it collects information about the site's browser in a vague and opaque way.

Information Collected

Personal information, technical information, and information used for advertising purposes, as well as profile information on social networks.

Use of Information

• For the purposes of analyzing, managing and developing the use of the Services, providing technical support, promoting and responding to requests.

Disclosure of Information

• User information may be shared with third parties according to the following circumstances: required by law enforcement authorities, to protect the rights, property and safety of customers or others, for the purposes of promotion, contest or survey.

Transfer and storage of information

• Information may be transferred and stored in a destination outside the framework of the company and its offices, and may be transferred to the subsidiaries of the parent company as well as local and international partners.

Manifestations of privacy infringement

Yemen ranked second among the top 10 countries and regions in terms of the percentage of users attacked by mobile malware, at a severity of 17.97, out of 26 degrees, according to the Kaspersky 2022 report.

The Trojan-Spy.AndroidOS.Agent.aas spyware was the threat that users in the country often faced.

There are many forms of privacy violations in Yemen, from censorship and espionage, through hacking websites and hacking into social media accounts, to malware attacks, and obtaining and disseminating citizens' data without their will, which represents a serious breach of their digital privacy.

Censorship and espionage

An October 2015 report by CitizenLab (a laboratory dedicated to the study of information controls affecting the openness and security of the Internet) stated that external and domestic electronic surveillance is widespread in Yemen, both by and during the current armed conflict. Prior to the conflict, Yemen had a track record of filtering political content, from a variety of categories, including anonymity tools.

Report of the UN Security Council Panel of Experts (January 2021) said that the committee is investigating allegations about the Houthis' use of communications tools to monitor data, messages, texts, and audio and visual traffic involving their opponents. However, Tele-Yemen in Sana'a explained to the committee "Yemeni laws oblige ISPs to filter certain content that contradicts Sharia and Islamic beliefs and that they use it for the purpose of protecting children from any inappropriate content and there is no illegal use.

Website Hacking

The fact that Yemen is a relatively inexperienced country when it comes to internet-related technical operations has contributed to creating a fertile environment for hacking websites, emails, and social media accounts. According to the World Observer Organization for the Information Society (previous source).

Illegal acquisition of personal data

The Yemeni Number Detector app, its policies and service are a flagrant violation of all user privacy and data, according to Adnan Othman, a web developer and digital security researcher, who spoke to Khayout (dated April 2022) saying: "The Yemeni Number Detector not only records usernames, but also stores their emails and other account addresses associated with the name register." Othman asserts that the worst threat is the sharing of name records with third parties, using the app's data search engine, saying: "This silent loophole is actually lagging behind and will have various tragic consequences, including violence, disagreements and inhabited family problems, because many users trust these results holistically, without any doubts."

There is no room to talk at length about what is mentioned in this section, and we will address the topics in some detail in future reports, to complete the bleak picture of the digital scene in Yemen.

Hacking social media accounts

In a report published by the website Post (dated November 2018), the editorial team revealed that the accounts of journalists on Twitter were hacked by parties that turned out to be operating from the capital Sana'a, and practiced hacking several Twitter accounts, mostly of well-known Yemeni journalists, by luring them with electronic tricks, reflecting in their entirety the existence of a network related to the mission of hacking and acquiring those accounts for the interests of those responsible for these operations.

Malware attacks

During the First National Cybersecurity Conference held in Sana'a during June 2021, the head of the information security department at Yemen Mobile, Eng. Ali Al-Wasabi, pointed out that telecommunications companies block hundreds of thousands of messages sent from some phones infected with malware, pointing out that this software works in secret and sends messages or calls without the user's knowledge, and if it succeeds in passing it later requires payment to external providers for these messages.

What's the solution?

The promulgation of the Privacy and Data Protection Act is the first step towards regulating the turbulent digital landscape and the violations that occur in it that affect digital rights, including the right to privacy.

The National Strategic Plan for Cybersecurity, which resulted from the First National Cybersecurity Conference, held in Sana'a during the period (7-9 June) 2021, included the theme of (adoption of individual cyber protection laws), to develop data protection and privacy laws, and to protect children on the Internet, in addition to the development of electronic intellectual property laws, and the adoption of a concept of a digital signature. This plan, with its directives, would be good to implement if it were to be re-discussed and amended in partnership and in agreement with the Ministry of Communications in Aden and other relevant parties.

In this context, Access Now (an international organization working to defend the digital rights of Internet users) proposes 10 recommendations that policymakers should consider when developing data law, as follows:

1 Ensuring transparent and inclusive negotiations

2 Identify and include a list of principles for the protection of personal data that are binding by law

3 Determine the legal basis that allows the processing of data

4 Inclusion of a list of users' rights binding on the law

5 Define a clear scope of application

6 Establish binding and transparent mechanisms for the safe transfer of data to third countries

7 Protection of data security and integrity of data

8. Develop mechanisms to prevent data breach and reporting.

9 Establishment of an independent authority and strong rescue mechanisms

10 Continued protection of data protection and privacy

Telecommunications companies can be guided by the European Union's General Data Protection Regulation (GDPR) (dated April 2016) on the protection of natural persons in relation to the processing of personal data and the freedom to transmit such data.

The Regulation sets out principles to be observed:

• Personal data may only be collected for specific, legitimate and clear purposes.

• The processing of personal data must be legal, fair and transparent.

• The personal data being processed must be appropriate, relevant and not extensive.

• The personal data processed must be accurate and up-to-date if necessary.

• Personal data may not be retained for as long as it is required for the purpose of processing only.

• When processing personal data, you must ensure that it is well protected by taking appropriate security measures.

When it comes to surveillance, civil society needs to do more systematic research to determine how surveillance is conducted. Researchers in Yemen, perhaps in collaboration with donors and international institutes, can work together to track and identify digital surveillance cases and propose solutions. Advocacy groups will be needed to coordinate their actions, hold discussions with various stakeholders, and propose policies to reduce abuse of power, whether by the government or any other party. For this to happen, it will be necessary to engage more closely with international and regional actors in this area and mobilize resources to launch systematic and long-term campaigns and projects that can put the issue of human rights online at the forefront. World Watch Organization for the Information Society - previous source.

In view of the violations and abuses suffered by Internet users that affect their digital rights, it is necessary to establish a body concerned with the rights of users, so that it is the expression of them before the authorities, and the representative of them in any relevant regional/international event or activity.

Privacy and protection of digital data in Yemen..
Reality and Hope

Digital Rights Project

| SamDigitalRight
| violations@samrl.org
| Digital.Rights.Yemen
| https://dg.samrl.org