Rakmana
Journal of Media and Communication Studies

Volume 02 | Issue 03
December 2022
Pages 206 - 000

ISSN-2773-4285
EISSN | 2830-8417
Legal Deposit | 07/2021
Address | 11, Dodo Mokhtar Road, Ben Aknoun, Algiers
Fax | (023) 23 88 50
Phone | (0561) 62 29 75

Received on	11/30/2022
Accepted on	12/14/2022
Published on	12/31/2022

Corresponding author |
Redouane Mokhtari
Algiers 3 University ((Algeria
mokhred@gmail.com

The digital identity management and the Major issues of reputation and privacy :

Impacts on the Algerian Informational System

إدارة الهوية الرقمية والقضايا الرئيسية المتعلقة بالسمعة والخصوصية:

التأثيرات على نظام المعلومات الجزائري

Redouane Mokhtari
Algiers 3 University (Algeria)
mokhred@gmail.com

Abstract

This paper tackles the digital identity , reputation and privacy dilemma, mostly by the awful use of social software, via blogs, wikis and other Web 2.0 software, presenting in the same area cybercrime serious dangers , due to the maximum sectors threats.

Thus, our basic goal meets the modern technologies oversimplification use by upgrading the serviceable informatics system , mainly sensitive ones, as I try to highlight cyber threat extent danger , thanks to the latest most dangerous software , which are punishable by Sharia condemns , law and society because of the threat it perpetrates to the reputation and lives of individuals and business institutions.

Keywords: Digital Identity, Reputation, Privacy , ICT (information and communication technology) , Cybercrime .

ملخص:

تتناول هذه الورقة معضلة الهوية الرقمية والسمعة والخصوصية ، و غالبا من خلال الاستخدام الفظيع للبرامج الاجتماعية ، عبر المدونات والويكي وبرامج Web 2.0 الأخرى ، مما يعرض في نفس المنطقة المجازف الخطيرة للجرائم الإلكترونية ، بسبب تهديداتها القصوى لكافة القطاعات.

وبالتالي ، فإن هدفنا الأساسي يوافق التقنيات الحديثة في التبسيط المفرط من خلال ترقية نظام المعلوماتية الصالحة للخدمة ، وخاصة الأنظمة الحساسة ، حيث أحاول تسليط الضوء على خطر نطاق التهديد السيبراني بفضل أحدث البرامج التي تدينها الشريعة و يعاقب علها القانون والمجتمع لما يمثله من تهديد لسمعة وحياة الأفراد والمؤسسات و الأعمال.

الكلمات المفتاحية: الهوية الرقمية ، السمعة ، الخصوصية ، تكنولوجيا المعلومات والاتصالات، جرائم الإنترنت..

1. Introduction:

The human civilisation is going through the knowledge era, based on I C T's manipulation, that turned this vast world into McLuhan small scary Global village , describing the phenomenon of the entire world becoming more interconnected , as result to the propagation of media technologies throughout the world (Poll, Ryan 2012. p. 160.)

Whereas the twenty-first century statistics shows huge wild flow of information in all fields despite its informatics pillars, conveying large inflation in output , thus the vital call for sharing large information amounts needed to broadcast it often regardless extended spaces. specially as century data indicate human civilisation passage through the knowledge age founded on informatics, transforming the spacious world into an electronic room, despite the awful inflation and huge information flow of humanity intellectual product, regarding its exchange urgent need over long distances .

Just as the Industrial Revolution enhanced threats to national security, and created an environment conducive to street/predatory crime through the concentration of the urban population, the Digital Revolution has created a new forum for both terrorist activity and criminal behavior. The latest technological era has exacerbated the vulnerabilities of government institutions and personal residences alike (Marjie, Britz, 2013, p5)

By these scientific and technological developments pattern, there comes a witnessed duty necessity for official and private ICT bodies, in various scientific activity and academic aspects of interests and those of scientific research, to initiate and formulate immediate development. Policies plans toward the advancing sophisticated new IT systems against the cyber crime riskiest dangers, threatening both national and global information networks.

As a matter of fact and from this basis unifying digital identity reputation and trust resource concepts stands in the context of human agents working with such software and in larger workflow processes. By analysing human agent activity within existing data sets and providing a mechanism for adding new data, it is possible to correlate human agent activities and data creation via a digital identity across disparate sources of data.

1.2 Study issue:

So from this available angle we may now point up the following issue:

What is meant by digital identity, and how to safe its reputation and privacy from the real threats and risks of cybercrimes globally and mainly in Algeria ?

2. digital identity , reputation and privacy concepts :

2.1 digital identity :

A digital identity is the body of information about an individual, organization or electronic device that exists online.Unique identifiers and use patterns make it possible to detect individuals or their devices. This information is often used by website owners and advertisers to identify and track users for personalization and to serve them targeted content and advertising. (techtarget.)

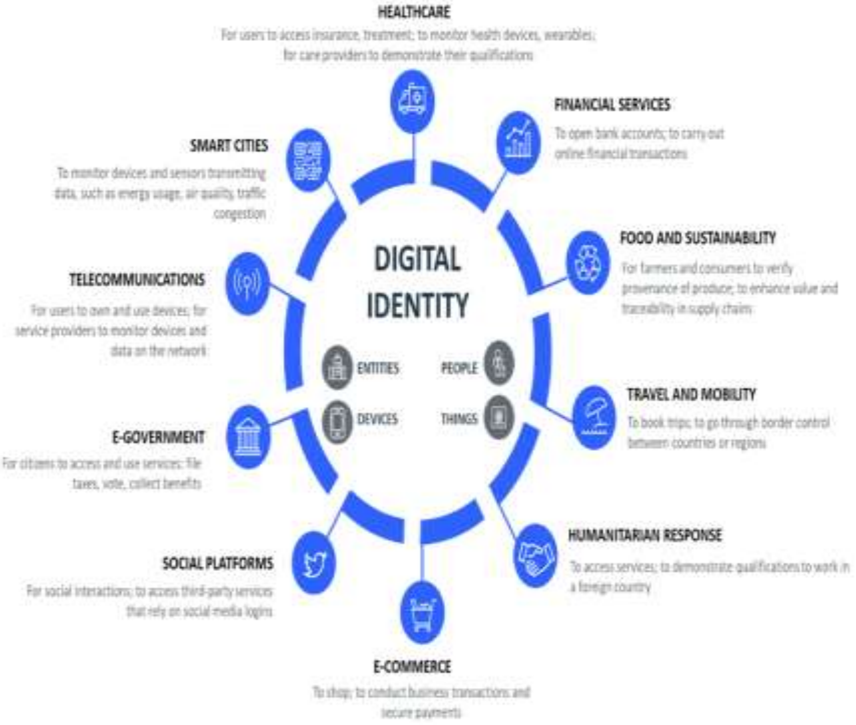
A digital identity is information used by computer systems to represent an external agent – a person, organization, application, or device. Digital identities allow access to services provided with computers to be automated and make it possible for computers to mediate relationships.

A digital identity arises organically from the use of personal information on the web and from the shadow data created by the individual's actions online. A digital identity may be a Pseudonymous profile linked to the device's IP address, for example, or a randomly-generated unique ID. Digital identities are seen as contextual in nature since a user gives selective information when providing authentication information.

The use of digital identities is so widespread that many discussions refer to the entire collection of information generated by a person's online activity as a "digital identity". This includes usernames, passwords, search history, birthdate, social security number, and purchase history,(What is a Digital Identity) especially where that information is publicly available and not anonymized and so can be used by others to discover that person's civil identity. In this broader sense, a digital identity is a facet of a person's social identity and is also referred to as online identity.(Global, IndraStra)

An individual's digital identity is often linked to their civil or national identity and many countries have instituted national digital identity systems that provide digital identities to their citizenry.

Fig.1. Digital Identity Multiple functions


HEALTHCARE
For users to access insurance, treatment; to monitor health devices, wearables; for care providers to demonstrate their qualifications
FINANCIAL SERVICES
To open bank accounts; to carry out online financial transactions
SMART CITIES
To monitor devices and sensors transmitting data, such as energy usage, air quality, traffic congestion
FOOD AND SUSTAINABILITY
For farmers and consumers to verify provenance of produce; to enhance value and traceability in supply chains
TELECOMMUNICATIONS
For users to own and use devices; for service providers to monitor devices and data on the network
DIGITAL IDENTITY
ENTITIES
PEOPLE
DEVICES
THINGS
TRAVEL AND MOBILITY
To book trips; to go through border control between countries or regions
E-GOVERNMENT
For citizens to access and use services: file taxes, vote, collect benefits
HUMANITARIAN RESPONSE
To access services; to demonstrate qualifications to work in a foreign country
SOCIAL PLATFORMS
For social interactions; to access third-party services that rely on social media logins
E-COMMERCE
To shop; to conduct business transactions and secure payments

source : https://www.google.com/search?q=Digital+identity

2.2 Reputation :

Overall quality or character as seen or judged by people in general , or recognition by other people of some characteristic or ability

has the reputation of being clever . a place in public esteem or regard : good name trying to protect his reputation (merriam-webster)

the opinion that people in general have about someone or something, or how much respect or admiration someone or something receives, based on past behaviour or character like saying the company has a worldwide reputation for quality , or she has the reputation of being a good doctor.

His reputation was destroyed when he was caught stealing some money.

The hotel has a bad/good reputation , or he earned / established/ gained /acquired a reputation as an entertaining speaker.(cambridge.org)

Reputation is the subjective qualitative belief a person has regarding a brand, person, company, product, or service.

In today's digital environment, reputation is more important, pervasive, unforgettable, and meaningful than ever. It's surprisingly easy to neglect, abuse, reject, or even intentionally shred someone's reputation. Building, sustaining, and protecting corporate or personal reputations can be difficult. Reputation damage can happen in minutes, doesn't need to be based on fact, and the blast radius of a reputation scandal can circle the globe within hours. (Daniel Threlfall)

Reputation has long been prized. In its traditional form, people who know something about you use this knowledge to form opinions. Their collective sense of who you are—your reputation—affects how people treat you: it shapes all of your social interactions.In today's world, additional knowledge about you resides in "big data" collected by individuals, organizations, companies, and governments. Increasingly, data about you are being processed by algorithms to draw conclusions: to form something like opinions.

This combination of data and algorithms creates a new digital reputation which increasingly shapes your life, from recommending purchases and suggesting friends to prompting actions based solely on your digital footprint.Who gathers, owns, and controls this data? Where do they get it, and how? How do they use it? Is it shared with people, processed by algorithms, used to construct your choices? What should we think about all of this? (Sol Bermann)

2.3 Privacy:

Privacy is an important individual right. However, this does not stand alone: people also have other rights (to shelter, safety and care) and sometimes the exercise of rights on behalf of one person can have negative consequences for another person. Community services departments and agencies, with duty of care and statutory obligations to protect the vulnerable, are constantly seeking to mediate between competing rights and obligations. (Community Services Ministers)

In fact it difined in Webster as : The quality or state of being apart from company or observation : SECLUSION: freedom from unauthorized intrusion one's right to privacy (merriam-webster)

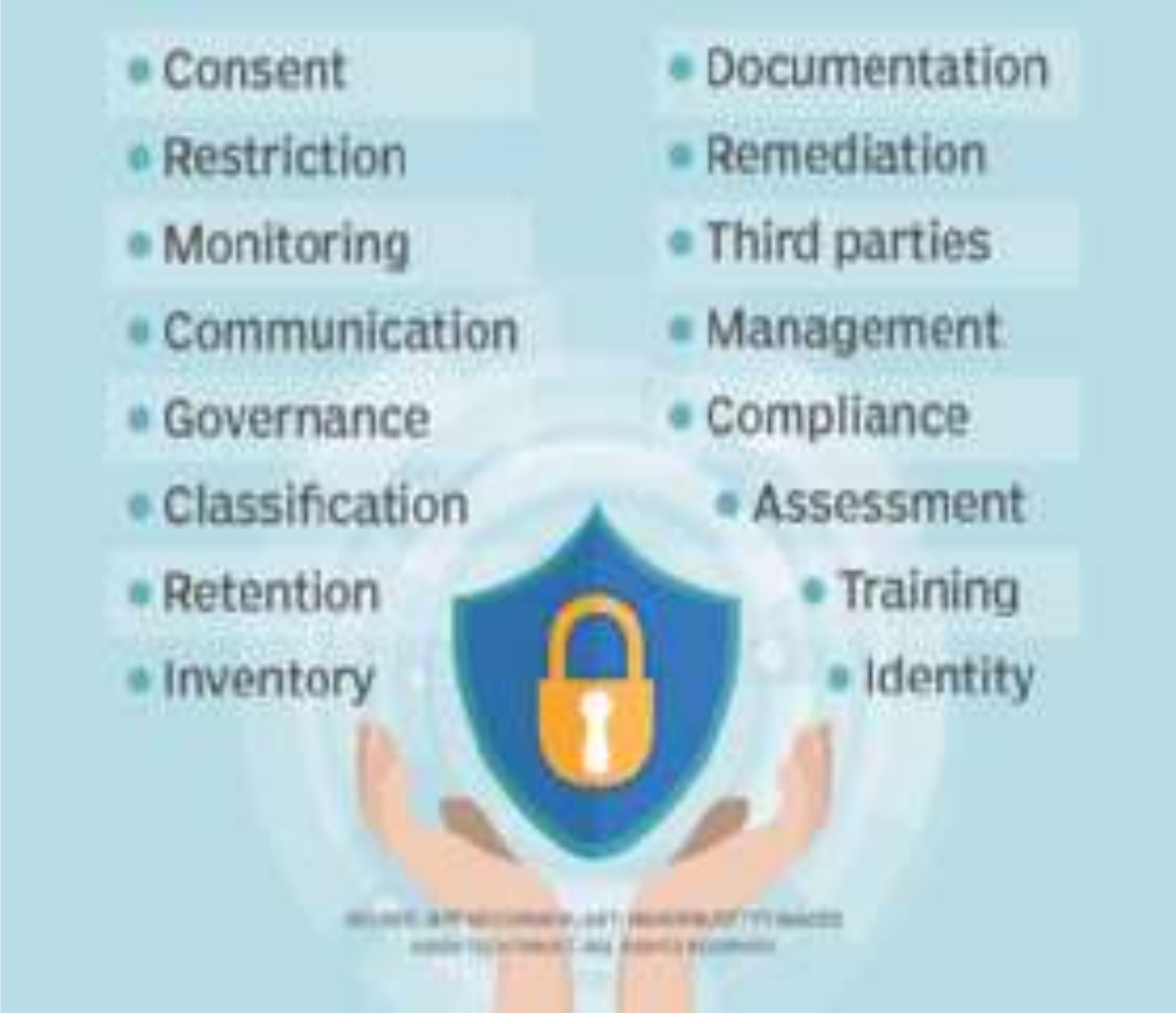
It has been suggested that privacy can be divided into a number of separate, but related, concepts:

- Information privacy, which involves the establishment of rules governing the collection and handling of personal data such as credit information, and medical and government records. It is also known as ‘data protection’;

- Bodily privacy, which concerns the protection of people’s physical selves against invasive procedures such as genetic tests, drug testing and cavity searches;

- Privacy of communications, which covers the security and privacy of mail, telephones, e-mail and other forms of communication; and Territorial privacy, which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space. This includes searches, video surveillance and ID checks.(D Banisar, 2008)

Figure02: **key component to data privacy program**



Source: https://www.google.com/search?q=privacy&tbm=isch&ved=

3 DI and ICTs :

Digital reputations can be curated but are often anchored directly to the social media platform, group, or community upon which they were created. Furthermore, an individual's social media persona and following are not directly portable from one platform to another and can easily be revoked at the discretion of the company running the platform. However, In Web 3, individuals will avoid such issues through direct ownership of a single digital identity that goes wherever they go, both online and in the real world.

3.1 Digital identifiers:

Digital identity requires digital identifiers—strings or tokens that are unique within a given scope (globally or locally within a specific domain, community, directory, application, etc.).Identifiers may be classified as omnidirectional or unidirectional.(Cameron, Kim , 2005). Omnidirectional identifiers are be public and easily discoverable, whereas unidirectional identifiers are intended to be private and used only in the context of a specific identity relationship.

Identifiers may also be classified as resolvable or non-resolvable. Resolvable identifiers, such as a domain name or email address, may be easily dereferenced into the entity they represent, or some current state data providing relevant attributes of that entity. Non-resolvable identifiers, such as a person's real name, or the name of a subject or topic, can be compared for equivalence but are not otherwise machine-understandable.

There are many different schemes and formats for digital identifiers. Uniform Resource Identifier (URI) and the internationalized version Internationalized Resource Identifier (IRI) are the standard for identifiers for websites on the World Wide Web. OpenID and Light-weight Identity are two web authentication protocols that use standard HTTP URIs (often called URLs). A Uniform Resource Name is a persistent, location-independent identifier assigned within the defined namespace.

A . The role of ICTs : ICT has become within a very short time, one of the basic building blocks of modern society , and one of the many challenges facing developing countries today is: preparing their societies and governments for globalization and the information and communication revolution.

ICT is an extensional term for information technology (IT) that stresses the role of unified communications and the integration of telecommunications (telephone lines and wireless signals) and computers (Murray, James 2011) , as well as necessary enterprise software, middleware, storage, and audiovisual systems, that enable users to access, store, transmit, and manipulate information.

When ICT is the target of the offence, cybercrime negatively affects the confidentiality, integrity and/or availability of computer data or systems (UNODC, 2020). Confidentiality, integrity and availability make up what is known as the "CIA Triad" (Rouse, 2014)

The internet is changing. The era of Web 2, dominated by big tech, social media, streaming, and subscription-based service models, is quickly fading away and giving rise to Web 3. Ownership and control of user data in Web 2 rests firmly in the hands of centralized tech companies.

By contrast, Web 3 allows individuals to seamlessly transfer their data and assets over multiple platforms privately, securely, and transparently. Most importantly, it doesn't expose an individual's information and metadata to commoditization unless the individual wishes to provide it, leaving them with complete control. While this self-sovereign approach to individual ownership and control will apply to most forms of personal information, such as financial and medical history, it will also be incredibly pertinent to our future digital reputations.

The Law on Information Security provides the basis for establishing the National Centers for the Prevention of Security will provide valuable support to individuals, government bodies, private sector companies, agencies and others who need to be protected when being online and prevent frauds and other abuses on the Internet.

A must requiring task of high technical competencies and expertise preparation reveals as much as specialized in ICT networks systems ; to secure a solide access to footholds in this technological revolution in applied fields, and provide advanced fast privacy information services to its employees , on the basis of overall quality and electronic form : electronic space imposes a new sophisticated level of practical security system facing the endangering threat of electronic crime .

Therefore once putting simply, private information should stay private, it should not be changed without permission from the owner, data, services and systems should be accessible to the owner at all times. When the ICT is part of the M.O., the cybercrime involves a traditional crime (e.g., fraud and theft) facilitated in some way by the Internet and digital technologies. These categories and the types of cybercrime that fall under them are explored in greater detail in Cybercrime (UNODC, 2020)

Cyber criminals may use computer technology to access personal information, business trade secrets, or use the Internet for exploitive or malicious purposes. Criminals can also use computers for communication and document or data storage. Criminals who are engaged in these illegal activities are often referred to as hackers.

3.2 Digital Identities function:

User metadata and consumer spending information, in the form of verifiable credentials and receipts, can be blind signed for the owner and encrypted within a digital identity and then provided across networks and platforms. Financial transaction data, account balances, digital assets, permissions and social network interactions would all be applicable. The data shared or requested could be customized to specific apps, and all data cryptographically secured so that no third party could access them without permission.

Another more current area in which digital identity and portable reputation could prove the most useful is within Decentralized Autonomous Organizations or DAOs. DAOs allow for cooperation between members in a way that has no central authority. There are a variety of different ways in which DAOs can be structured, but they increasingly require trust.

Having a merit-based reputation is essential in this case. With blockchain-based verified digital identity, it is possible to remain anonymous, but have cryptographic proof of a specific human's verified, merit-based credentials, even without revealing any of their secure personal information.

The digital identity can act as a reputation “scorecard,” which can be updated in real-time, proving what they have contributed or other relevant reputation data.

Perhaps most importantly, this digital identity could use an individual’s biometric data, such as face, fingerprints, or similar. These biometric credentials can be supported with storage of the individual's biometric template in a self-sovereign manner, allowing only the user to access and control them. This would make it impossible for anyone besides the actual owner of the identity to utilize the credentials.

This could then act as a form of universal Verifiable Credentials (VCs) that would be acceptable for any platform to confirm who someone is but wouldn’t give access to any information that an individual elected to restrict. As an individual demonstrates experience, earns certifications, or expands their credentials, this digital identity would instantly reflect that, evolving an online reputation.

In fact, the potential for this type of system goes way beyond just the internet. There is also a vast case for Digital IDs in more traditional offline settings. Most likely, through smartphone integration of a supporting ID wallet, individuals could access workplaces, entertainment venues, festivals, and events with verifiable credentials or NFT tokenized access. This will make security at such locations tighter, as only approved persons will be able to gain entry.

A. Individual Power : The benefits of digital ID to user security are many and will have major implications for combating scams, fraud and money laundering. However, perhaps the biggest boon for the adoption of digital ID adoption is their function in the empowerment of individuals. Centralized Web 2 businesses have had full access and control over user data for too long; Web 3 will change this.

Some have shared concerns about placing such responsibility in the hands of users. At worst, they can lose access to the digital identity; however, even in this instance, the ID would still be secure and unusable by others, Moreover, users could simply create another digital identity as they are the only ones in control of the assets required to recreate it, such as photo IDs and biometrics, which others could not substantiate.

In addition to protection from data mining, digital IDs will also protect people from scammers, hackers and other malicious activity. Data leaks, identity theft, and malware attacks that all too often cause havoc for Web 2 users will be all but eradicated. Even age verification requests can be actioned without having to reveal a person’s age, as the individual’s verified credentials are seamlessly tied to their digital ID through zero-knowledge proofs.

SSIDs and their integration with Web 3 are sure to dramatically impact how we all interact both online and in our day-to-day lives. A person’s reputation will become a form of currency because, unlike most of human history, it won’t be able to be falsified or obscured. This marks the end of the age when big tech companies govern our information and the beginning of an era where individual control over personal data is the standard and making a verified self-sovereign digital identity as the gateway to the internet.(Alastair Johnson)

Similarly, individuals will retain control over visibility and access to their personal information stored within their digital identity — otherwise known as Self-Sovereign Identity (SSI). This personal data can also be provided via homomorphic encryption or to Secure Enclave processing environments, which reap the benefits of contributing the data without disclosing any private user information.

If medical information does need to be shared with a healthcare provider, for example, it can be selectively disclosed or ideally provided as zero-knowledge proofs (ZKPs). Permission can even be time-based so that the data is removed once a predetermined expiry point is reached.Conventional reputation could even involve an individual's credit history or credit score. Credit history can be proven by the individual in the form of verifiable credentials or receipts held by the individual — proving their transaction history and eliminating the need to store it centrally with a third party.

4 Cybercrime threat:

4.1 Cybercrime concept :

The United Nation Office On Drugs And Crime (UNODC) defines cybercrime as an act that violates the law, which is perpetrated using ICT's to either target networks, systems, data, websites technology or facilitate a crime. (UNODC, 2020) thus Cyberbullying, cyber-harassment and cyberstalking that cover a variety of forms of behaviour that display similar features. Sometime the terms are usedinterchangeably and at other times they are distinguished (Gillespie 2016, p. 257).

The Merriam-Webster dictionary defines cybercrime as "criminal activity committed using a computer, especially to illegally access, transmit or manipulate data." But that definition may not cover the full scope of what cybercrime is today.

At its root, cybercrime is any illegal activity using a computer, either as the attacker's weapon or target. That covers a wide variety of types of crime, from phishing emails and identity theft that affect individuals, to ransomware and denial of service (DoS) attacks targeting businesses and organizations. (Mercedes , 2021)

4.2 E- crime : an eminent danger :

Cyber crime, as distinguished from computer crime, is an umbrella term for various crimes committed using the World Wide Web, (it will mentioned next) such as theft of one's personal identity (identity theft) or financial resources,and spread of malicious software code such as computer viruses; use of others' computers to send spam email messages (botnets). Than denial of Service (DoS) attacks on computer networks or websites by the hacker. And activism or attacking computer servers of those organizations felt by the hacker to be unsavory or ethically dubious.

a) Cyber and cyber security threats :

Individuals and businesses can suffer significant financial loss , this's because of cyber crime with the most obvious impact being theft. Loss of business can also be significant in the instance of a denial of service attacks for large corporations. In addition, reputational damage can also be a significant factor following cyber crime.

According to BBC Business News, Talk lost almost a third of their share value following their data breach in 2015. However, it’s important to truly understand this concept into its background “Cybersecurity risks pervade every organization and aren’t always under IT’s direct control. Business leaders are forging ahead with their digital business initiatives, and those leaders are making technology-related risk choices every day. Increased cyber risk is real — but so are the data security solutions.” Gartner explains.

The US government takes cyber threats seriously but appears to be moving too slowly to mitigate them. The White House’s Office of Management and Budget revealed that, of 96 federal agencies it assessed, 74 percent were either “At Risk” or “High Risk” for cyber attacks (Taylor , 2021). They needed immediate security improvements. The government has experienced numerous crippling data breaches in the last few years. Examples include the massive breach of the Federal Office of Personnel Management and the theft of secret US Naval codes. Both attacks have been attributed to Chinese state intelligence agencies.

By now ; cyber attack is a mounted attack , by means of cyberspace which means a virtual space that doesn’t exist, has become the metaphor to help us understand digital weaponry that intends to harm .While many cyber attacks are merely nuisances, some are quite serious, even potentially threatening human lives. It can cause electrical blackouts, failure of military equipment and breaches of national security secrets. They can result in the theft of valuable, sensitive data like medical records. They can disrupt phone and computer networks or paralyze systems, making data unavailable. It may affect the functioning of life as we know it.

b) Types of cyber security threats:

Cyber threats are never static, there are millions being created every year , and most threats follow the standard structures described above. However, they are becoming more and more potent. So far Cyber security threats come in three broad categories of intent, this is why and virtually every cyber threat falls into one of these three modes , so attackers are after the main Financial gain , disruption , espionage (including corporate espionage – the theft of patents or state espionage). (Taylor , 2021)

A new generation of “zero-day” threats are able to surprise defenses because they carry no detectable digital signatures, and another worrisome trend is the continuing “improvement” of what experts call “Advanced Persistent Threats” (APTs). As Business Insider describes APTs, “It’s the best way to define the hackers who burrow into networks and maintain ‘persistence’ a connection that can’t be stopped simply by software updates or rebooting a computer.” A fascinating example when the notorious Sony Pictures hack is an APT, where a nation-state actor lurked inside the company’s network for months, evading detection while exfiltrating enormous amounts of data.

4.3 The divert crashes of cyber crime:

Security Costs: Cyber criminals also focus their attacks on businesses, both large and small. Hackers may attempt to take over company servers to steal information or use the machines for their own purposes, requiring companies to hire staff and update software to keep intruders out. According to E-week, a survey of large companies found an average expenditure of $8.9 million per year on cyber security, with 100 per cent of firms surveyed reporting at least one malware incident in the preceding 12 months and 71 per cent reporting the hijacking of company computers by outsiders. (Mohammad, 2017)

Identity Theft: Becoming the victim of cyber crime can have long-lasting effects on life. One common technique scammers employ is phishing, sending false emails purporting to come from a bank or other financial institution requesting personal information. If one hands over this information, it can allow the criminal to access one's bank and credit accounts, as well as open new accounts and destroy credit rating.

Monetary losses: The overall monetary losses from cyber crime can be immense. According to a 2012 report by Symantec, more than 1.5 million people fall victim to some sort of cyber crime every day, ranging from simple password theft to extensive monetary swindles. With an average loss of $197 per victim, this adds up to more than $110 billion dollars lost to cyber crime worldwide every year(Mohammad, 2017).

As consumers get wise to traditional avenues of attack, cyber criminals have developed new techniques involving mobile devices and social networks to keep their illicit gains flowing.

Piracy: The cyber crime of piracy has had major effects on entertainment, music and software industries. Claims of damages are hard to estimate and even harder to verify, with estimates ranging widely from hundreds of millions to hundreds of billions of dollars per year. In response, copyright holders have lobbied for stricter laws against intellectual property theft, resulting in laws like the Digital Millennium Copyright Act. These laws allow copyright holders to target file sharers and sue them for large sums of money to counteract the financial damage of their activities online.

Social Impacts: Cyber criminals take full advantage of anonymity, secrecy, and interconnectedness provided by the Internet, therefore, attacking the very foundations of our modern information society.

So cyber crime can involve botnets, computer viruses, cyber bullying, cyber stalking, cyber terrorism, cyber pornography, denial of service attacks, hacktivism, identity theft, malware, and spam. Law enforcement officials have struggled to keep pace with cyber criminals, who cost the global economy billions annually.

Police are attempting to use the same tools cyber criminals use to perpetrate crimes in an effort to prevent those crimes and bring the guilty parties to justice. This article begins by defining cyber crime and then moves to a discussion of its economic and social impacts. It continues with detailed excursions into cyber bullying and cyber pornography, two especially representative examples of cyber crime, and concludes with a discussion of ways to curtail the spread of cyber crime.

Computer-related crimes date back to the origins of computing though the greater connectivity between computers through the Internet has brought the concept of cyber crime into public consciousness of our information society. "Billions of dollars in losses have already been discovered. Billions more have gone undetected. Trillions will be stolen, most without detection, by the emerging master criminal of the twenty-first century-the cyberspace offender" (Stephens, 2003)

4.5 Digital protection high measures:

Cybercriminals often use both technical and social approaches to commit crime. Some types of cybercrime are difficult to prevent, however, technology users can take certain actions to protect themselves (to an extent) from cybercrime. (UNDOC, 2020) Consequently each state has its own legal system, which affects the creation of substantive criminal law on cybercrime. These systems include (Maras, 2020)

The Information Society as an action against crime is responsible for media work , comprising standard setting, monitoring and cooperation activities on a wide variety of issues, including freedom of expression, data protection, internet governance, cybercrime, criminal law, fighting economic crime, corruption and money laundering as well as action against drug trafficking and drug abuse. It also promotes transparency and understanding of the functioning of audiovisual industries from a legal and economic point of view (Kleijssen , 2022).

a) **Password Safety :**Big security organizations cannot protect consumers against phishing or hackers who can guess passwords like "1234." Common sense and password hygiene can go a long way to protect consumers from cyber threats. Thus , passwords are a fact of life in today's online world. We use them for everything from sending emails and online banking to ordering the weekly groceries.

The leading security companies , have outlined tips can help make sure your online experiences are kept secure by selecting a password that cannot be easily guessed is the first step toward keeping passwords secure and away from the wrong hands. Strong passwords have eight characters or more and use a combination of letters, numbers and symbols like (e.g., # $ % ! ?).

b) **Identity and businesses theft :** The impact of identity theft and online fraud can be greatly reduced if you can catch it shortly after your data is stolen or when the first use of your information is attempted. One of the easiest ways to get the tip-off that something has gone wrong is by reviewing the monthly statements provided by your bank and credit card companies for anything out of the ordinary.

Many banks also have fraud prevention systems that highlight unusual purchasing behaviour (e.g. if you have attempted to make any purchases abroad). In order to confirm these out of the ordinary purchases are legitimate, your bank might call you to verify them. This can often be the first warning that someone has fraudulently used your account.

Enterprise best practices for defense from cyber defense include basic but extremely important countermeasures like patching systems. When a tech vendor discovers (or is informed of) a security flaw in their product, they typically write code that fixes or "patches" the problem.

c) **Online flirting offers:** Exercise caution when it comes to free software such as screensavers or smileys or special offers. There are a variety of things like 'secret investment tricks' that promise to make you untold fortunes, and competitions that you've 'won' without entering are enticing hooks used by unscrupulous people to try to hook you in.

While it may not directly be paid for the software or service with money, the free software or service you asked for may have been bundled with advertising software ("adware") that tracks your behaviour and displays unwanted advertisements. You may have to divulge personal information or

purchase something else in order to claim your ‘winnings’. Remember, if an offer looks too good to be true, it probably is. If in doubt, ask for someone else's opinion, read the fine print, or simply ignore it.

A host of new technologies and services as well are coming onto the market that make it easier to mount a robust defense against cyber threats. These include:

- Outsourced security service

- Systems that enable collaboration between security team members

- Continual attack simulation tools

- Point solutions for anti-phishing and secure browsing.

Unfortunately, not all victims of internet fraud whether they be businesses or consumers receive justice, but reporting the e-crime helps in many ways. It allows the authorities to keep abreast of the cyber threats and it acts as a mechanism to warn others in order that they can protect themselves. Often those warnings are communicated in the news and result in an increase in e-crime reporting in general.

Based on the “Law on organization and jurisdiction of state authorities to combat cybercrime” the High Public Prosecutor’s Office in Belgrade processes cyber criminal cases in Serbia through a special division to combat cybercrime. It prosecutes the perpetrators of criminal acts targeting computers (ie “every electronic device on the basis of automatic data processing and data exchange”), computer systems, computer networks, computer data, computer programs and copyright works, which can be used in electronic form.

Consequently **e**ach state has its own legal system, which affects the creation of substantive criminal law on cybercrime.

5. Algerian digital informational system:

Up to Paul Bischoff, privacy advocate at Comparitech, in his report findings that it is evidence that, generally, developed countries have better cybersecurity than developing ones , so fare Algeria is the least cyber-secure country in the world. It was the highest-ranking country for lack of legislation and computer malware rates, and It also received a high score in the category for mobile malware and and one of the lowest scores in preparation for cyber attacks (Michael , 2019)

That which looked at 60 countries and included a number of categories, from malware rates to cybersecurity-related legislation, creating rankings for 60 countries, from the least cyber safe to the most cyber safe. It says no single country was found to hold superiority in all categories.

However, the U.S, Japan, France, Canada, and Denmark ranked the best overall for their internet security protocols. The report concludes that in terms of better protections from malware and cyber attacks, and legislation, “Despite some countries having clear strengths and weaknesses, there is definite room for improvement in each and every one.”

The most up-to-date legislation was scored based on existing legislation that covered seven categories (national strategy, military, content, privacy, critical infrastructure, commerce, and crime). According to Global Cyber Strategies Index, Algeria has legislation only on privacy, and it goes back to 2012 . It seems that the study ignores the existence of a 2009 cybercrime law (Michael , 2019) “dealing with special rules related to prevention and the fight against crime related to information technologies and communication.” This law gives the authorities the right to block websites deemed “contrary to the public order or decency.”

5.1 Algerian judicial training on electronic evidence and cybercrime:

The Algerian government, In 2015 , officially created a National Authority for the prevention and combating of infringements related to information and communication technology. It is the Center for the Prevention and Fight Against Computer Crime and Cybercrime (CPLCIC).

According to a decree published in the Official Journal of October 8th, 2015 this new authority was put under the responsibility of the Ministry of Justice. And even it is true that a law specific to cybercrime is still lacking , but the finalization of the text on the fight against cybercrime was yet announced, highlighting the need to “adapt Algerian legislation to developments in the world”

In the past, such laws have always raised the concern of civil society for their restrictive nature. However, the ongoing movement in the country will certainly weigh on the drafting of the new law as eyes will be turned towards the aspects related to the respect of privacy, the freedom of expression and opinion, and the respect of collective freedoms.

Within the framework of CyberSouth projet, and with the support of Algerian Ministry of Justice, the advanced judicial training on cybercrime investigations and electronic evidence was organized in Algiers from 3-6 December 2018 , which was dedicated to the magistrates who successfully completed the initial training session .

The aim of this activity was to provide the participants with the complete knowledge related to cybercrime investigations according to international standards as well as the use of investigative instruments complemented with practical cases. Following this activity, Algerian authorities expressed interest to adapt and implement this training concept for domestic judicial training and the trained magistrates with the support of Council of Europe to be used as future trainers. CyberSouth projet will continue to support the efforts of Algerian authorities to implement the training at the domestic level, under the umbrella of the Judicial Institute(Council of Europe ,2022)

Although the Algerian legislator was corrected for the legal vacuum in the field of cybercrime, By criminalizing the assaults on computer products. However, He did not create a special text, for information fraud. Despite awareness of the Algerian legislator for this type of crime, through a phrase of the amendments, that knew the Algerian Penal Code and the Law of 09/04, Though, that is not sufficient with the newness of this type of crime, which he constantly increasing. As for the sentence of recommendations, they are as follows(Hichem, Wassila, Aziza , 2021):

- The legislator must develop its legislative environment in line with the rapid and remarkable development of this crime.

- Establishing departments specialized in cybercrime. And the conclusion of agreements and treaties for cooperation between countries to combat cyber crime.

- The need to allocate special criminal police and experts with high competence in the field of the Internet.

- The competent authorities should increase awareness campaigns for citizens; for taking to be The precaution and caution of these crimes that are increasing more and more.

- The necessity of training and qualifying members of the judicial police, as well as the Public Prosecution, on how to deal with this type of crime, and to achieve cooperation with technicians with experience. And setting up procedures such as investigation and trial for cybercrime that differ from traditional crime.

- Teaching courses of Information systems and crimes that may arise from she in a simple way in law schools and judicial institutes. (Hichem, Wassila, Aziza , 2021)

6. CONCLUSION :

Digital Identities will Change The Nature Of Online Reputation while cyber crime is indeed getting the recognition it deserves , however, it is not going to restrict that easily , but it is highly likely that cyber crime and its hackers will continue developing and upgrading to stay ahead of the law. And to make us safer we must need cyber security, mainly for the fulfillment of the saiying "Bytes are replacing bullets in the crime world".

As a mtter of fact cyber space offers a plethora of opportunities for cyber criminals either to cause harm to innocent people, then in the pursuing to make a fast buck at the expense of unsuspecting citizens. In the same context we know yet that forensic evidence is important in normal criminal investigations , other than collection and presentation of electronic evidence to prove cyber crimes have posed a challenge to investigation and prosecution agencies and the judiciary.

As a result it should have been needed a good combination of laws and technology in harmony with the laws of other countries and keeping in mind common security standards., and barely in the age of e-governance and e-commerce where a clearly seeable lack of common security standards can create chaos for global trade as well as military matters.

Deliberately we need to be raising digital privacy protection on the global agenda. Trust in the use of our personal data on digital platforms is more than a digital issue; it affects our broader trust in institutions and our society collectively. That is why our governments are calling out this issue with one voice, stating that we will work together in preserving and protecting the use of our citizens' data. (entrepreneur.com)

The DCO will continue to champion the cause of digital privacy by educating consumers, enabling prosperity by sharing best practices, negotiating between governments and the private sector, and shining a spotlight where regulations and terms of service can be improved– including through our social media channels.

Regulations can help to protect against the misuse of individual data, but as individuals, we should all take steps to educate and protect ourselves. Our young people are particularly vulnerable to privacy breaches, since while they are tech savvy, they also tend to be more willing to share personal data. Our elderly, who may be less familiar with digital technologies, are also at risk.

There are several steps we can all take to protect our privacy online, including reviewing privacy settings on applications, creating and refreshing passwords, and taking advantage of additional authentication methods. Although these may seem like trivial steps, they all help in the battle to protect digital privacy. Taking these steps also signals to companies that digital privacy is an important issue that must be protected. For Data Privacy Day, take a moment to think about how you can protect your data in the year ahead.

7. Bibliography List :

1. Books :

Poll, Ryan ,2012, "Afterword". Afterward: The Global Village. Rutgers University Press. p. 160. ISBN 9780813552903. JSTOR j.ctt5hjdkj.13 https://en.wikipedia.org/wiki/Global_village

Marjie T. Britz, Ph.D. Professor of Criminal Justice Clemson University, 2013 ,Computer Forensics and Cyber Crime An Introduction, Boston Columbus Indianapolis New York San Francisco Third Edition

Mohammad Anisur Rahaman , 2017 , Cyber crime affects society in different ways, Published by Syed Manzur Elahi for International Publications Limited from Tropicana Tower (4th floor), 45, Topkhana Road, GPO Box : 2526 Dhaka- 1000 and printed by him from City Publishing House Ltd., 1 RK Mission Road, Dhaka-1000. https://thefinancialexpress.com.bd/views/cyber-crime-affects-society-in-different-ways

Jan Kleijssen , 2022 , Information Society and Action against Crime Directorate, Council of Europe, Avenue de l'Europe F-67075 Strasbourg Cedex, France - Tel. +33 (0)3 88 41 20 00 https://www.coe.int/en/web/human-rights-rule-of-law/information-society-and-action-against-crime-directorate

Gillespie, A,2016,Cybercrime: Key issues and debate.Oxford: Routledge ISBN 978-0-415-71220-0.

Maras, Marie-Helen ,2015 , The Internet of Things: Security and Privacy

Implications. International Data Privacy Law, Vol. 5(2), 99-104.

UNODC,2020, (Draft) Comprehensive Study on Cybercrime.

2. **Journal article :**

Bahi Hichem, Mahi Wassila, Chebri Aziza , 2021 ,Algerian Legislative Mechanisms to Combat Cybercrime and Achieve Information Security , Journal of Rights and Freedoms, Folder09, Number02 2021, p1672-p1687 /https://www.asjp.cerist.dz/en/downArticle/123/9/2/167367

D Banisar, Privacy and Human Rights 2000: An International Survey of Privacy Law and Developments Privacy International <www.privacyinternational.org/survey/phr2000/overview.html> at 5 May 2008.

Steven Furnell , 2003,Cybercrime: Vandalizing the Information Society, Conference: Web Engineering, International Conference, ICWE 2003, Oviedo, Spain, July 14-18, 2003, Proceedings ,University of Nottingham ,https://www.semanticscholar.org/paper/Cybercrime%3A-Vandalizing-the-Information-Society-

Council of Europe ,2022, Cyber South Activities: Advanced judicial training on cybercrime and electronic evidence in Algeria , Council of Europe, Avenue de l'Europe F-67075 Strasbourg Cedex, France - Tel. +33 (0)3 88 41 20 00 https://www.coe.int/en/web/cybercrime/cybersouth-activities/-/asset_publisher/evi3rDpsvYdT/content/cybersouth-advanced-judicial-training-on-cybercrime-and-electronic-evidence-in-algeria?inheritRedirect=false&redirect

Rouse, Margaret ,2014, Confidentiality, integrity and availability (CIA Triad). TechTarget.

Mercedes Cardona, 2021, Types of Cybercrime and How to Protect against Them https://www.mimecast.com/blog/types-of-cybercrime/

Murray, James (2011-12-18). "Cloud network architecture and ICT - Modern Network Architecture". TechTarget =ITKnowledgeExchange. Archived from the original on 2017-09-20.

HUGH TAYLOR , 2021, What Are Cyber Threats and What to Do About Them, https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/

Michael Hill , 2019 , Algeria Ranked ‘Least Cyber-Secure’ Country in the World, Japan ‘Most Cyber-Secure’https://www.infosecurity-magazine.com/news/algeria-ranked-least-cybersecure/

Global, IndraStra. "Digital Identity – A Gateway to All Other Use Cases". IndraStra. ISSN 2381-3652

Community Services Ministers’ Advisory Council, Submission PR 47, 28 July 2006.

Cameron, Kim (May 2005). "The Laws of Identity". msdn.microsoft.com. Microsoft.

3. Internet Websites :

Daniel Threlfall https://blog.reputationx.com/whats-reputation
Sol Bermann https://online.umich.edu/teach-outs/privacy-reputation-and-identity-in-a-digital-age-teach-out/

Alastair Johnson https://www. forbes. com/sites/ alastairjohnson/ 2022/08/30/ digital-identities-will-change-the-nature-of-online-reputation/?sh=20f3739b584a

https://www.techtarget.com/whatis/definition/digital-identity"What is a Digital Identity? - Definition from Techopedia". Retrieved October 1, 2016.

https://www.merriam-webster.com/dictionary/reputation

https://dictionary.cambridge.org/dictionary/english/reputation

https://www.google.com/search?q=Digital+identity