Open Access Library Journal
2024, Volume 11, e10627
ISSN Online: 2333-9721
ISSN Print: 2333-9705

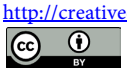
Economic Impact and Ethical Challenge of New Information and Communication Technologies in the Democratic Republic of Congo

Christophe Lwanyi Ashimalu[1], Jean Claude Bukasa Mukengeshayi[2]

[1]Department of Mathematics, Statistics and Computer Science, Faculty of Science and Technology, University of Kinshasa, Kinshasa, Democratic Republic of the Congo
[2]Department of Mathematics, Statistics and Computer Science, Faculty of Science and Technology, Pedagogic University of Kananga, Kananga, Democratic Republic of the Congo
Email: abbechristophelwanyi@yahoo.fr

How to cite this paper: Ashimalu, C.L. and Mukengeshayi, J.C.B. (2024) Economic Impact and Ethical Challenge of New Information and Communication Technologies in the Democratic Republic of Congo. *Open Access Library Journal*, **11**: e10627.
https://doi.org/10.4236/oalib.1110627

Received: August 19, 2023
Accepted: April 27, 2024
Published: April 30, 2024



Abstract

In the Democratic Republic of Congo (DRC) over the last few decades, digital work environments have gradually been set up to enable the various players in social life to work together, access resources, engage in distance learning, archive and trace data, and so on. These environments are set to become increasingly important in the daily lives of citizens, in order to maximize revenue while minimizing expenditure. To boost the DRC's development, the management of the Res Publica must meet the criteria of transparency, traceability and archiving. Our aim, therefore, is not to present a model of sustainable development based on the use of IT tools to combat the systemic and personal economic crimes that have mortgaged the future of the Congolese people, but rather to stigmatize the ethics involved in the use of this modern tool, and to determine the extent to which the integration of these new technologies into the economies of the South can influence ethics. However, in the use of these tools, we need to distinguish between two categories of users: native users and digital [im]migrants. Using survey, interview, documentary and reading techniques, we are going to show how the transparency of actions, the traceability of operations and their archiving constitute the milestones of sustainable development for the Democratic Republic of Congo. To achieve this, a great deal of work needs to be done upstream: boosting the citizen's mindset, making the IT infrastructure available, and training citizens in the use of this IT tool.

Subject Areas

Computer and Network Security

Keywords

Transparency, Traceability, Archiving, Ethics, Digital Natives and [Im]Migrants, Greater South

1. Introduction

Faced with dying democracies, crumbling administrations, deteriorating governance, growing mistrust among citizens and power losing its meaning, governments are seeking to take advantage of both digital technology and Machine Learning to propose new avenues for a governance project endowed with new legitimacies and new efficiency tools that promote a different culture of public service, general interest and management of the public good.

According to Christophe Stener, "Over the past 30 years, the phenomenal development of communication technologies has brought about a veritable revolution in every aspect of our economic, social and political lives, and even in the way we live. This movement has been accompanied by a gradual adaptation of the rights of the molecular world to the specificities of the binary world. The phenomenon has accelerated with the inescapable nature of electronic communications and the wealth of data that networks make available to us. We have thus moved from digital law to digital law and from human rights to digital human rights" ([1], p. 35).

As Congolese citizen-researchers with a passion for the proper use of reason, we cannot help but suggest a few possible solutions to improve the living conditions of our compatriots. This article looks at the question of how to make the best use of information and communication technologies to make the management of the res publica more profitable, while taking account of customs and traditions.

2. Digital Revolution and New Social and Cultural Practices

In the Democratic Republic of Congo, digital technologies are still in their infancy. There are several reasons for this. Lack of IT infrastructure, lack and/or regular power cuts, instability and/or lack of political will? Often paralyse digital technology initiatives.

The digital revolution (also known as the third industrial revolution) [1]-[6] is the shift from analogue mechanical and electronic technology to digital electronics that began in the second half of the twentieth century, with the adoption and proliferation of digital computers and digital archiving, and continues to the present day. Implicitly, the term also refers to the radical changes brought about by digital computing and communications technologies during this period. By analogy with the agricultural revolution and the industrial revolution, the digital revolution marked the beginning of the information age.

Many will agree with us that there is something very fascinating about tech-

nological evolution. Its advances continue to amaze. Older people remember the first voice emanating from a radio or the first image transmitted by a television set. Even today, we are still amazed when we simply point a smartphone at the sky to discover not only where the plane that flies over our heads has taken off from, but also its route, its scheduled landing time and the speed at which it is heading for the city where it will drop off the hundred or so passengers on board.

In fact, the digital revolution is an extremely rapid technical development that has been going from strength to strength since the second half of the twentieth century. Comparable to the industrial revolution, it is directly associated with the birth and development of information technology. By relying on ever more efficient means of communication, information technology has contributed to the emergence of a sprawling global network that continues to expand through new media.

The entertainment and leisure culture popularized by the internet is helping to delegitimize and marginalize classical culture. Such is the case with the Tik Tok application on social networks, which sometimes conveys messages that are unsuitable for young people. Over and above the debate on the quality of mass-consumed contemporary works such as TV series, Rémy Rieffer points to a factor that is often overlooked: cultural consumption for pleasure. According to the author, "The pleasure of the soap opera does not mean complete adherence to its content, but it does allow the viewer to give meaning to his or her own life. Watching it is a moment of relaxation and entertainment, an essential breathing space in today's rhythm of life" ([7], p. 16). What we all have in common with our use of the internet is that it combines knowledge and pleasure, allowing users to inform themselves, to learn and to improve: to fulfil themselves, in short.

The author explains that digital practices "are more deeply rooted in an economic and cultural context, in individual and social trajectories, in representations that strongly dominate investment in new technologies" ([7], p. 75). Finally, he points out that young people have adopted digital technologies more quickly and with greater dexterity. Thus, "the new digital technologies finally appear to be the medium of a youth culture based on a very marked expressive mode: we tell ourselves stories, we have fun, we wander, we project ourselves" ([7], p. 111).

The last sentence of the book is symptomatic. Rieffel states that "neither God nor the devil, digital technology is simultaneously a force for emancipation and domination; in any case, it remains a promise and a challenge today" ([7], p. 269).

Our ways of living and consuming are being profoundly transformed by the rapid development of the Internet and digital technology because of the very nature of this all-purpose medium, which allows us to access works, the products of the cultural industries and radio and television programs, to broadcast and share our own images, texts and music, to communicate orally or in writing, and to perform some of the most trivial tasks of everyday life.

All in all, it begs the question. Has culture gone virtual? Not entirely. Confinement has certainly accentuated a trend, further entrenching ways of seeing and listening via interposed screens. The world of culture has also found it a way of maintaining links with its audiences. But in the end, it is hybrid practices, halfway between the real and the virtual, that seem set to continue.

The extremely rapid spread of computers and the Internet in the home, which is clearly the most significant phenomenon of the last decade, should not be seen in isolation from the general trend towards increasing the number of domestic audiovisual equipment available since the early 1960s.

Indeed, many other things have changed in recent years in the audiovisual field: conditions for receiving television programs have improved, while the range of programs on offer has diversified considerably, with the success of flat screens and home cinema, which almost one household in five now owns; DVD players and burners have almost completely replaced video recorders, and games consoles have conquered new homes.

MP3 players have multiplied the number of ways in which people can listen to music, further amplifying the shockwaves of the music boom triggered more than thirty years ago by the arrival of the hi-fi system and the portable music player. And if we add the spectacular success of multi-function mobile phones, we can see the full extent of the considerable expansion in the possibilities for consuming, storing and exchanging music, images and texts that we have witnessed since the end of the 90s, both in the private space of the home and elsewhere, given the often nomadic nature of the most recent devices.

In a nutshell, the conditions of access to art and culture have changed radically as a result of the combined effects of considerable progress in household equipment, the dematerialization of content and the widespread availability of broadband internet: in less than ten years, fixed devices dedicated to a specific function (listening to records, watching television programs, reading information, communicating with a third party, etc.) have been largely supplanted or supplemented by devices, most often nomadic, offering a wide range of functions at the crossroads of culture, entertainment and interpersonal communication.

This development has firmly established screens as the preferred medium for our relationship with culture, while accentuating the porosity between culture, entertainment and communication. With digital technology and the versatility of the terminals now available, most cultural practices are converging towards screens: viewing images and listening to music, of course, but also reading texts or practicing as an amateur, not to mention the now commonplace presence of screens in libraries, exhibition venues and even some live performance venues… Everything is now potentially viewable on a screen and accessible via the Internet. It's the birth of a new culture based on information technology.

3. Use as Evidence

How did we get here so quickly? Such a universal and precipitous development

seems to defy logic.

Basically, then, computing is based on numbers historically, moreover, the first computers were simple calculating machines. In a way, this phenomenon dates back to antiquity, when humans began to design abacuses and abacuses.

To understand how its development gave rise to the emergence of a global village, it is interesting not only to look at its technical evolution, but also to highlight a few key stages in the construction of a communications network that today links almost the entire inhabited world. Far from listing all the stages between the computer and the abacus, let's take a general look at the major developments in computing and the way it has taken over our world.

In the seventeenth century, two events stood out: the invention of the Pascaline and the institutionalization of the spirit of telecommunications. Influenced by the hypothesis that thought could be formulated systematically using a mathematical language [8], Blaise Pascal developed the first calculating machine that could process an algorithm, a fundamental principle of computer science. At the same time, Henri IV had a corps of couriers set up to transport administrative and private correspondence. In 1612, a stagecoach service was set up to transport mail, parcels and travelers. The post office was born, and with it the first outline of a network that would continue to grow.

In the 18th century, with the aim of automating the operation of weaving looms, the Frenchman Jean-Baptiste Falcon invented the punched card system, a rigid piece of paper containing information represented by the presence or absence of a hole in a given position. This marked the emergence of what would become the core of computing: the binary system. The Enlightenment also saw the birth of the Encyclopedia, whose aim of promoting universalism prefigured, in a way, the notions of networks and the global village. A century later, the railway network would further refine this prefiguration.

The 19th century saw the birth of the analytical machine designed by the English mathematician Charles Babbage. The forerunner of the computer, this steam-powered device combined Pascal's calculating machine with Falcon's system of punch cards for weaving looms. The century was also marked by decisive inventions in the field of telecommunications.

In 1844, Samuel Morse gave the first public demonstration of the telegraph, sending a message over a distance of 60 kilometers between Philadelphia and Washington. In 1858, the first transatlantic cable was laid between the United States and Europe. In 1876, the American Graham Bell invented the telephone. Electricity, for its part, was better mastered. The end of the century saw the birth of the cathode ray tube, which was used for the first television screens and then for computers, until the invention of the flat screen.

At the beginning of the 20th century, electricity was used in industry, public lighting, on the railways and in the home. In 1906, voice was recorded for the first time on the radio waves and, in 1926, the Scotsman John Logie Baird made the first live public television broadcast.

The thirties and forties marked a decisive turning point. In 1930, the Englishman Fredrik Bull created the first company to develop and market mechanographic equipment using the principle of punched cards. Nazi Germany took a keen interest in this process. In 1941, in Berlin, the engineer Konrad Zuse developed the Z3 electromechanical calculator, the first fully automatic programmable machine.

It was in the United States, however, that the digital revolution really began. In the space of three years, from 1945 to 1948, three technological feats marked the beginning of American hegemony in terms of technical progress. During this period, the engineer Vannevar Bush designed a mechanical storage machine that stored microfilm. In 1946, within the walls of the University of Pennsylvania, ENIAC became the world's first computer. Finally, in 1948, the transistor paved the way for the miniaturization of components.

From then on, everything happened very quickly. In 1958 Jack Kilby invented the integrated circuit, a component capable of performing several complex functions on a tiny silicon substrate. That same year, the Bell telephone company developed the modem, a device for transmitting binary data over a telephone line, the Internet was just beginning to appear.

In 1961, Leonard Kleinrock developed a technology to speed up the transfer of this data. Thanks to his research, the Arpanet project was born in 1969. Set up in the context of the Cold War, this network, which was to become the Internet, initially had a military purpose. The aim was to create a decentralized telecommunications network capable of operating despite line outages. In 1971, twenty-three computers were connected to Arpanet and the first email was sent.

In 1977, the Apple II was one of the first mass-produced personal computers. Designed by Steve Wozniak, co-founder, with Steve Jobs, of Apple, it made its way into the private sphere. In 1981, digital technology literally invaded everyday life when the IBM-PC burst into the home. In 1983, the word Internet made its appearance. 562 computers were connected by August.

In 1990, Arpanet disappeared to make way for the World Wide Web. In 1992, there were one million computers connected to 130 websites. Very quickly this archipelago became a labyrinth. In just four years, the number of sites exploded. There were soon more than a million. From then on, orientation became a major challenge in this enormous mass of data. The first search engines were born.

The first smartphone dates from 1992. Marketed two years later, it is the most symbolic object of the digital revolution: it fits in the hand and can be used almost anywhere, combining all kinds of functions: telephone, camera, computer, radio, etc.

In 2000, as the Internet went broadband, 368 million computers were connected worldwide. The network was gradually being democratized. A large number of people were making it their own by opening their own websites. The new means of expression are becoming increasingly intuitive and no longer require very specific computer skills. From then on, the Internet was no longer

conceived as an information superhighway, but rather as a communications society.

What can also be called the participatory web will see the emergence of ever greater interaction. Jimmy Wales and Larry Sanger founded Wikipedia, the first collaborative encyclopedia. Social networks made their appearance. In 2004, Mark Zuckerberg created Facebook; two years later, Jak Dorsey set up Twitter. From then on, the Internet began to penetrate all areas of the private sphere.

The first years of the 2010 decade were characterized by two factors: firstly, the fact that the traditional distinction between private and public life was becoming increasingly blurred; and secondly, the advent of Big Data, linked to the fact that all the information circulating in the world had become so voluminous that it required new tools.

4. Crime Search Process

Computer forensics is the branch of digital forensics that deals with the processing of digital data such as computers, PCs, laptops, smartphones, tablets, hard drives to be used as evidence in a process. In particular, computer forensics is responsible for all activities relating to:

- computer crime in the strict sense (such as damage to a computer);
- offences committed using computer devices (for example, defamation via Facebook);
- behavior in which computer data can be recovered from one or more computer systems (for example, the recovery of deleted WhatsApp messages containing the organization of a murder);
- actors, roles and competences in criminal and civil proceedings;
- rules relating to computer forensics in criminal and civil proceedings;
- strictly computer-related crimes and crimes for which computer data may constitute evidence;
- reference technical and methodological aspects for those working in the field of digital forensics;
- paradigmatic scientific research techniques where tests in digital format are used;
- critical problems and operating methods for the acquisition, storage, analysis and production of digital data (with reference to ISO/IEC 27037);
- hardware and software tools for computer forensics;
- practical laboratories and simulations to put into practice what is learned in the theoretical part of the course.

The phases of digital data processing are as follows.

4.1. Identification

Computer forensics initially involves the identification of relevant computer data, in particular hard disks, computers, laptops, USB sticks, etc. Computer forensics in the strict sense does not deal with smartphones, tablets and mobile phones, which fall within the remit of mobile forensics (see **Figure 1**).

Figure 1. Computer forensics.

An important distinction between traditional computer forensics and mobile forensics is the reproducibility of evidence in the case of post-mortem analysis (device switched off). This is because, unlike traditional computers, phones are constantly active and their content is continually updated. The hash code produced by these devices therefore generates a different value each time the function is executed on the device's memory.

It is therefore impossible to obtain a bit-by-bit copy of a smartphone's memory with the same hash code, although some phones can be "dumped" when they are switched off and special procedures can be used to obtain the same hash again.

Computer forensics on laptops presents difficult problems of data retention, efficiency and accuracy. Forensic investigators can glean a lot of information about users of these portable devices, as often the target uses them to do business quickly and on the fly, while leaving no time to erase leads or encrypted data. Most forensic analysis of laptops is done offline rather than on a dynamic system, as users tend to turn laptops off after use. Many of the same principles of computer forensics apply to laptop investigations, with the added challenge of working with smaller and more portable internal parts.

The experts [9] all have several computers per office and are constantly keeping abreast of developments in new technologies. It is an integral part of their job to have access to data on an encrypted telephone or a password-protected computer, when these elements are necessary for the magistrate, in order to materialize an offence or look for links with other offences.

Computer scientists work alongside electronics engineers and cryptology experts. Signal processing ranges from the processing of data from a black box (orange in color) found in a plane crash, to the processing of video images, telephones or hard disks.

It's all about giving meaning to digital information. The study of documents falls into this category, because they are increasingly digital and require IT tools to be able to read them. However, traditional optical macroscopes or spectros-

copic analysis methods are still used on a daily basis to detect fraud or forgeries, or to establish links between these forgeries.

4.2. Collection

After identification, the systems containing the data of interest must be physically available. During the collection phase, IT forensic specialists dismantle the media and secure them for safe transport and storage.

4.3. Acquisition

Once the devices of interest have been detected, the acquisition phase deals with the duplication of data using specific forensic tools such as hardware copiers and write blockers. At the end of the acquisition phase, all the data collected is characterized by a digest that enables the integrity of the forensic copy produced to be checked at any time.

If carried out correctly, the acquisition phase can be repeated at a later date, using the same tool or even different software and acquisition procedures to those used the first time.

4.4. Analysis

The forensic analysis [10] of the copy produced during the acquisition phase is processed by specific software selected according to the type of questions: it may be necessary to carry out e-discovery rather than recovering the deleted browsing history. All the results of the analysis phase must then be correlated with each other in order to carry out a complete evaluation of the data processed.

Finally, all the data collected and evaluated in this way is compiled into a computer forensics technical report that can be used as a document to be produced in court. Computer forensics originated in the common law environments of the United States in the 1980s, when the demand for analysis of digital devices began to grow.

To meet this demand, the FBI first responded by setting up the Computer Analysis and Response Team (CART), and then numerous laboratories specializing in computer forensic services were created. The instruments used to process computer findings are also tested, notably by the National Institute of Standards and Technology (NIST).

4.5. Presentation

The primary objective of computer forensics is to perform a structured investigation on a computing device to find out what happened or who was responsible for what happened, while maintaining an appropriate documented chain of evidence in a formal report. The syntax or template for a computer forensic report is as follows (see **Figure 2**).

4.5.1. Executive Summary

The Executive summary section provides basic information about the conditions

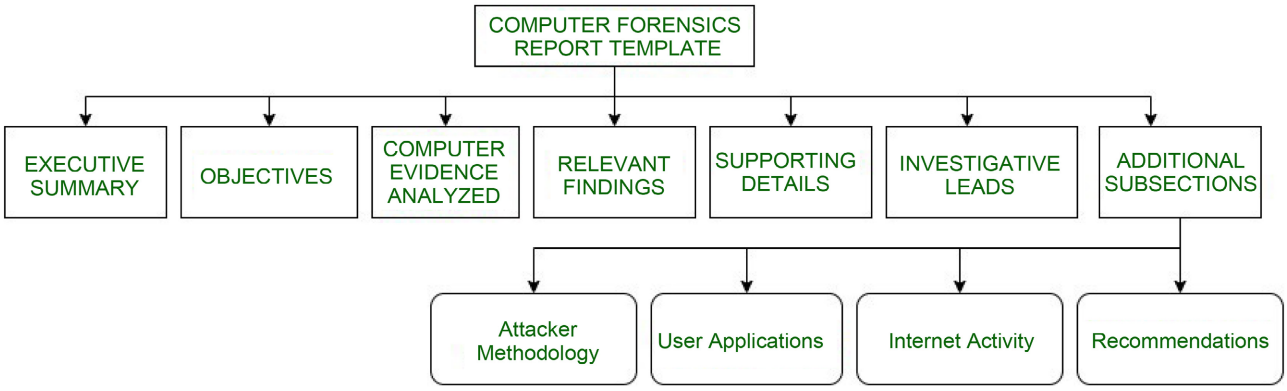


Figure 2. Computer forensic report.

that require investigation. The summary or translation of the summary is read by senior staff who do not read the detailed report. This section should contain a brief description, details and important indications. On one page, it includes the following elements:

- Acknowledgement of the person who authorized the forensic examination.
- A brief list of significant evidence.
- Explain why a forensic examination of the computer system was necessary.
- Include a signature block for the examiners who carried out the work.
- Full, legitimate and correct names of all persons connected with or involved in the case, job titles, dates of first contact or communication.

4.5.2. Objectives

This section (objectives) is used to describe all the tasks that an investigation plans to carry out. In some cases, it may not be possible to carry out a full forensic investigation when examining media content. The list of plans prepared should be discussed and agreed by legal counsel, decision-makers and the client prior to any forensic analysis. This list should include the tasks undertaken and the method used by the examiner for each task, as well as the status of each task at the end of the report.

4.5.3. Computer Evidence Analyzed

The "Computer evidence analyzed" section presents all the evidence collected and its interpretation. It provides detailed information concerning the allocation of evidence tag numbers, the description of the evidence and the serial numbers of the media, ecc.

4.5.4. Relevant Findings

When a match is found between forensic material recovered from a crime scene, for example a fingerprint, lock of hair, shoe print, etc. and a reference sample provided by a suspect in the case, the match is generally considered to be strong evidence that the suspect is the source of the recovered material. However, the probative value of evidence can vary considerably depending on how it is characterized and the assumption of its interest. It answers questions such as "What

objects or related items were found during the investigation?"

4.5.5. Supporting Details

This section is where the in-depth analysis of the relevant results is carried out. It explains how the conclusions drawn are relevant to the investigation. It contains a table of essential files with full pathname, search results by string, emails/URLs examined, number of files examined and any other relevant data. All the tasks undertaken to achieve the objectives are described in this section.

The Supporting Details section focuses more on technical depth. It includes graphs, tables and illustrations, as it conveys much more than written text. Numerous sub-sections are also included to achieve the objectives set. This section is the longest. It begins by giving details of the context of the media analyzed. It is not easy to report the number of files examined and the size of the hard disk in human-understandable language. As a result, the customer needs to know how much data has been examined in order to arrive at a logical conclusion.

4.5.6. Investigative Leads

Investigative Leads perform actions that may help uncover additional information related to the investigation of the case. Investigative Leads complete any outstanding tasks to find additional information if time permits. The Investigative Leads section is very important for law enforcement. This section suggests additional tasks to uncover information needed to progress the case. For example, find out if there are any firewall logs that go back far enough to give an accurate picture of the attacks that may have taken place. This section is important for a committed forensic consultant (see Figure 3).

4.5.7. Additional Subsections

Various additional subsections are included in a medico-legal report. These subsections depend on the client's wishes and needs. The following are most useful in specific cases:

Figure 3. Investigative leads.

- *Attacker Methodology*: Additional information to help the reader understand the general or exact attacks carried out is given in this Attacker Methodology section. This section is useful in cases of computer intrusion. Inspection of how attacks are carried out and what the pieces of attacks look like in standard logs are done here.
- *User Applications*: In this section, we discuss the relevant applications that are installed on the medium being analyzed because it has been observed that in many cases, the applications present on the system are very relevant. Give this section a title if you are investigating a system used by an attacker, e.g. Cyber Attack Tools.
- *Internet Activity*: The Internet Activity or Web Browsing History section gives the web browsing history of the user of the media being analyzed. This is also useful for suggesting intent, downloading of malicious tools, unallocated space, online searches, downloading of securely deleted programs or evidence deletion type programs that delete empty files and temporary files that often house evidence very important to an investigation.
- *Recommendations*: This section provides recommendations for the customer to be better prepared and trained for the next IT security incident. We look at some host-based, network-based and procedural countermeasures that are given to customers to reduce or eliminate the risk of a security incident.

5. Techniques

There are several types of computer forensics depending on the field in which a digital investigation is required. The fields are as follows: (See **Figure 4**)

- Network forensics;
- Email forensics;
- Malware forensics;
- Memory forensics;
- Mobile phone forensics;

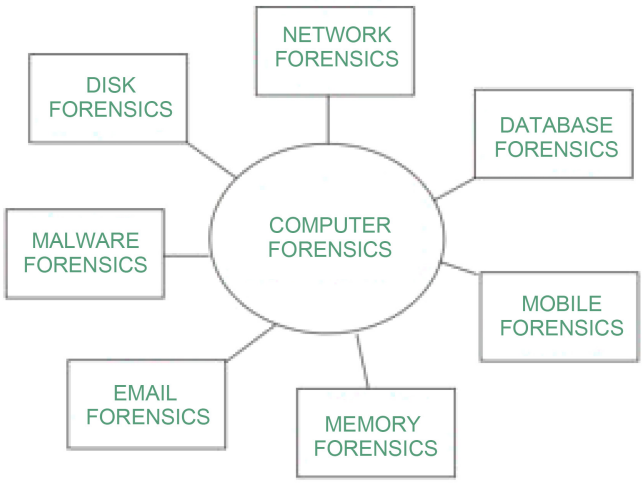


Figure 4. Areas of application.

- Database forensics;
- Disk forensics.

Computer forensic investigation normally follows the typical digital forensic procedure of acquisition, examination, analysis and reporting. These investigations are mainly carried out on static data (disk images) rather than live data or live systems, although in the early days of computer forensics investigators worked on live data due to the lack of tools. Various types of techniques are used in computer forensic investigations, such as:

Cross-drive analysis: Cross-drive analysis (CDA) is a technique that allows an investigator to quickly identify and correlate information from multiple data sources or information on multiple drives. Existing approaches include multi-disk correlation using text searches, for example, email addresses, SSNs, message IDs or credit card numbers.

Live analysis: This is used to examine computers from the operating system upwards using various forensic and system administration tools to obtain information from the device. In forensic analysis, the collection of volatile data is very important such as installed software packages, hardware information, etc. This approach is useful if the investigator is dealing with encrypted files. If the device is still active and running when it is handed over to the investigator, the investigator should collect all volatile information from the device, such as the user's login history, open TCP and UDP ports, services currently in use and running, etc.

Deleted file recovery: This is a technique used to recover deleted files. Deleted data can be recovered or searched using forensic tools such as CrashPlan, On-Track EasyRecovery, Wise Data Recovery, ecc.

Stochastic forensics: This is a method of forensically recovering digital activities that lack sufficient digital artefacts, analyzing emerging patterns resulting from the stochastic nature of modern computers.

Steganography: This is the technique of hiding secret information inside or on top of something, that something can be anything from an image to any type of file. Computer forensic investigators can counter this by examining and comparing the hash value of the modified file and the original file, the hash value will be different for the two files, even though they may appear identical on visual inspection.

6. Volatile Data

Computer forensics plays a very important role in the fight against terrorism and criminal activity. The fact is that the bad guys use computers, the Internet and other modern communication tools to transmit and store their plans. It would be naïve to think that they can barely open Word or Excel. They are aware of all the risks and protect themselves with modern encryption algorithms and general protection measures. Combating criminal activity is very different from discovering occasional breaches on company computers.

Many traces can be masked if the software used for criminal or otherwise undesirable activities is not present on the computer's disk and is running in the computer's memory. It is very easy to start a process and successfully cover all the traces that have been left behind. In this case, there is no point in analyzing the data on the disk because nothing suspicious can be found. The only solution to this problem are tools that can protect volatile data such as RAM.

Static analysis of computer data (*i.e.* analysis of a hard disk removed from the computer) is generally not sufficient as many advanced techniques can be used to erase all traces of file systems and the only relevant data remains in memory. Theoretically, it would be possible to freeze the computer's memory with liquid nitrogen and this would considerably increase the chances of recovering the data, but this approach is not practical. Live analysis of volatile data in a computer is essential for any serious forensic analysis.

There are many commercial, open source and professional forensic tools that can snapshot crucial volatile data for later analysis. These tools can discover open ports, virtual disk drives, VPN connections and other resources not visible to the normal user. In some cases, the entire disk drive or individual partition may also be encrypted. It is therefore important to create an image before shutting down the system. Once all the data is safely stored, it can be analyzed regardless of the state of the computer.

A logical question would be, for example, what can be done to successfully hide certain running processes in the computer's memory? Theoretically, it would be possible to eliminate traces from memory when the process is not active or when it is waiting for input. But even for such approaches, there are solutions. It is possible to create memory snapshots at periodic intervals and sooner or later the secret process will show itself.

7. Analysis Tools

Many tools enable investigators to process and obtain sufficient evidence following civil or criminal proceedings. There is open source and commercial software adapted to all platforms. It would be risky to claim to list them all in this work. Here are just a few of the top 8:

- Lace Carver makes it possible to efficiently extract evidence files and import them using the LIA or JSON format into all the different tools they choose to use to analyze and examine photo, video and documentary evidence.
- BlueBear Lace is one of the best software solutions for processing, categorizing and managing large volumes of visual media. It's simple, robust, won't crash, doesn't require a dongle and processes a million images in less than 2 hours. It enables investigators to efficiently categorize large amounts of image and video data from confiscated computers, dramatically reducing the time and resources required to take cases to court. Using advanced biometric analysis, faces found in images are automatically extracted and compiled to create lists of victims and suspects, or compared with existing facial databas-

es. The technology automatically detects and extracts faces from files. The extracted faces are stored in a database and matched with similar faces, both in the current case and in other cases. An investigator can quickly scroll, edit and select faces for further investigation or for inclusion in case reports. The tool also includes a unique single face search functionality that allows an investigator to search the accumulated face database using any image file.

- Digital Forensic Framework DFF is a data analysis and presentation tool that is capable of extracting, analyzing and correlating suspicious traces and data from various files acquired from digital media, such as hard disks, RAM or mobile phones. It can also be used to recover deleted data.
- Forensic Toolkit (FTK) is known for its efficiency in email analysis, keyword searching and stability. FTK is one of the most popular tools used by police forces: Acquisition, registry analysis, investigation, file decryption, password cracking, reporting.
- Recovers passwords for over 100 applications: computation can be distributed across the network to use the power of different processors to decrypt files and carry out robust dictionary attacks.
- Know File Filter (KFF) hash library with 45 million hashes.
- Supports several libraries.
- Disk Drill is a proven data recovery tool that has been successfully used by users around the world to recover documents, images, video files and other types of data from multiple storage devices.
- Magnet Forensics can be used to acquire physical data from telephones. These physical acquisitions can then be loaded into tools such as Cellebrite.
- EnCase Forensic Software is capable of performing acquisitions, restoring hard disks, completing a full disk investigation and producing comprehensive reports.
- Regripper enables analysis of system registers. This is important for the discovery of evidence. Regripper can be used to discover programs and deleted files.

8. Congo in the Digital Age: A Plea for Digital Legislation

Napoleon Bonaparte's now famous maxim, taken up by the various schools of law, that *nemo censetur ignorare legem*, represents a legal fiction, *i.e.* a principle whose realization is known to be impossible, but which is necessary for the functioning of the legal order. If this fiction did not exist, it would be sufficient for any person prosecuted on the basis of a law to plead (and even prove) ignorance of the text in question to escape punishment.

With the rise of digital technology, the Democratic Republic of Congo is facing a surge in publications of an insurrectionary nature. In addition to the digitization of data, this situation has been reinforced by two other factors: on the one hand, the Democratic Republic of Congo's lack of commitment to democratization, and on the other, the absence of solid legislation governing the use of IT

tools.

Preventing and combating the dissemination of false information requires the coordinated implementation of various means, most of which are more a matter of political encouragement or self-regulation by the players involved than binding legal standards. Nevertheless, in a state governed by the rule of law, it is essential for the law to provide a number of instruments to counteract and punish certain serious forms of such dissemination, particularly on digital networks.

To halt the proliferation of incitement-based publications, the issue must be tackled at two different levels:

8.1. From the Citizen's Point of View

At this stage, it would be reasonable to define what is best called digital citizenship. This refers to the ability to engage positively, critically and competently in a digital environment, drawing on the skills of effective communication and creation, to practice forms of social participation that respect human rights and dignity through the responsible use of technology.

However, in the Democratic Republic of Congo, this concept is far from being unanimously accepted in its general sense. To put an end to this imbroglio, updating and strengthening the legislation must be a priority. The legislation also needs to be publicized so that everyone can make good use of it!

So the digital revolution is having an ambivalent effect on the exercise and protection of fundamental rights. It catalyzes and amplifies the exercise of certain rights. Whereas the so-called traditional media acted as a filter, depending on their editorial lines and the quality of the content they offered, the internet has allowed the emergence of digital platforms that host, without any a priori control or intermediation, all kinds of content from people who are no longer necessarily professionals in the dissemination of information and opinions, but ordinary individuals.

In theory, there are no barriers other than language or the reputation of the sender to prevent anyone from accessing the content posted online on the other side of the world. According to the Congolese Constitution, the free communication of thoughts and opinions is one of the most precious human rights. This is why citizens need to be trained in digital citizenship so that they can take advantage of the potential offered by information technology.

At the same time, the digital revolution is giving rise to new or increased risks for certain fundamental rights. The right to respect for private and family life is a typical example of the risks whose scale has been increased by the development of the Internet. The Internet encourages a worrying collective hypermnesia. The ease with which people can publish online has potentially harmful effects on their reputations. These effects are reinforced by the capacity to collect and store data, and the power of data processing, making it possible to compare information that was previously impossible or very difficult to do.

The protection of public order and security is also destabilized by the rise of

digital technologies. First and foremost, these technologies increase the risk of disseminating illegal content, such as that inciting racial hatred, discrimination, violence or crime. The development of digital technology, as a catalyst for the exercise of certain fundamental rights and freedoms, gives rise to new risks that call into question the traditional balance expressed in existing constitutional, legislative and case law provisions.

In a country where this sector is still in its infancy, as is so clearly demonstrated by its legislation [11] on the subject, it is more than imperative to look into it in order to produce a legal text that will protect the user.

The challenges facing citizens in the digital age are having a greater impact than ever before. The collapse of borders brought about by the interconnectivity of networks calls for a greater awareness of this new citizen because of the social, ethical and economic implications of sharing data in cyberspace. The citizen of Athens now has a planetary impact, because the walls of the city have collapsed since the advent of digital technology. As the French philosopher Michel Serres so aptly put it, "new technologies have condemned us to become intelligent" [12]. The Congolese people expect digital transformation to simplify their lives. To achieve this, the public administration must undergo a transformation towards the use of IT tools.

8.2. From the Point of View of the Government of the Republic

The legislation on digital services and the legislation on digital markets set a high global benchmark for the regulation of digital services, with clear obligations adapted to the importance of online platforms.

In the face of this digital revolution, support for citizens is becoming an imperative. Like all sectors of the economy, the public sector is currently faced with the need to rethink the way it operates, taking digital technology into account. The Congolese government needs to do a number of things to make this easier. Here are a few actions that are likely to strengthen the State's power over the management of this sector in the Democratic Republic of Congo:

- Education in digital citizenship.
- Building digital infrastructure.
- Raising awareness of digital culture.
- Creating and/or strengthening digital legislation.
- Publicizing the law on digital technology.
- The creation of a brigade known as the postal police.
- Acquiring hardware and software for computer and/or mobile forensics operations, etc.

9. IT and Ethics

Before tackling this section, it is essential to understand ethics. Ethics is a philosophical discipline concerned with moral judgements, and its concept is therefore very close to that of morality. It is a fundamental reflection of all people in

order to establish their standards, limits and duties. Computer ethics deals with the procedures, values and practices that govern the process of consuming computer technology and its related disciplines without damaging or violating the moral values and beliefs of any individual, organization or entity.

In a country where the majority of the population is made up of computer immigrants, we need to sound the alarm about how to integrate IT not only into the economy but also, and above all, into society. Hence the urgent need to adapt the laws in this area in line with developments in computer technology.

Introduce people to the ethical, legal and social issues involved in the development of certain uses of information technology in different areas of scientific, technical or industrial activity (nanotechnologies, home automation, telecommunications, etc.) in the health, education, economic and security sectors; understand the social system of ethical values and the normative mechanisms governing practices, in particular laws, regulations, codes of ethics, ecc.; Develop ethical deliberation and dialogue on these issues, which must be a major concern for governments in the Deep South.

Fundamental notions of applied ethics and the main contemporary ethical theories in technology impact assessment; IT law, moral principles and ethical values in the development of technologies; social acceptability and ethical acceptability in impact studies; the process of global impact analysis and ethical acceptability must be high on the agenda of our governments [13].

10. Conclusions

Reconciling the interests at stake also requires the definition of a stable legal and ethical framework adapted to the specificities of digital technology. Computer forensics is an important element in dispute resolution. Computers have become an important part of your life. This does not exclude criminals who have the technical know-how to hack into computer network systems. Electronic evidence has played a role in court, but obtaining it can be difficult.

The authentication of a crime committed through the misuse of IT tools requires the contribution of several experts. These days, the tools and techniques offered by computer forensics are used to solve this kind of problem. In this sense, computer forensics is beneficial, but it also has its drawbacks.

This article has had the advantage of highlighting the advantages as well as the disadvantages of the application of computer forensics. The main advantage of computer forensics is its ability to search and analyze a mountain of data quickly and efficiently. They can search for keywords on a hard drive in different languages, which is beneficial because cybercrime can easily cross borders via the Internet.

Valuable data that has been lost and deleted by offenders can be recovered, which becomes substantial evidence in court. In this way, computer forensics becomes an auxiliary branch of the law insofar as it helps the latter to gather scientific evidence for computer-related offences.

The main drawback is the cost of data recovery. Computer forensic experts are hired on an hourly basis. Analyzing and communicating the data can take up to 15 hours, but this will also depend on the nature of the case. Another is that during data recovery, the analyst may inadvertently disclose privileged documents.

Although computer forensics has its drawbacks, these can be resolved by the party involved. Evidence, on the other hand, can only be seized once. The use of computers and the rise of cybercrime also call for an equally sophisticated method of stopping it. At this stage, the only solution is education in digital citizenship and digital legislation.

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] Stener, C. (n.d.) Dictionnaire politique d'Internet et du numérique. Les 66 enjeux de la société numérique. La Tribune.

[2] Strauss, A. (1989) L'individu face à la révolution technologique. Centre d'Etudes Appliquées a la Communication, Paris.

[3] Chantepie, P. and Le Diberder, A. (2005) Révolution numérique et industries culturelles. La Découverte.

[4] Lipkin, J. (2006) Révolution numérique: Une nouvelle photographie. éditions de la Martinière, Paris.

[5] Scherer, E. (2009) La révolution numérique: Glossaire. Dalloz, Paris.

[6] Alain Bravo, A. (2009) La société et l'économie à l'aune de la révolution numérique: Enjeux et perspectives des prochaines décennies. La Documentation française. https://fr.wikipedia.org/wiki/La_Documentation_fran%C3%A7aise

[7] Rieffel, R. (2014) Révolution numérique, révolution culturelle? Editions Gallimard, Paris, 16 p.

[8] Hobbes, T. (1651) Léviathan. Traité de la matière, de la forme et de la forme de la République ecclésiastique et civile, London.

[9] Broucek, V. and Turner, P. (2001) Forensic Computing: Developing a Conceptual Approach in the Era of Information Warfare. *Journal of Information Warfare*, **1**, 95-108.

[10] Farmer, D. and Venema, W. (2000) Forensic Computer Analysis: An Introduction. Reconstructing Past Events. *Dr Dobb's Journal*, n˚29, 70-75.

[11] https://www.numerique.gouv.cd/.

[12] https://anaishugo.wordpress.com/2011/11/14/michel-serres-%C2%AB-les-nouvelles-technologies-nous-ont-condamnes-a-devenir-intelligents-%C2%BB/.

[13] https://programmes.uqac.ca/4ETH236.