International Journal of Science Academic Research
Vol. 02, Issue 12, pp.3301-3309, December, 2021
Available online at http://www.scienceijsar.com

ISSN: 2582-6425

Research Article

PROTECTION OF PERSONAL DATA IN CHAD

***RAMARDE Nedoumbaiel**

University of Moundou / Chad

Received 20th October 2021; **Accepted** 26th November 2021; **Published online** 30th December 2021

Abstract

Chad, like other countries, adopted legislation protecting personal data in 2015. According to article 5 of Law No. 007 / PR / 2015 of February 10, 2015, the scope covers " *any information relating to a natural person identified or identifiable directly or indirectly, by reference to an identification number or to one or more elements, specific to his physical, physiological, genetic, psychological, cultural, social identity or economic* ". Nevertheless, some shortcomings likely to hamper the effectiveness of this protection are to be underlined. This concerns in particular the gaps relating to the principle of protection of personal data, under which, the difficulties of proving the existence of the consent of an illiterate, in the absence of witnesses, the non-respect of consent in the event of data transfer abroad. Regarding implementation, it is necessary to note the difficulties inherent in the absence of specialized courts and those concerning the territoriality of the criminal sanction. It follows that the intervention of the legislator to remedy these deficiencies is desirable with a view to effective protection.

Keywords: Protection, Personal data, Consent, Will.

INTRODUCTION

The s laws are not acts of pure power; these are acts of wisdom, justice and reason [1] . These laws have the essential functions of contributing to the development of man. From this perspective, the right to respect for private life is a fundamental human right. The privacy of individuals must be protected against all attacks that may affect them, especially those relating to their personal information. It is advisable to grant to the individual a secret sphere of life from which he will have the power to exclude third parties. Modern doctrine thus recognizes the right to respect the privacy of his person, the right to be left in peace, that is to say, a freedom [2]. Respect for private life essentially translates into a duty to abstain. It is the psychological value that is protected. The right to the protection of private life is recognized for everyone, even those who are unable to exercise it [3]. Privacy is designed by article 7 of the civil code [4] as the subject of a subjective right. We deduce that the text comes into effect by the sole fact of the damage suffered, without the victim having to prove the conditions of liability for fault [5]. The increasing development of digital technology, the protection of privacy and personal data are hot topics. Nowadays, the Internet has become an essential tool for communication and exchange of all kinds, and the question of the protection of privacy is raised with acknowledgment in the digital air.

Protection is an original Latin word *protecio* verb *protegere* which means protecting [6]. For CORNU, protection is a precaution which, responding to the needs of the person or what it covers and generally corresponding to a duty for the person providing it, consists in protecting a person or property against a risk, guarantee its security and integrity, by legal or material means [7]. This precaution designates both the action to protect or the protection system established [8]. More generally, it concerns the means intended to defend a right, a situation [9].

Corresponding Author:** ***RAMARDE Nedoumbaiel
University of Moundou / Chad

In this sense, we can say that the protection of personal data is a legal mechanism provided for by the legislator, which makes it possible to ensure the security or to guarantee this data against the risks likely to harm the said personal data. It should be remembered that the law is a product of a civilization, that is to say of the culture, mentalities and behaviors of the members of a determined social body, with its aspirations, its beliefs, its dominant ideology and its economic structures. The aspirations of man, his culture and the need to satisfy his needs, particularly in the variable economic order according to places and times, are the basis of any social organization and therefore of any legal system [10]. According to some authors, the Law must tend towards " *fair sharing, the good conduct of individuals, their usefulness, their pleasure, their security, their well-being* ", or towards " *the power of the nation, the progress of humanity., the regular functioning of the social organism*" [11]. In this context, it should be noted that the legislature's concern to ensure the protection of personal data contributes to the achievement of the purposes of the ends of the welfare of the person, on the right.

From this perspective, Chad, like other states on the continent or the world, is not immune to this global phenomenon. This is why it has adopted legal instruments to combat this scourge in general, under which, more specifically, an arsenal is set up for the protection of personal data. These include, in particular, Law n ° 007 / PR / 2015 of February 10, 2015, relating to the protection of personal data, its implementing decree n ° 075 / PR of January 21, 2019, laying down the provisions of 'application of Law No. 007 / PR / 2017, and Law No. 001 / PR / 2017 of May 8, 2017, on the Penal Code [12]. It should be emphasized that ordinary Internet citizens, by their actions, can entrust personal information to third parties, often without their knowledge. It should also be noted that the construction of a suitable legal system is therefore subject, on the one hand to technical developments and, on the other hand, to the necessary arbitration between the interests of the companies responsible for collecting and processing personal data in order to commercial and invasion of the privacy of individuals, subject of these collections. It emerges from point 2, of article

2 of decree n ° 075 / PR / 2019 of January 21, 2019, fixing the implementing provisions of Law n ° 007 / PR / 2015, that by personal data, it should be understood " *any information relating to a natural person identified or identifiable directly or indirectly, by reference to an identification number or to one or more elements, specific to his physical, physiological, genetic, psychological, cultural, social or economic identity* ". This definition is identical to that of article 5 of Law n ° 007 / PR / 2015 of February 10, 2015.

The essential question is, are the aforementioned personal data protection mechanisms effective?

Effectiveness can be defined as "*the character of an act or a decision which produces the effect sought by its author*" [13], or as property that was the norm to produce not only the effects, but "*the impact that was expected of it*" [14]. Effectiveness goes beyond effectiveness. It is certainly, like the effectiveness, of "*the a posteriori assessment of the real results of a standard, of its concrete effects*" [15]. But it is not enough for a standard to be effective, respected by its addressees, to be able to be considered effective: it is also necessary, and this condition is particularly demanding, that it produce the desired effect [16]. It is important to stress that the desired effect is not limited only to the application of the standard. According to one part of the doctrine, effectiveness refers to the relationship between the intention or objective supposed to be sought by the authors of the initial statement and the result obtained. Therefore, "*a text can apparently be applied* [17] *without producing effects which appear to be sought*" [18]. The protection of personal data is effective, if and only if the guarantee is ensured, according to the desired effect, in both its qualitative and quantitative dimensions.

The interest of this study is to make an assessment, both in *concreto* and in *abstracto,* on the value of the protection of personal data envisaged by the Chadian legislator, with a view to strengthening said protection.

The consent to the processing of personal data generates or gives birth to a *sui generis* contract, framed by specific provisions, reinforcing the provisions of common law. This contract can in no case be disconnected from the sacrosanct principles of contract law, in particular contractual freedom, consensualism, the binding force of the contract with its corollaries of requirement of good faith in performance. From this perspective, there are some gaps in the principle of the protection of personal data (I). If the sanction is a reaction intended to restore order [19], the implementation of the protection of personal data, as a sanction seems questionable in the digital air according to the principle of territoriality in criminal matters (II).

I- Gaps in the principle of the protection of personal data

A gap should be understood to mean the limits or difficulties which could hinder the effective protection of personal data. The work of the legislator is laudable and very interesting insofar as it aims at the protection of privacy. But, we must emphasize that this ambition protection of personal data seems to offend the principle of autonomy, especially regarding the proof of the existence of consent (A) and the expression of said consent in case of data transfer to a third country (B).

A- Deficiencies inherent in consent

According to PLANIOL, "*the consent indicates the similarity of the wills contributing to the formation of the act*" [20]. This means that consent is fundamental for the processing of personal data. It will be difficult to prove the existence of this consent for an illiterate, when the latter does not acknowledge having expressed his will (1). In addition, with regard to the duration of the retention of personal data, the legislator has not required to obtain the consent of the data subject. The legislator gives the prerogative to the person in charge of processing personal data to set this period. Such a prerogative is liable to hamper the sacrosanct principle of the autonomy of the will (2).

1- Difficulties in proving the consent of an illiterate person

Giving consent to a contract consists in expressing freely and in full knowledge of the facts, favorably. Consent is the manifestation of the will in a holy spirit [21]. Whoever expresses his will must be able to appreciate the extent or the value of the obligation, of his commitment. Consent is the tool that allows individuals to assert their autonomy and exercise control over their personal information. The law requires organizations that wish to collect, use or disclose personal information to seek and obtain consent from individuals. Proof of the consent of those concerned who can read and write does not often arise, except in bad faith. However, in the presence of people who cannot read or write, managing the proof of the existence of consent seems difficult. In Africa, we can underline the very impressive presence of the workforce and some relatively illiterate or semi-literate economic operators [22]. The question arises as to how to prove the existence of the consent of this category of workers or economic operators relating to the processing of their personal data?

Consent is one of the few elements of privacy that can still be protected from the monstrosities of the internet and others. Proof, according to the legal dictionary, is the demonstration of the reality of a fact, state, circumstance or obligation [23]. Contracts on evidence are valid when they relate to rights which the parties have freely available, however they cannot be established s in favor of one party an irrebuttable presumption [24]. Consent being an element of private life which the person cannot freely dispose of, its proof cannot be the subject of a contract between the parties. It seems that by legislating on the protection of personal data, this vulnerable layer, requiring special protection, has been forgotten or ignored. This oversight exposes this vulnerable layer to the uncertainty of its consent to the processing of personal data. The provision relating to proof of the consent of the illiterate surety, ensuring legal certainty in the law of security interests, should be used as inspiration to propose a possible solution. According to paragraph 2 of article 4 of the Uniform Act on the organization of sureties, "*a surety who does not know or cannot write must be assisted by two witnesses who certify, in the act of surety, his identity and his presence and certify, moreover, that the nature and effects of the act have been specified to him.* (…) ". This requirement makes it possible to prove the existence of consent but also facilitates the possibility for the surety to assess or understand the extent of his commitment. The presence of two witnesses undoubtedly contributes to strengthening the consent of the illiterate surety. This is a precautionary measure favorable to the illiterate surety. Should we or should not consider two witnesses, like

the OHADA legislator in terms of security for the protection of personal data ? It should be recalled that Article 16 of Law No. 007 / PR / 2015 requires a written exclusively in terms of biometric data s and not for any personal data. In this circumstance, in the absence of writing, it would be very difficult to prove the existence of a valid consent in the absence of the witnesses, especially, in the hypothesis of a work relationship, or commercial where are in the presence a professional and a generally illiterate non-professional. It would be desirable to consider, by analogy with the provisions of OHADA security law, the requirement of two witnesses, to facilitate the analysis of the existence of evidence. It is not a question of informing the person about the processing of their personal data. It is mandatory to clearly and previously obtain the consent of the person concerned. This requirement would participate in the protection of private life which is a fundamental, imprescriptible and inalienable human right. Indeed, if the aim of the law is to establish rules capable of leading " *to the greatest happiness of the greatest number* "[25], the requirement of two witnesses in strengthening the consent of illiterate s seems a nécessi side POUVA nt cont r ibuer the purpose of the law. Failure to comply with proof of the existence of consent gave rise to sanctions. By way of illustration, the real estate appraisal company which had carried out a commercial prospection by SMS "*without having previously obtained the explicit consent of the prospects when collecting their telephone number* (...) "was fined [26]. This decision was objectively confirmed by the EC [27]. It will be noted that the company did not respect the right to information and the right of opposition of the persons concerned either [28]. The right to information is conceived as "*a universal, inviolable and unalterable right of modern man. It is a right that is both active and passive: on the one hand, the possibility for everyone to receive it* " [29]. In other words, " *the right to information is the fundamental right of the individual and of the community to know and to make known what is happening and what one has an interest in knowing* " [30]. It is up to the State to ensure that it is respected. In this option, the State must take its precautions, ensuring that the illiterate person who must give his consent on his personal data, can ensure the effectiveness of his consent, but also that the duration is fixed data retention.

The obstacle to the principle of the autonomy of the will

According to the classical theory, which went back to the old law, which still reigned indisputably during the XIX th century, the will is the fundamental element of the contracts. This theory is known under the name of "*theory of the autonomy of the will*" which should be emphasized. The principle of the autonomy of the will, it should be remembered again, means that the parties are free to consent and to submit to the obligations they wish [31]. The autonomy of the will is explained by the political and economic principles which dominated in 1804. The autonomy of the will is based on the postulate of the natural freedom of man proclaimed in 1789 and his dignity is not far away [32]. Another political foundation is that of the social contract. The social contract and the contract itself therefore come under the same idea. Letting individuals contract and letting them organize their private interests in the best possible way is the best way to establish the most just and most socially useful relations between them. It is therefore economic liberalism that dominates the theory of the autonomy of the will [33]. No man could allow himself to be imposed an obligation that would harm him: "whoever *says contractual says just* " says Fouillée [34]. The postulate is therefore that the best way to satisfy social utility is to satisfy one's own interests. The general interest is consistent with the sum of all special interests [35]. At the reading of paragraph 1 st of article 11 of Law No. 007 / PR / 2015 on the protection of personal data, " *data must be kept for a period not exceeding the period necessary for the purposes for which they were collected* ". The law did not determine the duration, nor gave the parties the possibility of fixing this period by mutual agreement, according to the presentation of the need. This provision allows the person responsible for processing personal data, a prerogative in determining the period necessary for the needs of the cause. Otherwise, the data controller implicitly has a discretionary power in setting the necessary period of which the data subject will simply not have to adhere to it. It should be noted that this provision is debatable under the principle of *mutual consensus,* which is cardinal in contractual matters. In fact, it seems that the legislator has failed in its orientation duties towards the preservation of contractual freedom. The Law may, for example, stipulate that video surveillance recordings must not, in principle, be kept for more than one month, personal data relating to customers, for its part, must not be kept. beyond one year at the end of the contractual relationship in current cases. In the same logic of limitation, the Law may require that data relating to the management of payroll or the control of employees' schedules must not be kept beyond five years, etc. such an orientation would make it possible to better appreciate or control the principle of contractual freedom. Because it "*is the corollary of individual freedom"* [36], "*the freedom of conventions [is] admitted as a fundamental principle*" [37]. Already in the spotlight in Portalis's famous opening speech [38], it forms, in our legal system, " *a starting principle*" [39]. In other words, contractual freedom is already a "*guiding principle*" in positive law. At least if we mean by that a directive of general scope, irrigating and dominating the matter, embodying a certain conception of the contract. In the absence of a legislative direction, the Law could leave the possibility to the parties to fix by mutual agreement, this duration. According to doctrine, the human will is its own law, creates its own obligation [40]. It manifests itself when the contract is formed, then once the contract is formed. In the formation of the contract, the individual has a double freedom, that is to say to contract or not to contract, this is the fundamental option. But still and above all determine the content of the contract at will [41]. Only public order is the limit of contractual freedom according to article 6 of the civil code. There appears to be an obstacle to the autonomy of the will in fixing the duration of the processing of personal data. This same difficulty also seems visible in the event of data transfer to a third country.

B- Failure to respect consent in the event of data transfer to a third country

It is common for personal data to circulate. It should be emphasized that from an organizational point of view, personal data circulate between several co-controllers, between a controller and a subcontractor, between several successive subcontractors. From a geographical point of view, these data circulate between the countries of the community, but also towards third countries. This operation which consists in circulating personal data is the transfer. According to CORNU's legal vocabulary, transfer is a legal operation of transmission of a right, an obligation or a function. This is a

mutation [42]. This concerns in particular the transfer of a right of a holder [43] to another [44]. The transfer designates both the result of the operation, the translative effect [45] that the operation itself [46]. The question arises as to whether personal data can be transferred to a third party without the consent of the author, or that of the authority in charge of protecting said data. The consent of the individual constitutes one of the legal bases on which any processing of personal data must be based. Its objective is to allow data subjects to retain control of their data. According to article 29 of Law n ° 007 / PR / 2015, "*the data controller cannot transfer data of a nature to another country which is not a member of CEMAC and ECCAS unless this State ensures a level sufficient protection of the privacy, fundamental rights and freedoms of individuals with regard to the processing of which these data are or may be subject*". Article 30 to complete that ANSICE must be informed beforehand. It should be noted that this is a simple information to be given and not a requirement of an opinion on the part of ANSICE in this matter. By sticking to this provision of article 29, the legislator seems to ignore the principle of specific consent according to each purpose of the processing (2), indirectly, this results in non-compliance with the principle of *mutuus consensus* (1).

1- Failure to respect the *mu tuus consensus* principle

If the transfer is a material operation, requiring the movement in space of an object [47], a transfer of personal data to a third State, being a transfer, can objectively be analyzed as a modification of the initial contract. It should be remembered that according to the classic principle in contractual matters, modification of the contract requires the consent of all parties. This is the *muutus consensus* principle. In this view, before personal data can be transferred to a third country, outside of public policy reasons, respect for the contractual principle would have required that the consent of the person concerned be collected in due form. Otherwise, the consent of the data subject must necessarily be requested. Carrying out this transfer without obtaining the expression of the person's will on the orientation of the provisions of article 29 of Law n ° 007 / PR / 2015, would constitute an infringement of the fundamental right to contractual freedom. According to doctrine, neither the judge can revise the contract, nor the legislator can alter. Only the parties themselves could, by mutual agreement, modify the contract once concluded. [48]. Otherwise, any change in the initial contract requires the consent of the parties, in complete freedom. The transfer of personal data being analyzed in a mutation must require the mutual consent of the parties. The requirement of ' u do simple information to the authority responsible for the protection of personal data without requiring the consent express of the parties to the original contract, seems to undermine the principle *mutuus consensus*. Implicitly, the specificity of consent is hampered, with the consequent failure to respect loyalty.

2- Failure to respect the principle of fairness in processing

It is a principle that the consent of the person must be prior. Each individual has the right to be informed before the data is for the first time communicated to third parties or used on behalf of third parties for prospecting purposes and to be expressly offered the right to object, free of charge to said communication. This requirement is justified by the principle of the specificity of consent. In this sense, the question arises as to whether the transfer of personal data to article 29 of Law n ° 007 / PR / 2015, is it consistent with the principle of fairness in processing?

The lack of consent requirement for the transfer of personal data according to the provisions of article 29 of Law n ° 007 / PR / 2015 constitutes an inconsistency with the principle of loyalty, depending on the purpose of the processing.. According to paragraph 1 st of article 159 of the Uniform Act draft bill to the general law of obligations OHADA that " *the convention 's obligations not only that ' it is expressed, but also to all the consequences which loyalty, equity, custom or the law give to the obligation according to its nature* ". In accordance with the spirit of this provision, contracts must be performed in good faith, that is to say, with respect for the spirit of loyalty. According to legal vocabulary, loyalty designates more specifically either contractual sincerity, in particular in the formation of the contract, or contractual good faith in the execution of the contract, or in the legal debate, the good behavior which consists, for each adversary, to put the other in a position to organize his defense, by communicating to him in good time his means of defense and proof [49]. This is a fundamental principle which must underlie any processing operation relating to personal data. It is therefore necessary to ensure that the data are collected fairly, that is to say that the persons concerned are well informed and that their rights are respected. It should also to ensure that data is protected against any attack that might come third in putting in place the human and adequate technical resources [50]. If the consent is a free, specific and informed manifestation of will, by which the data subject accepts that the personal data concerning him / her are subject to processing [51], the operation of transferring these data cannot be done without the will of this person.

The request for consent for the transfer of personal data is part of the good faith performance of the contract. According to some authors, the obligations arising from good faith constitute requirements arising from social relations.[52]. Another attempt to define the concept consists of an illustrative enumeration of the obligations that good faith gives rise to: obligation of collaboration, information, moderation, loyalty [53] . According to MAZEAUD, "*at the end of a contractual altruism, respectful of particular interests but sensitive to the collective interest of the contractors and the difficulties which can strike each one, a" contractual ethics "develops, based on fraternity and solidarity. The contract is then considered as the crucible of the common interest of the parties and the seat of a sacred union between the contracting parties in the face of the crisis which may strike one of the partners, which translates into a double currency of cooperation and selfless*" [54]. In the same vision, u No other author points out, that the good faith of Article 1134 of the Civil Code is the good will, loyalty, the desire to spend for the benefit of its contractor, to work with him to facilitate his the task, in a word, to love him like a brother [55]. In other words, good faith introduces new rules of behavior in order to obtain more loyal, more equitable, more reasonable solutions [56]. Indeed, obtaining consent for the processing of personal data is one thing, that is to say the object of the initial contract, to transfer the data to a third country is another thing .that is to say, a certain mutation of the initial contract. In any case, the prerogative of the data controller cannot be allowed to simply justify the guarantees of protection and proceed with this transfer, without requiring the consent of the data subject. The consent of the data subject must be given, separately, for each

purpose of processing. The controller must therefore plan to collect separate consent for each purpose so that users can give specific consent for each of the specific purposes [57].

It should be noted that the principle of loyalty is part of the logic of good faith in the performance of the contract. According to the doctrine, it seems that contractual good faith can be linked to more or less active duties. More actively, it is a duty of cooperation that will be required [58]. No one has been as concerned as DEMOGUE with giving a legal face to this duty of cooperation: "*the contractors form a kind of microcosm, a small society where everyone must work for a common goal which is the sum of the individual goals pursued by each, absolutely as in civil or commercial society*" [59]. The idea flourished, and the other authors today evoke the spirit of collaboration as a duty between contractors [60]. It should be emphasized that good faith is relatively close to the notion of solidarity, of contractual fraternity [61]. Good faith implies a certain duty of cooperation between the parties, which may be more or less marked depending on the nature of the contract [62]. According to TERRE, certain contracts constitute the land of choice. This is how in society, the *jus fraternitatis* must reign [63]. It has been pointed out that most of the contracts recently created by commercial practice [64] were based on a "sort *of affectio contractus*" [65]. Otherwise, the controller must cooperate, collaborate and obtain the prior consent of the data subjects before any transfer to a third State. It should be noted that it is in this perspective that the legislator has expressly prohibited "*grouped* " consents which consists in bringing together several distinct treatments [66]. As this is a company specializing in the publication and communication of periodical magazines and the websites of these magazines, the CNIL was able to observe that the Internet user, by checking a box to receive the newsletter of the title of the site that he consulted, could also receive those of other magazines or periodicals issued by the company, but without having information on these other newsletters. Also, she considered that the information provided did not allow to consider that the consent of people to receive newsletters by electronic means is free and specific [67].

More recently, in its deliberation of January 21, 2019 [68], sanctioning Google, the CNIL noted the lack of specific consent, because "(…) before creating an account, the user is invited to tick the boxes" *I accept Google's terms of use* "and " *I agree that my information s are used as described above and detailed in the rules of confidentiality* " to " *to create an account*" Such a process leads the user to consent block for all the purposes for Google on the basis of this agreement, including, customizing advertising, speech recognition etc. it should be noted that this sanction against Google makes it possible to restore the specificity of the consent according to the purpose of the processing. In this perspective, it should be noted that the prerogative granted by the legislator to the person in charge of the processing of personal data, relating to the transfer of said data according to article 29 of Law n ° 007 / PR / 2015, mentioned above seems inconsistent. with the principle of the requirement of the specificity of consent. Logic would have required that the authority in charge of the protection of personal data could give an express opinion, in addition to the necessary consent of the parties to the initial contract. The transfer is a legal operation causing the change of the contract on personal data. As a result, the parties' consent must always be required, objectively, by the legislature. This requirement would help strengthen the protection of privacy.

It follows from this analysis that consent is fundamental to the conclusion and performance of the contract, particularly in the event of a transfer. From this perspective, the transfer of personal data without consent would be an attack on the autonomy of the will, an essential principle in contractual matters. It appears an inconsistency favoring the invasion of privacy which the legislator intends to protect. Moreover, the implementation of the protection of personal data seems uncertain due to the requirements of the principle of sovereignty.

II- The obstacles inherent in the principle of territoriality

In 1972, Dean CARBONNIER already affirmed that "*the evolution of customs and techniques gives rise to new forms of delinquency*" [69]. In fact, most of the great technological discoveries have "*almost always generated, alongside the economic progress they bring to humanity, negative consequences, among which the advent of new forms of crime is prominent. The Internet is no exception to this sociological law of development*" [70]. Like the fight against global warming, the fight against cybercrime is the subject of summits and political debates. The World Summit on the Information Society, held in Geneva in 2003 and in Tunis in 2005, notably helped to identify the need for more international, more "UN" Internet governance, and the need to a more reliable Internet that is more accessible to the whole planet. Global measures were then taken to develop cyber security and fight against cybercrime. Thus, the International Telecommunication Union, through its Global Cyber Security Agenda program launched in 2007, published a strategic report which makes reference, and it helped to create in 2009 the IMPACT Center [71] for combating cyber threats, based in Malaysia. In addition, in 2008, NATO decided to set up a training center in Estonia for the defense against cyber attacks on the Internet. Although it is impossible to list all the institutions concerned with the control of computer security and the fight against cybercrime, let us quote the ENISA [72], or the OECD[73] which provide activities, events, publications and guidelines in these areas. The establishment of these mechanisms at the international level seems edifying for the protection of personal data. However, at the national level, particularly in Chad, practical shortcomings are still visible. We can observe the insufficiency of specialized institutions for effective protection (A) and the limits relating to the territoriality of the criminal sanction (B).

A- The lack of specialized institutions

The development of new information technologies improves the exchange and information capacities within society but at the same time offers a new field of action for crime. Very diverse forms of delinquency which now represent a real threat. It should be noted that the legislator has made very remarkable efforts by adopting a very rigorous law for the fight against this scourge. But the need for special jurisdictions (1) and the special brigade (2) seems to elude the Chadian legislator.

1- The absence of specialized courts

There is no doubt that the protection of personal data would be at the heart of tomorrow's litigation. Cybercrime is "*democratizing* ". Far from targeting only large groups, it now affects small and medium-sized enterprises, communities, hospitals and nuclear power stations, to name

but a few. All sectors are concerned, from agriculture to education through heavy industry, almost all of our activities and interactions are linked to an information system, yet vulnerable to intrusions and hacking. If the digital revolution primarily concerned industries and services using numbers, text, sound, images and videos, which could only induce a transformation of related sectors, such as banking, publishing, music, photography and cinema. Our world of data now connects individuals, objects, robots, sensors in a vast reticular ecosystem. In this perspective, we can underline that law n ° 009 / PR / 2015 of February 10, 2015 is enacted at the appropriate time for the needs of the cause. However, it should be noted that its application seems limited insofar as the legislator has not provided for the establishment of a specialized jurisdiction, like the commercial, labor and social security jurisdictions, or for children.

There are still few arrests or trials in this area given the reality of the malicious acts and no sense of justice for the victims. The cases are not sufficiently denounced and few are investigated. The victims are doubly penalized. First, by the attacks they suffer and secondly, by the ineffectiveness of the instruments supposed to contribute to their protection. It should be noted that these difficulties can be justified in practice, due to the overflow of ordinary courts for traditional cases. The solution to the problem would be possible by the urgent establishment of specialized courts. Judges, by virtue of their initial training, cannot effectively ensure the repressive management of this newly very complex phenomenon, which is the protection of personal data. Judges, being guardians of the fundamental rights of citizens, must receive adequate training to better understand the threats arising from the new information and communication technology. Given its complexity, the effective fight against cybercrime in general, the protection of personal data in particular, requires specialized training for judges. This is a very urgent imperative that seems to escape the Chadian legislator. It is desirable to initiate this circumstantial training to better equip our guards to better perform their republican function. The National Financial Prosecutor's Office in France could thus serve as an example [74]. The creation of a public prosecutor's office specializing in digital technology would make it possible to respond to the problems posed by offenses specific to electronic networks, in particular attacks targeting information systems, denial of service and hacking as well as those committed using electronic networks. Electronic communication networks and information systems when these reach a certain degree of complexity or constitute particularly serious damage. Its high level of specialization and the cutting-edge tools that would be entrusted to it would, for example, make it possible to identify authors who use encryption processes and collect evidence made more difficult to obtain by advanced technologies. Some initiatives have already been deployed in the State of Rio in Brazil, or in Spain, where there is a General Prosecutor in charge of cybercrime who benefits from the help of 70 prosecutors gathered within a specific prosecution dedicated to this type of crime criminality. The creation of a digital judicial branch presupposes discussing upstream the type of specialization of judges, their number, the centralization or decentralization of such a prosecution, or even the possibility of setting up a prosecution at European level. A major challenge will then be to coordinate the action of the Digital Prosecutor's Office with the various existing specialized services, digital technology often being a means allowing serious organized crime to launder money or finance terrorist networks, for which others bodies are already competent. At term, the creation of a specialized 33rd Correctional Chamber and exclusively dedicated to the trial of offenses investigated by the National Prosecutor's Digital - the image of the 32 th French Criminal Chamber, dedicated to business from the National Financial Parquet [75] could be relevant.

Urgency now requires us to reflect on the development of digital litigation. It is above all a question of change management, awareness, education that will instill a digital culture. This development will appear prospective for some. Anticipating it is however essential. Driving change is a long process. But inevitably it will be the only way to dispose of tomorrow parquetiers, survey services with the knowledge and resources necessary to address matters of protection of personal data. This specialized judicial institution needs to be reinforced by a specialized brigade.

2- The absence of the brigade specializing in digital crime

For a layman, the term law evokes a set of rules that one is bound to respect under the threat of a judicial sanction. The law, for non-jurists, is the fear of the gendarme and recourse to the judge. The idea is not wrong if we can stick to the Latin term *juice,* which means right [76]. In this perspective, to see a special brigade against cybercrime in general and the protection of personal data is an absolute necessity given the complexity of the technique or the means used by the new generation of criminals. The traditional institutions of the fight against delinquency are already overwhelmed by other files and generally do not have time to analyze or assess the offenses resulting from the new technology. The mission of the special brigade will be, on the one hand, to conduct specific judicial investigations (a), on the other hand, to collect specific criminal intelligence (b).

a- Conduct specific judicial inquiries

For a country, having a competent military force dedicated to "*cyber* " issues is imperative, as is its preparation to be able to manage major crises due to its dependence on information technologies as well as its energy supply. The stability of a country, its sovereignty and its economic development now depend on its ability to control cyber risks. Ensuring the cyber security of people, tangible and intangible goods but also public safety is part of a political project in the service of a sustainable development strategy for society [77]. It seems the establishment of a specialized brigade is necessary to meet these challenges. The main mission of the brigade will be to conduct judicial inquiries, exclusively carried out in criminal matters on direct referrals or in support of judicial police units. In 2013, Senegal created its first service to fight cybercrime, then in 2017 a "cyber security division" dependent on the Senegalese judicial police. This structure, established in six months, enabled in 2017 "the arrest of forty hackers broke into the computer system of large Senegalese companies to divert are estimated at over 100 000 euros" [78]. The 2 ^{e} mission of the brigade would be to collect information for the purposes of the case.

b- Collect specific criminal intelligence

On the Internet, the marketing of war and terrorism borders on that of legal and illegal businesses and the cybercrime black

market is doing well. Internet is a privileged ground of expression of the crime, the communication of influence and the surveillance. Disrupt vital infrastructure [79] of a country, serving criminal strategies, generating losses in productivity, competitiveness or power seizures is not only possible but greatly facilitated by the Internet. The second mission of the brigade will be to collect criminal intelligence. This mainly involves operational monitoring to monitor the state of the cybercrime threat on a daily basis. It must study the main trends of the phenomenon and identify the different families of offenses in the country and in Africa. It must also analyze the emerging modus operandi and the typology of perpetrators and victims. Senegal has advanced digital capacities and actively cooperates with other States in the sub-region and elsewhere in this field. In addition, Senegal organizes the *Security Days* every year ,on digital security in Africa, with French companies, and the country adhered to the Budapest Convention on Cybercrime in 2016 [80].

However, we can deplore the absence of legal auxiliaries specialized in the matter to face this fight of the robust on the national territory. The auxiliaries of justice being central agents, inescapable, strategic as regards investigation and research, must be trained to carry out their mission well in the general interest. It should be noted that their initial training is not adaptable to the development of new technology. E onsider strengthen their special way of competence is a public policy requirement which seems to escape the legislator. Another difficulty of the sanction is the principle of territoriality in criminal matters.

B- The limits inherent in the territoriality of the criminal sanction

Territoriality in criminal law, with its corollaries, the principle of sovereignty (1) and the virtual nature of delinquency (2) do not facilitate the repression of computer offenses in general, and that relating to personal data in particular.

1- The dogmatic principle of state sovereignty

The repression of offenses committed on the Internet, in particular with regard to personal data which is often of an international nature, is far from being satisfactory at present since the rules of classic international criminal law, deduced from the principle of national sovereignty in criminal matters and the principle of territoriality, constitute obstacles to the effectiveness of repression[81]. As a result, in the name of national sovereignty, the State presents itself as " *the sole master in the assessment of its interests and in the development of punishable offenses which it intends to protect* " [82]. This results in the exclusivity of national jurisdiction in criminal matters (a) and the refusal of recognition of the foreign judgment (b) which hamper the effectiveness of virtual repression in relation to personal data.

a- The exclusivity of national powers in criminal matters

The International Court of Justice (ICJ) in an advisory opinion of April 11, 1949, was one of the first institutions to recall that "*the State occupies a central place on the international scene. He has the sovereignty to know the fullness of the competences*" [83]. This is, moreover, what differentiates a State from an international organization, which has only functional competences, narrowly circumscribed to the achievement of its object and its goals[84]. It appears that the idea of a sovereign state is difficult to reconcile with the coercive nature inherent in criminal law. Indeed, " *justice, and more specifically criminal justice, is one of the attributes of a State's sovereignty, at least one of its essential components* " [85]. This is a prerogative inherent in each sovereign state[86], egalitarian in international practice. Moreover, for the cybercriminal, the risk is that of a plurality of prosecutions, even of convictions in different States. The result of this analysis is that the international dimension of digital networks gives the crimes and offenses committed there a particular legal complexity, in particular in terms of territorial jurisdiction and the execution of their decisions. The principle of territoriality and the expression of the national sovereignty of a State are even more open to criticism when they fail to execute a foreign conviction judgment.

b- The principle of the territoriality of criminal judgments

It should be noted that by virtue of this principle, the effects of a conviction decision are strictly confined to the territory of the State where it was rendered. As a result, a foreign conviction judgment is not enforceable in Chad. This solution is unfortunate and necessarily plays into the hands of cybercriminals who play off borders. The case of the Yahoo case can perfectly illustrate the principle of sovereignty available to the United States. Indeed, on May 22, 2000, the French judge in interim proceedings of the Paris TGI had ordered, under penalties to the American company Yahoo to find technical solutions to prevent French Internet users from accessing the auction site on which items appeared. Nazis. According to French law, simple viewing constitutes a violation of penal provisions [87]. Confirmed by the decision of the Paris TGI on November 20, 2000, the interim order was accompanied by a report drawn up by a panel of experts detailing the measures likely to be implemented, in particular in terms of filtering Internet users in according to their email address, in order to put an end to this unlawful disturbance of public order. But to become effective, this French decision had to be confirmed by an American judge. But even before the judge basically cannot decide, the American company turned to the Court of 9 th Northern California district, according to the procedure known as "*declaratory judgment* ", so it examines compliance the provisions of the US constitution protecting freedom of expression. In his judgment of November 7, 2001, Judge Jeremy FOGEL considered that the French decisions would be "*clearly incompatible with the ^{1st} Amendment if they were made applicable in the United States by a court (...). Although France is sovereign in determining the limits of freedom of expression on its territory, this Court cannot enforce a foreign decision which does not respect the American Constitution, except to annihilate the freedom of expression protected within our borders*". It should be noted that this decision is not surprising when it aims to protect freedom of expression in the United States. Nevertheless, it generates serious consequences insofar as even if the foreign courts *ultimately* accept the international jurisdiction of the distant court, the implementation of these decisions can always be stopped, in the name of the principle of national sovereignty, by a judgment refusing recognition and / or declaration of enforceability [88]. It is clear from this case that only an international cooperation effort will make it possible to overcome the risk of seeing the implementation of repression annihilated, because of the differences existing between international legal spaces.

2 - The difficulties relating to the virtuality of delinquency

With regard to the virtualization and dematerialization of data, the place of commission of the offense is no longer necessarily located on the national territory or in the jurisdiction where the consequences of an offense are concretely manifested. The result is a complexity in the fight against perpetrators or virtual and borderless delinquents (a), and above all a difficulty for digital-proof criminal evidence (b).

a- The obstacles to identifying virtual delinquents, without borders

The classic methods of apprehending crime cannot be applied to Internet networks because of the volatile nature of the offenses which circulate there and the relative anonymity which reigns there. The anonymity of cybercriminals makes it very difficult to identify perpetrators. The number of holes in which cybercriminals can slip increases mechanically and the possibilities of attacks are thus greater. Preventive policies in this direction remain insufficient and states seem to lack judgment. For there to be a criminal sanction, the perpetrators of the offense must necessarily be identified and brought to justice. Putting a "*face*" on these cybercriminals is often a real technical challenge for investigators. Generally, since the author is abroad, cooperation with third countries is desirable and necessary in order to be able to challenge him [89]. In the absence of a cooperation agreement, the identification of authors located in these third countries seems ineffective. Indeed, with regard to content providers and foreign operators, the difficulties can be significant. In the case of large American operators, for example, Chadian law can come up against, like French law, the 1st amendment of the American Constitution on freedom of expression [90]. On the other hand, experiences abroad, particularly in the fight against pedophilia, have shown that the filtering operated by online investigators is ineffective. The authors, knowing that they are openly tracked, are now turning to encrypted systems, which are more difficult to detect. It results from this study that the identification of a virtual offender is not obvious. This obstacle results from the difficulties of proving virtual offenses.

b- Obstacles to the proof of virtual offenses

According to DOMAT, "*proof is what persuades the spirit of truth (...). We call proof in justice the manners regulated by the law to discover and to establish the truths of a contested fact*" [91]. With the development of digital means of investigation, the demand for truth seems more pressing. " *Digital proof is a particular method of establishing the truth which consists in having recourse to various and varied digital means which go from the study of the contents in the data of a hard disk, to electronic messages, while passing by digital recording*' [92] . However, the intangible, volatile and evolving nature of digital information constitute obstacles to its election as evidence. The legal difficulties raised by cybercrime seem to stem above all from the inadequacy of certain provisions of the Code of Criminal Procedure to crime committed on the Internet. " *The instruments available to judicial police officers in the search for evidence of offenses were not designed in times of the digital and dematerialized universe, nor even adapted to it*" [93]. Indeed, the many technical possibilities facilitate anonymity on the Internet, the erasure of data, the complexity of the facts, raise real difficulties for investigators in terms of establishing evidence. Moreover, the principle of sovereignty prohibits a State from exercising its powers outside its borders.

The result of this analysis is that by establishing personal data protection mechanisms, the legislator seems to be contributing to improving the business environment, while watching over the interests of all economic players. However, the work is not finished, efforts are still expected for effective security.

REFERNCES

1. Portalis, Preliminary speech on the draft civil code, presented on 1 st pluviôse year IX, www.senat.fr .
2. J. CARBONNIER, Civil Law T.1 Introduction, persons, families, children, couples, PUF 2017, n ° 278, p.518.
3. Following the example of minors.
4. This is the French Civil Code of 1958 applicable in Chad, by Legislative Act n ° 1 establishing the constitution of March 31, 1959 and by Constitutional Law n ° 2/62 of April 16, 1962.
5. J. CARBONNIER, op. cit ., n ° 280, p.519
6. G. CORNU, Legal vocabulary, PUF ed. 2018, p. 824
7. Ibid .
8. Including measures, regimes, devices.
9. G. CORNU, op. cit ., p. 825.
10. C. LARROUMET, Civil Law T.1 Introduction to the study of private law, Economica 1998, n ° 8, p.8.
11. M. VILLEY, Philosophy of law - definitions and purposes of law ", Bibliothèque Dalloz n ° 24, p.51.
12. Articles 431 to 438 of the penal code .
13. F. RANGEON, "Reflection on the effectiveness of law " in social uses of law, university center for administrative and political research (CURAPP), PUF 1989, p.130.
14. D. DE BECHILLON, What is a rule of law ? Odile Jaco b, 1997, p. 10.
15. F. RANGEON, op. cit ., p. 130.
16. F. ROUVILLOU, The effectiveness of standards, Reflection on the emergence of a new legal imperative, www.fondapol.org, consulted on November 2, 2020 .
17. And therefore effective.
18. E. MILLARD, General Theory of Law, Paris, Dalloz, Collection knowledge of law, 2006, p. 53.
19. D. GUGGENHEIM, " The invalidity of legal acts in Swiss and comparative law, Essay of a general theory ", Thesis University of Geneva, LGDJ Paris 1970, p.17.
20. M. PLANIOL, Basic Treaty on Civil Law, LGDJ, Paris, 1946, n ° 278, p.127.
21. A rti cle 58, preliminary draft of a Uniform Act on the general law of obligations in the OHADA area.
22. The merchants, artisans, entrepreneurs, farmers, planting, surface technicians, guards, gardeners, housekeepers ...
23. S. BRAUDO ,www.dictionary-juridique.
24. Cass. Com., December 6, 2017, appeal n ° 16-19615, BICC n ° 880 of April 15, 2018, www.actualité-juridique.com.
25. J.-L. BERGEL, General Theory of Law, Dalloz 2003, p.31.
26. Cnil, Délib. Restricted training, n ° 2011-384 of January 12, 2012.
27. CE, n ° 357 556 of March 23, 2015.
28. C. FERAL-SCHUHL, The protection of personal data, ed. Dalloz, 2019, P.47.
29. www.ritimo.org .
30. Ibid .
31. To give oneself laws.
32. E. KANT ,Doctrine of Law : "a person cannot be subject to other laws than those which he gives to himself. Any obligation of which it is not itself the source would be contrary to the dignity of the individual ".
33. The parties are free to freely determine the content of the contract, subject to respecting public order and good morals.

In principle, therefore, contractors contract on whatever they want, on the terms they choose.

34. Rapp. E. KANT : “When someone decides something with regard to another, it is always possible that he does some injustice to him ; but all injustice is impossible when he decides for himself ”.
35. The will of the parties is sufficient to give rise to the contract. It is not necessary to add any shape to it. Indeed, if it was necessary to perform certain rites for the contract to be formed, it would mean that the will is not all-powerful. It is said that the contract is formed in principle solo consensus, by the only force of the consents.
36. G. RIPERT, The democratic regime and modern civil law, LGDJ, 1936, n ° 137, p. 269, quoted by C. PERES, in " Contractual freedom and public order in the project to reform the contract law of the chancellery " (concerning article 16, paragraph 2, of the project), Recueil Dalloz 2009 p.381.
37. A.-M. DEMANTE, Cours analytique de Code civil, t. I, G. Thorel Libraire-éditeur, Paris, 1849, n ° 12 bis, p. 55, quoted by Cécile Pérès, in " Contractual freedom and public order in the project to reform the contract law of the chancellery " (regarding article 16, paragraph 2, of the project), Recueil Dalloz 2009 p .381.
38. LOCRE, The civil, commercial and criminal legislation of France, or commentary and complement of the French Codes, t. I, Treuttel and Würtz, Paris, 1828, p. 302, quoted by C. PERES, in " Contractual freedom and public order in the project to reform the contract law of the chancellery " (regarding article 16, paragraph 2, of the project), Recueil Dalloz 2009 p.381.
39. JM MOUSSERON, “A starting principle : contractual freedom ” ,in New spaces for contractual freedom, Cah. dr .entr. 1995/2. 5 s, quoted by C. PERES, in " Contractual freedom and public order in the project to reform the contract law of the chancellery " (regarding article 16, paragraph 2, of the project), Recueil Dalloz 2009 p.381.
40. J. CARBONNIER, Civil Law T.2 goods, obligations, PUF ed. 2017, p.1945, n ° 931.
41. Freedom of contract.
42. G. CORNU, Legal vocabulary, PUF 2018, p.1036.
43. The author.
44. Having cause.
45. Example, the transfer of ownership resulting from the sale.
46. The transfer act.
47. G. CORNU, op. cit ., p.1036.
48. J. CARBONNIER, op. cit ., p. 1945.
49. G. CORNU op. cit.,p. 629.
50. M. KETTANI, Legal regime for the protection of personal data, www.dlapiper.com (04).
51. M. KETTANI, op. cit ., (03).
52. L. CORNELIS, The good faith : development or sprain to the autonomy of the will, in the good faith, ed. Young Bar of Liège, 1990, p.35.
53. JJ FAGNART, The execution in good faith of agreements : an expanding principle, note under cass. September 19, 1983, RCJB 1986, p.295-308.
54. D. MAZEAUD, “Loyalty, solidarity, fraternity : the new contractual motto ? »In Mélanges in honor of F. TERRE, Dalloz-PUF J-Cl ., 1999, p.603.
55. A. SERIAUX, Les obligations, Paris, PUF, coll. “Fundamental right ” 2006, n ° 55.
56. JV ZUYLEN, Faults, good faith and abuse of rights : convergences and divergences, Annales de Droit de Louvain, vol.71, 2011, n ° 3, p.269.
57. C. FERAL-SCHUHL ,op. cit ., p.52.
58. For example, in insurance law, insureds have a duty to spontaneously inform the insurer about events specific to him.
59. Quoted by J. CARBONNIER, op. cit ., n ° 1030, p.2119
60. J. MESTRE, RT 86, p.101 ; Y. PICOD, JCP 88, 1, p. 3318.
61. C. THIBIERGE -GUELFUCCI, free speech, on the transformation of contract law, RT 97, 382.
62. Y. PICOD, The obligation of cooperation in the execution of the contract, JCP 1988.I.3318.
63. F. TERRE and others, Civil law Les obligations, Dalloz ed. 2009, n ° 441, p.459.
64. Concession contracts, franchise, exclusive supply contract, engineering, technology transfer, factoring, etc.
65. J. MESTRE, obs. RTD Civ. 1986, 101 ; J.-M. LELOUP, the creation of contracts through commercial practice, in the contemporary evolution of contract law, René SAVATIER day 1985, p.167 et svts ; L. AYNES, Dalloz 1993, chron. P.25.
66. Article 7 of Law n ° 007 / PR / 2015.
67. CNIL Delib, limited training, No. 2015-155 of 1. St June 2015 imposing a financial penalty against the company Prisma Media ; CNIL, June 12, 2015 and CNIL, Décis. N ° MED-2017-075 of Nov. 27, 2017.
68. CINIL, Délib ., N ° SAN-2019-001 of Jan. 21, 2019.
69. J. CARBONNIER, “Legal sociology ”, ed. A. COLIN, 1972.
70. R. GASSIN. "The criminal law of computer science ", Dalloz Sirey 1986, chron.35.
71. International Multilateral Partnership Against Cyber Threats.
72. European Network and Information Security Agency, the European Network and Information Security Agency.
73. Organization for Economic Co-operation and Development .
74. www.latribune.fr.
75. Case Cahuzac, Wildenstein, Fillon, etc.
76. C. LARROUMET, op. cit ., n ° 1, p. 5.
77. S. Ghernaouti " for cyber security and a cyber defense at the level of challenges facing Switzerland " RMS 2 March-April, 2015, p.7.
78. www.france24.com.
79. These include the health, energy, water and food sectors, telecommunications and even finance.
80. Announced in 2017 at the 4th edition of the Dakar International Forum on Peace and Security in Africa, the school of fight training against cybercrime will put just a year to be created. Provisionally installed in Dakar, in the premises of the National School of Administration (ENA) of Dakar, it should subsequently be moved to Diamnadio, a new town under construction about thirty kilometers from the Senegalese capital.
81. R. BOOS ,op. cit.,p. 184.
82. F. DINOIS, “The solidarity of legislative and jurisprudential competence in international criminal law ”, Thesis, Jean Monnet University, Paris, 2012-2013, p.13.
83. ICJ, April 11, 1949, case of damages suffered in the service of the United Nations, ICJ. Rec. 1949.
84. R. BOOS ,op. cit ., p. 185.
85. K. GACHI, “Universal jurisdiction ”, DEA Criminal law and penal sciences, University Panthéon-Assas, Paris II, 1999-2000, p. 41.
86. Crim. March 21, 1862, Sirey 1862.I.542, Faustin HELIE report, concl. SAVARY.
87. Article R. 645-1 of the penal code.
88. R. BOOS ,op. cit.,p. 187.
89. R. BOOS ,op. cit ., p. 199.
90. Yahoo judgment, supra.
91. J. DOMAT, " Civil laws in their natural order ", Paris, ed. Cavelier, t.1 1771, p. 204.
92. CNEJITA, " Digital proof to the test of litigation ", Colloquium of April 13, 2010 at 1 st ch. of the Paris CA, p. 11.
93. M. TABAROT, Report n ° 608 (2 nd part) on bill n ° 528 for confidence in the digital economy (2013).

****