CONFERENCE AFRICAINE SUR LA REGULATION ET L'ÉCONOMIE NUMERIQUE (CAREN) 2018

16-18 OCTOBRE 2018 – OUAGADOUGOU (BURKINA FASO)

PROJET DE COMMUNICATION SUR LA PROTECTION (OU LA VIOLATION ?) DES DONNEES A CARACTERE PERSONNEL A TRAVERS LES SERVICES FOURNIS PAR DEUX OPERATEURS MAURITANIENS DE COMMUNICATIONS ELECTRONIQUES

- PROJET INSPIRE PAR DES FAITS REELS S'ETANT DEROULES COURANT JUIN / JUILLET 2018 –

Présenté par Mamadou Alpha KANE,

Chef du Département Juridique de l'Autorité de Régulation Multisectorielle de Mauritanie

1ère Promotion Mastère Spécialisé de l'Economie et des Contenus Numériques

THEME : Piratage du compte de messagerie électronique d'un citoyen ; Cas d'une triple transgression :

1. **Violation par le pirate des données à caractère personnel de l'abonné (Loi sur les données personnelles et loi sur la cybercriminalité) ;**
2. **Manquement des opérateurs impliqués à leurs obligations légales (Loi sur les communications électroniques et Loi sur la protection des DP) ;**
3. **Manquements par omission(s) du régulateur sectoriel**

EXPOSE ET RECONSTITUTION DES FAITS

Un imposteur, qui a pu mettre la main sur le passeport expiré de son cousin, a réussi à se faire réattribuer les 2 numéros de téléphones de ce dernier dont il a ensuite fait usage aux fins de pirater sa messagerie électronique.

Voici le déroulement chronologique des faits :

+ Voyage de l'abonné, jeune homme d'affaires mauritanien, qui s'est longtemps absenté de Nouakchott pour les besoins de ses activités ;

+ Présentation d'un individu (le cousin de l'abonné) chez le 1er opérateur de la victime (opérateur A), muni du passeport expiré de cette dernière, où il déclare la perte de sa carte SIM, dans le but de se faire réattribuer le même numéro (le numéro de la victime) ;

***(N.B. :** La procédure normale consiste en la présentation, par le titulaire de carte SIM lui-même, d'un document officiel en cours de validité confirmant son identité)*

+ Scénario similaire auprès du second opérateur de la victime (opérateur B), à la différence que cette fois-ci, l'individu en question n'a présenté aucune pièce d'identité, ayant tout bonnement bénéficié de la complaisance, pour ne pas dire de la complicité d'un agent de l'opérateur, qu'il connaissait et qui a accepté de réactiver, à sa demande, pour le compte de son cousin, le numéro de la victime déclaré perdu et ce, sans procéder à la moindre vérification ni quelconque formalité ;

+ Une fois en possession des deux nouvelles cartes SIM associées aux numéros de l'homme d'affaires en déplacement, son cousin – appelons le "le pirate" – a procédé au piratage du compte Gmail (google) de l'abonné, de la manière la plus simple :

En entrant, d'abord, dans Gmail pour y déclarer la perte de son mot de passe et en lançant, ensuite, la procédure automatique de récupération de mot de passe par envoi (par Gmail), d'un nouveau mot de passe sur celui des 2 numéros de sécurité (numéros de l'abonné) que le véritable titulaire du compte avait enregistré sur Gmail.

C'est ainsi que notre pirate a non seulement littéralement "aspiré" le compte Gmail de son cousin, accédant à toutes ses correspondances avec ses partenaires d'affaires, mais a passé avec ces derniers, d'après la victime plaignante, nombre de transactions à son propre profit.

Remarque : La victime, qui bénéficiait d'un service de roaming sur ses 2 numéros, a constaté, étant toujours à l'étranger, que d'abord, ces derniers n'étaient plus fonctionnels à son niveau et qu'ensuite, toutes ses tentatives pour se connecter sur Google aboutissaient à des échecs, ce qui lui a mis la puce à l'oreille.

Rentré à Nouakchott, il s'est donc rapproché de ses opérateurs et de l'Administration Centrale pour, respectivement :

- faire "griller" les puces ayant servi au piratage et récupérer ses numéros ;
- s'adjoindre les services d'un expert "IT" agréé auprès des tribunaux dans le but de récupérer son compte de messagerie piraté ;
- Et saisir l'Autorité de Régulation chargée des communications électroniques (ARE) pour déposer une plainte officielle.

Qu'a fait le régulateur ?

Il a, dans un premier temps, adressé aux 2 opérateurs impliqués un courrier relatant la version du plaignant et demandant à chacun d'entre eux de diligenter une enquête interne pour faire la lumière sur les faits.

Entre temps, un accord étant intervenu entre la famille du pirate et celle du plaignant, ce dernier est revenu vers le régulateur pour lui notifier le retrait de sa plainte et ce, au moment même où l'un des opérateurs était sur le point de licencier ses deux (2) agents qui s'étaient rendus coupables du forfait (réattribution illégale du numéro du plaignant au tiers "pirate").

L'Autorité de Régulation a ensuite adressé un 2ème courrier aux opérateurs pour les informer du retrait de la plainte et leur demander de prendre des mesures disciplinaires pour éviter que de tels agissements se produisent à nouveau ; l'affaire a été classée sans suite.

ANALYSE DE LA GRAVITE ET DE LA PORTEE DES FAITS AU REGARD DE LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

L'étonnante facilité avec laquelle les moyens d'intrusion dans le compte de messagerie du plaignant (cartes SIM d'autrui) ont pu être obtenus, mais aussi et surtout l'issue - pour le moins déconcertante - "heureuse" de l'affaire, constituent un exemple éloquent de la menace et des risques qu'une numérisation "sauvage" de l'économie et de la société peuvent représenter, non seulement pour la sécurité patrimoniale et économique d'un individu mais également pour la protection de sa vie privée et de ses données personnelles.

Par numérisation "sauvage", nous entendons principalement deux (2) choses :

- D'abord, l'accomplissement de transactions numériques qui ne soient pas strictement encadrées en amont, au plan légal et règlementaire, puis, sanctionnées, en aval, en cas d'infraction à la législation en vigueur ;
- Et, ensuite, tout défaut, toute défaillance ou toute insuffisance de protection de la "vie numérique" d'un individu, à l'occasion d'un quelconque traitement[1] de donnée à caractère personnel, à fortiori lorsque ce traitement concerne un sujet aussi délicat que l'identification des abonnés auprès d'opérateurs de communications électroniques.

La thématique du cas d'espèce objet de la présente communication soulève donc une triple problématique en ce sens qu'en dehors de la violation manifeste de données personnelles qu'il met à jour (le piratage d'une messagerie), il nous interroge à la fois sur la confiance que les citoyens peuvent accorder à leurs opérateurs de communications électroniques, lorsque ceux-ci agissent en infraction de la règlementation régissant leur secteur (dispositions de la Loi sur les communications électroniques ayant vocation à assurer la protection des consommateurs) mais, pire encore, sur l'opportunité et le bien-fondé de la décision d'un régulateur de classer un cas "irrégulier" de traitement de données personnelles, quand il est confronté à un retrait de plainte de la personne victime de violation de donnée(s).

L'utilisation frauduleuse du passeport du concerné et celle de ses cartes SIM aux fins de piratage constituant le point de départ et les infractions centrales de la thématique objet de

[1] Constitue notamment un traitement de donnée à caractère personnel : la consultation, la collecte, la diffusion, la communication, la modification, l'utilisation, la mise à disposition, l'interconnexion, le transfert, le verrouillage, l'effacement ou la destruction de cette donnée.

la présente discussion, nous prenons la liberté de présenter le cadre légal applicable aux dites infractions (1) avant de revenir sur l'infraction connexe engageant la responsabilité de chacun des opérateurs qui ont, à cette occasion, enfreint leur propre règlementation sectorielle ainsi que celle qui encadre les données personnelles (2) et de finir par la position, ou, plutôt, ce qui aurait dû, à notre sens, être la position du régulateur face au casse-tête juridique dans lequel il s'est malencontreusement retrouvé (3).

1. LA VIOLATION PAR LE PIRATE DES DONNEES A CARACTERE PERSONNEL DE L'ABONNE

Rappelons que le pirate s'est doublement servi des données d'identification de la victime :

- une première fois, auprès de l'un des opérateurs de téléphonie mobile de cette dernière (présentation de documents d'identité appartenant à autrui pour la réactivation du numéro dont il voulait faire usage) ;
- et, une seconde fois, pour accéder au contenu de la messagerie personnelle qu'il a piratée.

Il a donc, par conséquent, pu disposer à la fois d'informations sur des aspects de la vie privée du piraté (courriers personnels, fichiers de diverses natures) et d'informations et / ou documents spécifiques à sa vie professionnelle.

Au plan juridique, les agissements du pirate tombent, par conséquent, aussi bien sous le couperet de la loi sur les données personnelles que sous celui de la loi sur la cybercriminalité.

1.1 – Les infractions à la loi sur les données personnelles

La violation des données personnelles de la victime s'est tout d'abord légalement matérialisée par la réalisation de quatre (4) actes condamnables :
- usurpation d'identité (possession et utilisation illégales de documents d'autrui)
- recel de vol (retrait et possession de biens (cartes SIM) issus d'un acte frauduleux)
- piratage (accès illégal à la messagerie d'autrui)
- Escroquerie (avantages tirés ou escomptés du piratage auprès des partenaires de la victime).

En se référant à la définition d'un traitement de donnée à caractère personnel, il est aisé d'établir qu'en dehors du recel, tous ces actes ont été commis en infraction d'au moins trois

(3) dispositions de la Loi N ° 2017-020 du 22 juillet 2017 portant sur la protection des données à caractère personnel :

- L'article 5, qui consacre, sauf dérogation légale[2], le principe de base en vertu duquel tout "traitement des données à caractère personnel effectué sans le consentement de la personne concernée est interdit" ;

- L'article 6, qui précise que tout traitement d'une donnée personnelle doit "se faire de manière licite, loyale et non frauduleuse" ;

- Et l'Article 37, qui subordonne tout traitement de DP portant sur un quelconque numéro d'identification ainsi que tout traitement de donnée personnelle occasionnant une interconnexion de fichiers à l'autorisation préalable de l'Autorité de Protection des Données à caractère personnel.

2.2 – Les infractions à la loi sur la cybercriminalité

Pas moins de neuf (9) articles de la Loi N ° 2016-007 du 20 janvier 2016 relative à la cybercriminalité incriminent ensuite les agissements du pirate et prévoient les sanctions devant lui être infligées ; Il s'agit de ses articles 2, 3, 9, 10, 13, 14, 25, 28 et 29.

- L'article 2 énonce d'emblée que la loi sur la cybercriminalité "porte sur les crimes et délits liés à l'usage des Technologies de l'Information et de la Communication" ;

- L'article 3 précise, pour compléter la disposition précédente, que les pouvoirs et procédures prévus par ladite loi s'appliquent non seulement aux infractions spécifiques qu'elle a listées, mais également à toutes les autres infractions pénales commises au moyen d'un système informatique ainsi qu'à la collecte des preuves électroniques de toute autre infraction pénale ;

- L'article 9 fixe les peines (emprisonnement de 2 à 4 ans et amende de 200 000 à 3 000 000 MRO) applicables à l'introduction ou la tentative d'introduction intentionnelle "et sans droit", de données informatiques dans un système informatique ;

[2] Les 4 dérogations prévues par la Loi sont : le traitement d'une DP répondant à une obligation légale (1), le traitement d'une DP nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique (2), le traitement d'une DP nécessité par l'exécution d'un contrat liant la personne concernée (3) et le traitement d'une DP nécessaire à la sauvegarde de l'intérêt ou des droits et libertés fondamentaux du concerné (4).

- L'article 10 établit la confusion entre les peines applicables à la seule production, vente, utilisation ou mise à disposition d'un dispositif ou d'un programme informatique destiné à commettre une cyber infraction (mot de passe, code d'accès notamment) avec celles prévues pour la commission de l'infraction elle-même ;

- L'article 13, qui traite des infractions informatiques, détermine les peines auxquelles s'expose quiconque porte préjudice à autrui par un quelconque traitement de donnée informatique ainsi que l'auteur de toute forme d'atteinte non autorisée au fonctionnement d'un système informatique en vue d'en retirer un bénéfice économique pour soi-même ou pour autrui (2 à 5 ans de prison et 500 000 à 3 000 000 MRO) ;

- L'article 14, relatif aux infractions se rapportant aux contenus, sanctionne les atteintes à la propriété intellectuelle et aux droits connexes, commises délibérément dans un but commercial, au moyen d'un système informatique (1 à 3 ans d'emprisonnement et amende de 100 000 à 2.000.000 d'ouguiyas) ;

- L'article 25, qui vise particulièrement les faits qui nous intéressent, définit les peines à infliger à quiconque usurpe, sur un système informatique ou tout support technique, l'identité d'une personne physique, morale, ou d'une autorité publique dans le but, soit d'en tirer un profit ou bénéficier d'une faveur quelconque, pour soi-même ou pour autrui, soit de porter préjudice à la personne dont l'identité est usurpée, soit en vue de commettre ou faciliter la commission d'une cyber infraction (1 mois à 1 an de prison et amende de 100 000 à 600 000 MRO) ;

- L'article 28, qui concerne les infractions portant atteinte aux biens, établit les peines applicables à quiconque reproduit intentionnellement et sans droit, des données informatiques au préjudice d'autrui (1 à 3 ans d'emprisonnement et amende de 100 000 à 2 000 000 MRO) ;

- L'article 29, enfin, indique les sanctions à requérir à l'endroit de quiconque reçoit, intentionnellement et sans droit, des données informatiques personnelles, confidentielles ou celles qui sont protégées par le secret professionnel, en usant de manœuvres frauduleuses quelconques ou en faisant usage de faux noms ou qualités (1 à 3 ans d'emprisonnement et amende de 100 000 à 2 000 000 MRO).

2. MANQUEMENT DES OPERATEURS IMPLIQUES A LEURS OBLIGATIONS LEGALES (LOI SUR LES COMMUNICATIONS ELECTRONIQUES ET LOI SUR LA PROTECTION DES DONNEES A CARACTERE PERSONNEL)

Les opérateurs impliqués se sont rendus coupables d'un double manquement à leurs obligations légales : à celles, d'abord, que met à leur charge leur propre Loi sectorielle (Loi sur les communications électroniques) et, ensuite, à celles que leur enjoint la Loi sur la protection des données à caractère personnel.

a – Obligations des opérateurs prévues par la loi sectorielle

La Loi N ° 2013-025 du 15 juillet 2013 portant sur les communications électroniques a mis en place un certain nombre de dispositions concourant toutes à la protection des utilisateurs de réseaux et de services de communications électroniques.
C'est ainsi que le chapitre XII de cette loi, relatif aux "droits et protections des utilisateurs de réseaux et services de communications électroniques" (articles 83 à 100), comprend une première section, intitulée "Vie privée" (articles 83 à 89) et une seconde section entièrement réservée au "traitement des données à caractère personnel" (articles 90 à 95).

Du point de vue des obligations afférentes à la vie privée de leurs abonnés, les opérateurs ont enfreint celle qui est édictée par l'article 83 au terme duquel les opérateurs et leurs employés doivent prendre toutes les mesures utiles pour assurer la protection de la vie privée et des données nominatives des usagers[3] .

Pour en revenir aux obligations des opérateurs en matière de traitement de données à caractère personnel, la section qui y est consacrée commence par l'article 90 qui, sans la moindre équivoque, précise que toutes les dispositions de ladite section s'appliquent "notamment aux réseaux qui prennent en charge les dispositifs de collecte de données et d'identification", autrement dit aux opérateurs, entre autres acteurs du monde des communications électroniques !

Or au terme de l'article 93, alinéa 1er, **les opérateurs ne sont autorisés à transmettre des données personnelles de leurs abonnés qu'à des tiers directement concernés par la facturation ou le recouvrement de leurs services** de communications électroniques.

[3] Sous réserve, bien entendu, des obligations relatives aux prescriptions exigées par la Défense Nationale et la Sécurité Publique et les prérogatives de l'autorité judiciaire.

L'alinéa 2 de cet article édicte, en outre, en guise de précision complémentaire, que les opérateurs ne peuvent réaliser de traitement de données relatives au trafic qu'en vue de commercialiser leurs propres services de communications électroniques ou des services à valeur ajoutée et ce, avec l'accord exprès de leurs clients, ce qui ne laisse aucun doute sur leur non habilitation à transmettre de quelconques données personnelles de leurs clients, sans le consentement de ces derniers, à des tiers.

L'article 95 in fine, enfin, dispose de manière très claire, que les opérateurs prennent toutes les mesures nécessaires pour empêcher une utilisation des données relatives aux utilisateurs de leurs services à des fins autres que celles prévues par :

- L'article 91 (trafic de données et réponses aux autorités compétentes)
- L'article 92 (recherche, constatation et poursuite des infractions pénales, ordre public, défense nationale et sécurité publique)
- L'article 93 (facturation et recouvrement des prestations de l'opérateur, commercialisation de ses propres services).

En résumé, nous pouvons soutenir que les opérateurs impliqués sont responsables d'une faille de sécurité (accès non autorisé à des données) qui a eu pour conséquence la violation des quatre (4) principes universels qui président à tout traitement de DP :

- Le principe de légalité : La réactivation des cartes SIM est illégale, ne serait-ce qu'au regard des conditions exigées par la Loi sur les communications électroniques, qui n'ont pas été respectées ;

- Le principe de finalité : Le pirate s'étant procuré des cartes à puces sur lesquelles ont été activées les numéros de la victime dans l'intention d'accéder au compte de messagerie de ce dernier, il n'est nul besoin de revenir sur le caractère illicite et délictuel du piratage opéré ;

- Le principe de légitimité : La victime étant l'abonné, donc, le co-contractant exclusif des opérateurs, elle est légitimement la seule personne à pouvoir suspendre, résilier ou faire réactiver l'abonnement auquel elle a souscrit auprès de ses opérateurs fournisseurs de services ;

- Le principe de proportionnalité : Le piratage est non seulement en lui-même excessif, mais il piétine complètement les droits et libertés fondamentaux de la victime.

b – Obligations des opérateurs prévues par la loi sur la protection des données personnelles

Plusieurs dispositions de la Loi N ° 2017-020 sur la protection des données à caractère personnel visent implicitement les opérateurs de communications électroniques, même si elles ne les citent pas nommément.

Il s'agit, tout d'abord, de son article 10, qui dispose, relativement aux obligations de sécurité, "que les données à caractère personnel sont traitées de manière confidentielle et sont protégées"…. "notamment lorsque le traitement comporte des transmissions de données dans un réseau".
A ce sujet, certains pourraient soutenir, peut-être à raison, que la remise d'une carte SIM ne constitue pas en soi une transmission de données dans un réseau ; nous pouvons comprendre un tel raisonnement.
Mais de notre point de vue, il ne faut pas perdre de vue deux (2) aspects aux implications juridiques inéluctables, si l'on garde bien à l'esprit la définition légale[4] donnée aux traitements de données personnelles :

- Les services d'exploitation technico-commerciale des opérateurs étant entièrement informatisés, la simple consultation de leurs bases de données, pour vérifier l'exactitude des informations concernant un abonné ou l'exécution des commandes informatiques servant à enclencher le processus de réactivation d'une carte SIM – opérations constituant toutes deux des traitements de DP - nécessitent la transmission des données relatives à ce client ou à la puce à réactiver dans leur réseau ;

- A supposer que la remise d'une carte de SIM au pirate ne constitue factuellement pas ou n'implique pas en elle-même une transmission de données sur le réseau d'un opérateur donné, il n'en demeure pas moins que la commission de cet acte constitue une infraction qui vise et rend possible la réalisation d'une infraction autrement plus grave – le piratage d'une

[4]Consultation, collecte, diffusion, communication, modification, utilisation, mise à disposition, interconnexion, transfert, verrouillage, effacement ou destruction, par exemple.

messagerie électronique – qui, lui, pour reprendre la terminologie de l'article 10 précité, est un traitement qui "comporte" forcément "des transmissions de données dans un réseau".

La seconde disposition de la Loi sur les DP qui vise les opérateurs résulte de l'article 37 qui énonce, lui, que parmi six (6) autres catégories de scénarios possibles, ne peut être mis en œuvre un traitement de donnée à caractère personnel portant sur un numéro national d'identification ou tout autre identifiant de portée générale qu'après autorisation de l'Autorité de Protection des Données à caractère personnel (Régime de l'Autorisation).

La troisième et dernière règle du même texte, qui pointe du doigt les opérateurs, découle de l'article 47, qui dispose que le responsable du traitement (dans notre cas l'Administration de l'opérateur) doit prendre toutes les dispositions utiles :

- non seulement pour empêcher tout accès, par des tiers non autorisés, à des données traitées ;

- mais également pour garantir que puisse être vérifiée et constatée, à postériori, l'identité des personnes ayant eu accès au système d'information et savoir quelles données ont été lues ou introduites dans le système, à quel moment et par quelle personne ;

- et, enfin, garantir que puisse être vérifiée et constatée l'identité des tiers auxquels des données à caractère personnel peuvent être transmises.

3. MANQUEMENT(S) PAR OMISSION(S) DU REGULATEUR SECTORIEL A 3 LOIS : SA LOI SECTORIELLE, LA LOI SUR LES DONNEES PERSONNELLES & LA LOI RELATIVE A LA CYBERCRIMINALITE

C'est l'Autorité de Régulation Multisectorielle (ARE), créée par la Loi N ° 2001-18 du 25 janvier 2001, qui est chargée, en Mauritanie, de la régulation du secteur des communications électroniques et doit veiller, entre autres :

- au respect, par les opérateurs de communications électroniques, des dispositions de la Loi sectorielle (Loi N ° 2013-025 portant sur les communications électroniques) et de celles de ses textes d'application ;
- à la protection des intérêts des utilisateurs et des opérateurs du secteur, conformément aux dispositions législatives et règlementaires ;

- et à la stricte exécution des cahiers des charges des opérateurs de communications électroniques.

Ces précisions étant apportées, l'attitude du régulateur (sommation d'enquête suivie d'un classement de l'affaire) met certes en lumière, de prime abord, une réalité consistant en un manquement par rapport à certaines de ses obligations (a), mais une analyse plus poussée des faits et des différents textes de lois peut cependant venir tempérer, voire justifier ou, à tout le moins, tenter d'expliquer le paradoxe du choix qu'il a opéré (b) ; se posera alors la question de savoir si le régulateur, avant de classer l'affaire, a épuisé, ou au moins exploré toutes les voies de sorties possibles au dilemme factuel et juridique dans lequel il s'est retrouvé (c).

a – Les manquements par omission(s) en question

Il conviendrait peut-être de rappeler, à ce stade, qu'en droit pénal, contrairement à une idée très répandue au sein de la plupart des personnes non averties en la matière, la commission d'une infraction ne s'accomplit pas forcément de manière active (poser un acte réprimé par la Loi).
En effet, l'inaction (le fait de rester passif alors que la situation qui se présente exige justement d'agir) suffit à réaliser, consommer une infraction ; c'est ce que l'on appelle une "infraction par omission" à l'image, en guise d'illustration, de la "non-assistance à personne en péril", qui est condamnée par tous les dispositifs pénaux du monde.

Il ne fait donc aucun doute qu'en ne sanctionnant pas les opérateurs impliqués et qu'en ne posant aucun acte devant aboutir à la sanction du pirate, qui n'a été ni poursuivi, ni, du reste, même été inquiété, le régulateur a méconnu à la fois des dispositions de sa loi sectorielle et des dispositions d'autres textes législatifs, dont nous ferons ici l'économie, mais sur lesquels nous reviendrons plus bas, au point (c) consacré aux mesures que, à notre sens, il aurait dû prendre.

a.1 – Les manquements par omission(s) à la Loi sur les communications électroniques

Bien que la loi mauritanienne sur la protection des données à caractère personnel date seulement de 2017, le régulateur sectoriel - l'ARE - a eu le mérite, lors du bilan de la réforme du secteur des communications électroniques qu'il a initié courant 2012, d'avoir, à l'occasion

de la mise à jour de l'ancienne loi de 1999, anticipé sur certaines thématiques, qui n'avaient pas été prises en compte à l'époque, pour les intégrer dans le nouveau corpus légal, notamment en matière :

- d'obligations d'information ;
- de renforcement des pouvoirs de sanction du régulateur ;
- et, encore plus important, de droits et moyens de protection des utilisateurs de réseaux et services de communications électroniques, concepts qui ont fait, comme déjà indiqué plus haut, l'objet de tout un chapitre consacré à la vie privée, au traitement des données à caractère personnel et à l'information des utilisateurs.

Cela dit, l'article 6 de la loi nouvelle sur les communications électroniques (Loi N° 2013-025) dispose ainsi, en substance, que c'est à L'Autorité de Régulation qu'il revient de veiller au respect de toutes les dispositions qu'elle édicte et de celles de ses textes d'application et qu'à ce titre, cet organe doit :

- contrôler le respect, par les opérateurs, des prescriptions résultant des dispositions législatives et réglementaires qui leurs sont applicables ainsi que celui des obligations afférentes aux licences et autorisations dont ils bénéficient ;
- prendre les mesures nécessaires pour protéger les intérêts des utilisateurs ;
- et sanctionner les manquements des opérateurs à leurs obligations ;

De façon plus concrète, le régulateur a donc méconnu, dans le traitement de cette affaire :

- L'article 83 de la loi sur les communications électroniques, qui vise les mesures que les opérateurs doivent prendre pour assurer la protection de la vie privée et des données nominatives des usagers ;
- L'article 47 du même texte, qui interdit aux opérateurs tout accès par des tiers non autorisés à leurs bases de données.

a.2 – Les manquements par omission(s) à la Loi relative à la cybercriminalité

Il a été signalé plus haut que les agissements du pirate répondaient à la qualification légale d'une cyber infraction (voir point 2.2).

Il résulte donc de cet état de fait et du sacro-saint adage "NEMO CENSETUR IGNORARE LEGEM" ("Nul n'est censé ignorer la loi) que le régulateur, en ne posant pas les actes concourant à ce que le pirate réponde de son forfait, n'a tenu compte :

- Ni des dispositions de l'article 3 de la Loi relative à la cybercriminalité, qui fait rentrer dans son champ d'application aussi bien certaines infractions déterminées que toutes les autres infractions pénales commises au moyen d'un système informatique ;

- Ni des autres nombreuses dispositions de la même loi qui traitent, d'une part, de toutes les peines applicables aux infractions contre la confidentialité et l'intégrité des données, aux infractions se rapportant aux contenus, aux biens, à la responsabilité des personnes morales pour les infractions commises par leurs agents et, d'autre part, de la compétence des juridictions en la matière.

b – Le paradoxe juridique et factuel ou blocage hypothétique

Bien que strictement analysée, la décision du régulateur, de classer l'affaire, a été prise au mépris des dispositions ci-dessus évoquées, il n'en demeure pas moins que son attitude peut cependant s'expliquer par :

- un paradoxe juridique posé par la juxtaposition, le rapprochement ou la combinaison de certaines dispositions contradictoires de la Loi sur les communications électroniques ;

- certains éléments factuels tenant à la fois aux principes sous-tendant la mission du régulateur et à un vide institutionnel et juridique patents en matière de protection des données à caractère personnel.

b.1 – Le Paradoxe juridique susceptible de constituer un blocage à l'action du régulateur

Une lecture attentive de la Loi sur les communications électroniques permet de soulever une contradiction entre certaines de ses dispositions relatives aux prérogatives du régulateur en matière de recevabilité et de traitement des plaintes.

Il s'agit, notamment, des articles 81 et 82 de ce texte.

L'article 81 dispose, en effet, que l'Autorité de Régulation ne peut directement recevoir des plaintes et arbitrer des différends en première instance entre un opérateur et des utilisateurs, la condition, pour ce faire, étant que lesdits utilisateurs :

- soit, jouissent de la personnalité morale ;
- soit, soient représentés par un groupe organisé, une association d'utilisateurs ou par une autorité compétente (élus, autorité administrative, etc.).

Il va de soi qu'aucune de ces deux conditions n'est remplie dans le cas d'espèce, puisque le plaignant a agi seul et pour la défense de ses propres intérêts.

Mais la contradiction provient de l'article 82 qui, lui, dote l'ARE du pouvoir de sanctionner tout manquement qu'elle constate de la part des opérateurs et ce, soit d'office, soit à la demande du Ministre, d'une organisation professionnelle, d'une association d'utilisateurs ou d'une personne physique ou morale concernée.

La remarque que cet article appelle de notre part est que nous ne voyons pas très bien la différence, tant la frontière est floue, entre la recevabilité d'une plainte contre un opérateur qui serait déposée par un utilisateur agissant isolément (démarche non prévue par la Loi) et la prononciation d'une sanction à l'encontre d'un opérateur auteur d'un manquement à la requête de ce même utilisateur.

Le régulateur s'est-il fondé sur cet article 82 pour demander aux opérateurs impliqués de mener une enquête et situer les responsabilités ? Vraisemblablement oui, même si, au final, cette procédure n'a pas été suivie d'effet.

b.2 – Eléments factuels inhérents aux principes de régulation et aux vides institutionnel et juridique en matière de protection des données à caractère personnel

A la décharge du régulateur, deux (2) faits que l'on ne peut purement et simplement ignorer : Son action est guidée par certains principes et il peut arriver que celle-ci soit contrecarrée par un vide aux plans institutionnel et juridique.

b.2.1 – Principes directeurs et philosophie du régulateur

Même si cela peut paraître "léger" comme argument, il ne faut tout de même pas oublier que le régulateur, de par la nature et les objectifs de sa mission, est plus un conciliateur et un arbitre qu'un "punisseur", ce qui n'enlève cependant rien à son rôle de gendarme du secteur, devant sévir lorsque les circonstances l'exigent.
Nous gageons donc qu'à la suite du retrait de plainte de la victime du piratage, notre régulateur a, de bonne foi, saisi cette occasion qui lui a été ainsi été offerte d'éviter de sanctionner les opérateurs concernés.

b.2.2 – Vides institutionnel et juridique en régulation des données personnelles

Il existe d'abord un premier vide institutionnel patent en matière de protection des données personnelles, puisque l'Autorité de Protection des Données à Caractère Personnel, dont la création est légalement prévue par l'article 64 de la Loi N° 2017-020 portant sur les données personnelles, n'a toujours pas, à ce jour, été mise sur pied[5].

Or, selon l'article 73 de ladite loi, c'est cette Autorité de Protection qui est compétente en matière d'infractions portant sur des données personnelles, puisque c'est elle qui :

- "reçoit les réclamations, les pétitions et les plaintes relatives à la mise en œuvre des traitements des données à caractère personnel et informe leurs auteurs des suites données à celles-ci " ;
- " informe sans délai le procureur de la République des infractions dont elle a connaissance et peut ester en justice" en cas de violation de la loi sur les données personnelles ;
- prononce les sanctions à l'égard des responsables de traitement.

Il subsiste également un vide juridique, découlant de l'article 99 de la Loi sur la protection des données à caractère personnel, qui octroie un délai de deux (2) ans pour se conformer à ladite loi, à compter de son entrée en vigueur.
Le triste constat à faire est donc, que puisque la loi a été promulguée le 22 juillet 2017, il y a fort à redouter qu'énormément de traitements de données à caractère personnel

[5]Il n'en demeure pas moins que la Loi 2017-020 est tout de même en vigueur et a donc vocation à règlementer le domaine, la question se posant alors étant par quelle institution !?

échapperont probablement à son empire et ce, durant toute la période restant à courir jusqu'au 21 juillet 2019.

c - Ce qu'aurait dû être la suite à donner

Après s'être un moment "mis dans la peau" du régulateur pour tenter de trouver une explication cohérente à sa démarche, l'épilogue, pour ne pas dire le fin mot de cette discussion, réside dans la question de savoir ce qu'aurait pu, voire aurait dû faire le régulateur pour, à défaut de sanctionner les opérateurs, au moins ne pas laisser impunis les agissements du pirate, qui se révèlent être d'une extrême gravité au vu des enjeux et conséquences pour la victime.

Pour répondre à cette interrogation, nous rappellerons qu'une infraction pénale suppose la réunion de trois (3) éléments, à savoir l'élément légal, l'élément matériel et l'élément moral ou intentionnel.
A partir du moment où l'utilisation d'un document d'identité et le piratage de données appartenant à autrui dans le dessein d'en faire un usage illicite, qui sont prévus et réprimandés par la loi pénale, se sont matériellement produits, les agissements en question échappent légalement aux seuls domaine et règlementation du régulateur, mais tombent de facto sous l'emprise légale :

- de la loi sur les données personnelles, puisqu'ils constituent un traitement interdit de données personnelles ;
- du code pénal, parce qu'ils répondent à la qualification d'infractions pénales ;
- du code de procédure pénale, qui détermine les règles de poursuites, compétences juridictionnelles, jugements et exécutions des peines ;
- et de la Loi relative à la cybercriminalité, étant donné que le droit pénal spécial mauritanien leur confère la qualité de cyber infractions.

Cette précision étant apportée, le régulateur pourrait à la limite – ce qui reste à démontrer - ne pas user de ses prérogatives en matière de sanctions administratives et pécuniaires vis-à-vis des opérateurs, mais il n'a, légalement, aucune qualité, ni la moindre compétence ou légitimité pour "relaxer" le pirate.

Pour soutenir cette assertion, nous reprenons, si besoin est, l'article 106 de sa propre loi sectorielle qui énonce, à son alinéa 1er, que les "infractions prévues par la Loi sont constatées conformément aux dispositions du code de procédure pénale" et l'article 107 du même texte, qui précise que "Les infractions à la Loi relèvent du tribunal de la Wilaya[6] dans laquelle l'infraction a été commise, conformément aux règles du code de procédure pénale et de l'Organisation Judiciaire en vigueur".
En clair, ces deux (2) dispositions attribuent exclusivement aux tribunaux de l'ordre judiciaire la compétence de connaître de toutes les infractions à la législation des communications électroniques.

Quatre (4) autres preuves de la compétence des juridictions pénales pour connaître du cas qui nous intéresse nous sont données par :

- L'article 87 de la Loi sur les données à caractère personnel, qui fixe la peine applicable à toute collecte de donnée personnelle par un moyen frauduleux, déloyal ou illicite (1 à 2 mois d'emprisonnement et amende de 50 000 à 500 000 Ouguiyas) ;

- L'article 98, Alinéa 1er du même texte, qui énonce que "Le procureur de la République avise le président de l'Autorité de Protection des Données à caractère personnel de toutes les poursuites relatives aux infractions pénales prévues par la présente loi, et le cas échéant, des suites qui leur sont données" ;

- L'article 48 de la loi relative à la cybercriminalité, qui attribue, tout comme la loi sur les communications électroniques, compétence aux juridictions mauritaniennes pour connaître des cyber infractions lorsque celles-ci sont commises :
a - sur le territoire national ou à bord d'un navire battant pavillon mauritanien ou d'un aéronef immatriculé selon les lois de la République Islamique de Mauritanie;
b- lorsque l'infraction commise, porte atteinte aux intérêts de l'État, ou a pour victime une personne de droit mauritanien ;

- Et l'article 36, alinéa 1er du Code de Procédure Pénale qui dispose que "Le procureur de la République reçoit les dénonciations, les plaintes et les procès-verbaux, **et apprécie la suite à leur donner**".

[6] Tribunal régional de 1ère instance

A la lumière de tout ce qui précède, une conclusion, au moins, s'impose, c'est que le régulateur, même si son intention n'était pas d'outrepasser ses attributions, s'est arrogé une prérogative ne relevant que du pouvoir du procureur de la république, en prenant la décision de classer systématiquement une affaire revêtant plusieurs aspects pénaux.

Pour en revenir, de manière concrète, à la conduite qu'il aurait dû tenir, il nous semble que l'une (1) des solutions les plus judicieuses aurait consisté, en dehors du traitement qu'il aurait donné au cas des opérateurs (dont la responsabilité civile et pénale est engagée), à ce qu'il :

- se déclare incompétent quant au sort à réserver au pirate et aux sanctions à lui appliquer ;
- et se dessaisisse du dossier, en le transmettant, en l'état, au procureur de la république de la Wilaya de Nouakchott, lieu de commission des infractions.

Autrement, il aurait aussi bien pu, à notre avis, transférer l'affaire à son homologue, l'Autorité de Protection des Données à Caractère Personnel.

L'une ou l'autre de ces options aurait au moins eu pour mérite un effet dissuasif à l'égard de tout nouveau candidat potentiel à la piraterie des données personnelles d'autrui ou à des traitements irréguliers de données personnelles d'un autre ordre. /.

_____

Mamadou Alpha KANE
Ancien Conseiller Juridique du Conseil National de Régulation
Chef du Département Juridique
De l'Autorité de Régulation Multisectorielle (ARE)