International Multilingual Journal of Science and Technology (IMJST)
ISSN: 2528-9810
Vol. 9 Issue 9, September - 2024

Les Enjeux Et Defis De Protection D'identité Des Abonnés Via Carte Sim En Rd Congo

ASINGYA KULE Gratia-Roméo

O. Introduction

Dans son manuel de sociologie juridique, le Doyen CARBONIER observait que « l'évolution des mœurs et des techniques donne matière à des nouvelles formes de délinquance. Aujourd'hui, cette observation résonne toujours avec autant de force et de gravité. Indéniablement, les nouvelles techniques d'internet ont changé radicalement nos civilisations. Elles ont bouleversé des pans entiers de la vie sociale, culturelle, économique, juridique et politique. Elles sont porteuses d'innombrables avantages et opportunités mais les enjeux qui leurs sont attachés sont de nouveaux types de délinquance qui amplifient la commission de délits classiques[1].»

En abordant cette réflexion, l'outil ciblé dans cette révolution technologique est le téléphone mobile dont l'importance dans le domaine des communications et des informations n'est plus à démontrer, et dont il ne fait aucun doute qu'il exerce un impact considérable sur le développement économique, social et culturel des États et des particuliers. Les interactions humaines sont devenues quasiment impossibles sans l'usage du téléphone.

Devenu donc partie intégrante de la vie, le téléphone a ouvert également une porte béante à des nouvelles formes de criminalités dirigées contre ses usagers dont l'aspect intéressant cette réflexion est l'atteinte à l'identité des abonnés ou des usagers des services des réseaux mobiles ,appelés aussi services des télécommunications et des technologies de l'information et de la communication .

Par « service des télécommunications et des technologies de l'information et de la communication » il faut attendre le *« service fourni normalement contre rémunération qui consiste entièrement ou principalement en la transmission ou l'acheminement des signaux ou une combinaison de ces fonctions sur des réseaux des télécommunications et des technologies de l'information et de la communication, y compris les services de transmission sur les réseaux utilisés pour la radiodiffusion(.)[2]»*

Tous ces services sont opérationnellement possibles au travers la carte Sim, ou tout simplement SIM, en anglais *« Subscriber Identiy Module »*, c'est une carte à puce électronique « nécessaire pour identifier l'abonné sur le réseau de téléphonie mobile. Elle permet donc de téléphoner, d'envoyer et de recevoir des messages textes ou encore de surfer sur le net[3].»

Par essence, outre ses multiples fonctions, la carte SIM sert à identifier les abonnés d'un réseau. Identifier, « c'est considérer comme identique, comprendre sous une même idée[4]. » En clair, l' « identité » d'une personne signifie que cette personne est elle-même et non une autre[5] , c'est en vertu d'un certain nombre de caractères[6] tel que le nom, sexe, adresse physique, les origines de l'intéressé, etc.

En vue de protéger les citoyens contre les abus des personnes inciviques et mal intentionnées qui ont transformé le téléphone portable en un moyen de commettre des infractions (menaces, arnaques, chantages, escroquerie, attentats, actes terroristes, cybercriminalité.), l'identification des abonnés a été lancée depuis 2015 par Arrêté interministériel n°25/CAB/VPM/MIN/INTERSEC/024/2015,n°003/CAB /VPM/PTNTIC/ 2015, n°MDNAC-RCAB/009/2015, n°004/CAB/MIN/ J&DH/2015,n°CAB/MIN.FINANCES/2015/0144 n°008/CAB/MIN/CM/LMO/2015 du 19 mai 2015 modifiant et complétant l'Arrêté interministériel n°068/CAB/MIN/INTERSEC/2009,n°212/CAB/MIN/J/2009,n°CAB/MIN/PTT/011/2009 du 21 décembre 2009 fixant les conditions de souscription à l'abonnement téléphonique en République Démocratique du Congo.

C'est ainsi que, pour utiliser les différents services de communications électroniques, il est nécessaire d'identifier le demandeur, personne physique ou morale. Cette identification se fait généralement sur présentation de la pièce d'identité pour les personnes

[1] J. DJOGBENOU**,** *La cybercriminalité : enjeux et défis pour le Bénin*, disponible sur http://www.capod.org, consulté le 24 Juilliet 2024.

[2] Art.83 de la loi n° 20/017 du 25 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication

[3] « Carte Sim, les formats », htps:/lwyy, hten.frl blog, p.1, consulté le 03 Décembre 2023.

[4] Voir Dictionnaire Universel, Hachette Edicef ,5e éd. 2008, p.622

[5] G. CORNU, Association Henri Capitant, *vocabulaire juridique*, Paris 10e éd. PUF, 2014, *v «* identité. »

[6] Idem.

physiques tel que le stipule l'arrêté en ces mots : *« S'agissant d'un mineur d'âge, la souscription à l'abonnement est faite par la personne exerçant sur lui l'autorité parentale ou tutélaire*[7]*,»* et pour les personnes morales c'est notamment par : *« la raison ou la dénomination sociale ; le numéro du Registre de Commerce et de Crédit Mobilier (RCCM) ou l'équivalent et le numéro d'Identification Nationale (IDN) pour les personnes morales commerçantes,*[8] *(.) »*

Si l'on considère le développement astronomique des récentes technologies , le caractère fugace de ces nouvelles formes de criminalité qu'il favorise et les mutations incessantes auxquelles est soumis le cyberespace sans omettre le fait que la population elle-même n'est pas assez rodée à l'utilisation de ces nouvelles technologies, cela ouvre la voie à l'émergence et à la multiplication des activités criminelles dans le domaine numérique.

Eu égard à ce qui précède, l'on peut dans cette optique se poser la question de savoir si l'arsenal juridique et l'organisation institutionnelle mises en place par l'État congolais peuvent assurer effectivement et efficacement la protection des abonnés des SRM contre toute forme d'atteinte à leur identité? Cette interrogation parait d'autant plus pertinente en ce sens que l'arnaque aux cartes Sim aux fins d'escroquerie et autres crimes ne cessent de prendre de l'ampleur.

L'on constate en effet que malgré toutes les mesures prises par les autorités au plan législatif et réglementaire, ainsi que toutes les barrières mises en place, les personnes malveillantes brillent toujours par plus d'ingéniosité que de fourberie, et ne cessent d'agrandir leur spectre. Il est donc impérieux de diagnostiquer les failles de riposte législative et institutionnelle contre la contrefaçon des cartes SIM via laquelle les criminels portent atteinte à l'identité de leurs victimes afin d'escroquer ou orchestrer d'autres faits nuisibles.

Ainsi, au regard de la question ci-dessous posée, nous pensons que pour rendre plus effective et efficace la protection d'identité via carte SIM, il faut qu'au-delà de l'identification traditionnelle par l'enregistrement des cartes d'identité des abonnées ou numéro RCCM, la loi doit également exiger aux SRM l'authentification biométrique de leurs abonnés. Pour que cela soit faisable, elles doivent améliorer leurs outils technologiques et leurs autorités de régulation doivent veiller plus sévèrement à l'application de ces normes, sans complaisance aucune.

[7] Cfr Article 5 al.4 de l'arrêté interministériel n°25/CAB/VPM/MIN/ INTERSEC/024/2015 fixant les conditions de souscription à l'abonnement téléphonique en République Démocratique du Congo

[8] Idem article 3 a.

1. Du mécanisme juridique de protection de l'identité

Les pouvoirs publics ont progressivement développé une politique préventive reposant sur des mesures de type social, et visant à lutter contre les facteurs étiologiques de la criminalité, l'amélioration de la formation, l'intégration professionnelle, occupation des jeunes désœuvrés et dans cette même perspective d'une politique préventive, l'État fait l'intervenir de nouvelles législations en proposant des solutions purement techniques en vue de faire face à toute forme de délinquance [9] ,comme c'en est le cas de l'obligation pour les SRM d'enregistrer leurs abonnés .

Tout en s'inscrivant dans la même logique, le premier point de cette réflexion s'attardera à apprécier les efforts menés par l'État congolais dans la protection des abonnés des SRM sur le plan législatif en présentant les instruments juridiques de protection en vigueur dont les uns portent sur l'identité réelle et d'autres sur l'identité numérique.

1.1. De la disposition textuelle de protection d'identité

Le droit pénal présente une importance théorique ou philosophique dans la mesure où ses règles touchent d'une part à la sécurité de la société, et, d'autre part, à la liberté des individus[10]. Au travers toutes atteintes contre l'identité le criminel vise très souvent un moyen de commettre une autre infraction. Il s'agit donc ici d'une infraction formelle dont la consommation se réalise du seul fait d'avoir employé un procédé ou un moyen pouvant causer un dommage a autrui. Conscient de cet état de chose, le législateur en congolais a entouré l'identité d'une certaine protection remarquable dans divers textes légaux dont notamment :

- L'article 92 al.2 de la loi relative aux télécommunications et aux technologies de l'information et de la communication qui dispose que : « *Tout exploitant d'un réseau de télécommunications ouvert au public ou tout fournisseur des services d'accès à l'internet est tenu d'identifier ses abonnés au moment de la souscription aux services de télécommunications. »*
- L'article 2 de l'arrêté interministériel fixant les conditions de souscription à l'abonnement téléphonique en République Démocratique du Congo y revient presqu'avec un libellé similaire : *« Tout exploitant d'un réseau de télécommunications ouvert au public ou tout fournisseur des services d'accès à l'internet est tenu d'identifier ses abonnés au moment de la souscription aux services de télécommunications en mode post-payé ou prépayé*. »

[9] V. Gautron, *La Fin de la singularité du modèle français de prévention de la délinquance*, AJ pénal 2007, p.205.

[10] C.KAKULE KALWAHALI, *Droit pénal général*, Edition Blessing, Kampala, Janvier 2017, p.1

-L'article 8 du même arrêté y revient en ces termes : *« L'exploitant d'un réseau ou le fournisseur des services de télécommunications ouverts au public est tenu de procéder immédiatement à la suspension du service du numéro ou de la connexion de tout abonné trouvé non ou insuffisamment identifié et ce, conformément à la procédure décrite dans l'annexe 3 du présent Arrêté interministériel.»*

❖ Article182 du code numérique stipule que : *« Le titulaire d'un moyen d'identification électronique est tenu de prendre toutes les mesures nécessaires pour le garder sous son contrôle exclusif afin de prévenir le vol, la perte ou la divulgation. Dans ce cas, le titulaire doit immédiatement révoquer le moyen d'identification électronique. » Lorsque le moyen d'identification électronique vient à échéance ou est révoqué, son titulaire ne peut plus l'utiliser. »*

❖ Le nom, partie intégrante de l'identité est aussi légalement protégé. En effet, l'article 69 de la loi n° 87 /010 du 1er août 1987 portant code de la famille incrimine l'usurpation du nom.

❖ Les articles 349,351 et 352 du code numérique congolais :

-Article 349 : *« Est puni d'une peine de servitude pénale de six mois à deux ans et d'une amende de vingt-cinq millions de Francs congolais, ou d'une de ces peines seulement, celui qui utilise les éléments d'identification d'une personne physique ou morale dans le but de tromper les destinataires d'un message électronique ou les usagers d'un site internet en vue de les amener à communiquer des données à caractère personnel ou des informations confidentielles. »*

-Article351 : *« Est puni d'une servitude pénale d'un an à cinq ans et d'une amende de vingt millions à cent millions de Francs congolais, quiconque usurpe, par hameçonnage, phishing ou tout autre moyen, intentionnellement et sans droit par le biais d'un système informatique, l'identité d'autrui, une ou plusieurs données permettant de s'attribuer faussement et de manière illicite l'identité d'autrui dans le but de troubler sa tranquillité, de porter atteinte à son honneur, à sa considération ou à ses intérêts. »*

-L'article 352 du code numérique : « *Quiconque aura utilisé des données à caractère personnel ou des informations confidentielles communiquées dans le but de détourner des fonds publics ou privés, sera puni d'une peine de servitude pénale de cinq à dix ans et d'une amende de cinquante millions à cent millions de Francs congolais. »*

❖ L'article 123 de la loi relative aux systèmes de paiement et de règlement-titres stipulant que, *« Est puni de cinq à dix ans de servitude pénale et d'une amende de 50.000.000 à 500.000.000 de francs congolais ou de l'une*

de ces peines seulement, toute personne qui, en connaissance de cause:

1. utilise sans autorisation des données d'identification pour le lancement ou le traitement d'une opération de paiement électronique;

2. utilise des données d'identification fictives pour le lancement ou le traitement d'une opération de paiement électronique;

3. manipule des données ou des informations portant sur des comptes ou d'autres données d'identification, en vue du lancement ou du traitement d'une opération de paiement électronique[11]*. »*

En substance ces dispositions sus-évoquées s'adressent d'une part aux Opérateurs de Réseaux Mobiles et aux Services Numériques en leur imposant l'obligation d'identifier leurs abonnés et à ces derniers de se faire identifier. D'autre part ces dispositions s'adressent à quiconque d'éviter tout acte attentatoire à l'identité, qu'elle soit réelle ou numérique.

Cet arsenal juridique de protection sur l'identité démontre éloquemment son caractère très sensible et pertinent, surtout à cette ère où le monde virtuel offre une possibilité de disposer d'une identité numérique dont la moindre négligence de protection peut donner accès aux personnes malveillantes de l'usurper et de s'en servir contre leurs victimes.

Tout en gardant de vue sur la protection d'identité via carte Sim, il convient d'apprécier le bienfondé de cette protection imbibant de nombreux textes législatifs, il s'agit en d'autres termes d'analyser leur ratio legis.

1.2. De la « ratio legis » des dispositions de protection d'identité

Dans le langage juridique, la « ratio legis » fait allusion au but visé par le législateur en édictant une loi ; c'est le sens même contenu dans la traduction littérale du concept : « la raison d'être de la loi »,voisin de l'expression « élément axiologique » de la loi. L'axiologie (du grec : *axia* ou *axios*, valeur, qualité) peut définir comme la science des valeurs (.)[12]Sous l'angle du droit pénal, il fait allusion aux valeurs à protéger par le législateur en incriminant un comportement.

Ainsi, par divers textes législatifs relatifs à l'identification, le législateur vise protéger une panoplie de valeurs dont le contenu peut varier en consideration des bénéficiaires :

1) Pour les opérateurs, il s'agit d'identifier tous leurs abonnés, réaliser et mettre à jour une base de données d'identification fiable et sécurisée des abonnés, procéder à la suspension systématique des abonnés sans nom ou sans numéro de pièce d'identité, mais actifs dans leurs réseaux

[11]Voire la Loi n° 18-019 du 9 juillet 2018, relative aux systèmes de paiement et de règlement-titres (J.O.RDC., 23 juillet2018, n° spécial, col. 53)

[12] Encyclopédie libre, « Axiologie » disponible sur Axiologie — Wikipédia (wikipedia.org) consulté le 28 Juillet 2024 à 11h08

téléphoniques respectifs, et de répondre aux réquisitions judiciaires[13].

En fait, l'identification permet aux SRM et aux Fournisseurs des Services Numériques de connaitre le nombre de leurs abonnés, ce qui peut servir d'un des indicateurs de croissance ou décroissance de la clientèle et même identifier les clients potentiels et les clients inactifs. S'agissant de ces derniers ,après une durée généralement de trois mois,la carte SIM n'est plus operationnnelle et les numéros telephinique peuvent faire objet d'une nouvelle réattribution à un autre client[14].

2) Pour les services publics de sécurité de l'État, les objectifs sont de : diligenter les enquêtes et les procédures judiciaires relatives aux infractions commises à l'aide des réseaux de communications électroniques – la cybercriminalité : menaces, injures, dénonciation calomnieuses, diffamations, extorsions, attentats -, adresser aux opérateurs des réquisitions de la Police judiciaire à l'effet d'identification des présumés délinquants, assurer l'identification de l'appelant des services d'urgence[15].

Cela s'avère être plus évident en ce sens que plusieurs dispositions textuelles contraignent les SRM et les Fournisseurs de Services Numériques (FSN) à fournir les données personnelles de leurs abonnés lors des enquêtes judiciaires. C'est notamment :

❖ la loi n° 20/017 du 25 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication à son l'article 126 alinéa 1 et 2, il est prévu ce qui suit : *« Toute personne a droit au secret des télécommunications et des technologies de l'information et de la communication. Le secret des correspondances est levé sur réquisition du ministère public ou sur autorisation des Cours et Tribunaux dans le cadre de l'instruction judiciaire. Les services publics compétents de l'État dérogent au secret des correspondances pour des raisons de sécurité intérieure et/ou extérieure de l'État, de défense nationale ou d'ordre public.».*

Cette disposition met en exergue l'une des hypothèses dans lesquelles le secret professionnel peut être révélé pour la raison d'enquête ou instruction judiciaire, le but etant celui fournir des preuves ou d'identifier une personne recherchée par la justice pour la manifestation de la vérité. Le succès de cette démarche reste possible si l'identification des abonnées est dûment faite en amont par les SRM, d'où l'importance sans mesure de l'identification des abonnés par leurs SRM.

❖ l'article 287 qui dispose que : « *Le fournisseur d'accès à internet et le fournisseur de services en ligne concourent à la lutte contre les infractions prévues dans la présents ordonnance-loi. Ils mettent en place, à ce titre, un dispositif facilement accessible et visible permettant à toute personne de porter à leur connaissance les faits constitutifs de ces infractions. Ils sont également tenus, d'une part, d'informer et promptement les autorités compétentes de toutes les activités illicites mentionnées qui leur seraient signalées et qu'exerceraient les destinataires de leurs services, et d'autre part suspendre tout contenu susceptible de porter atteinte à la moralité.*

L'autorité judiciaire peut enjoindre, conformément à la loi, à tout fournisseur de services en ligne, et à défaut, à tout fournisseur d'accès à l'internet, toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service en ligne. »

Comparativement à la disposition précédente, celle-ci requiert encore l'avantage d'agir en amont du crime, en identifiant le criminel avant la réalisation de son forfait. Il est donc heureux de trouver ici un cas rare où le professionnel est dédouané de l'obligation de tenir secret avant la réalisation du crime ou la survenance d'un dommage. Pour la disposition précédente c'est pendant les enquêtes judiciaires lorsque le crime est déjà réalisé que l'on peut lever le secret alors que la disposition sous examen est une vraie expression du principe de prévention criminelle telle qu'encrée dans la philosophie du droit pénal ,par le fait qu'elle combat le crime depuis sa gestation même. Cette anticipation criminelle demeure également possible si l'identification des abonnés est dûment faite en amont.

3) Pour les abonnés : le législateur s'est montré si protecteur au travers plusieurs textes visant protéger de nombreuses valeurs dont les unes sont d'ordres patrimoniaux et d'autres extrapatrimoniaux.

❖ Valeurs d'ordres patrimoniaux :

À ce propos l'on peut évoquer notamment :

-L'article 123 de la loi relative aux systèmes de paiement et de règlement-titres stipulant que, *« Est puni de cinq à dix ans de servitude pénale et d'une amende de 50.000.000 à 500.000.000 de francs congolais ou de l'une de ces peines seulement, toute personne qui, en connaissance de cause:*

1. utilise sans autorisation des données d'identification pour le lancement ou le traitement d'une opération de paiement électronique;

2. utilise des données d'identification fictives pour le lancement ou le traitement d'une opération de paiement électronique;

3. manipule des données ou des informations portant sur des comptes ou d'autres données

[13] Disponible sur Identification des abonnés de réseaux de communications électroniques : quelle approche de protection des données dans un cadre légal insuffisant ? - Digital Business Africa ,consulté le 28 Juillet 2024 à 15h01

[14] Propos concordants de Serge Kanyunyu,Bineguro Furaha et Dolph Kalambay, respectivement chargés des services comerciaux dans la SRM Airtel,Vodacom et Orange

[15] Idem

d'identification, en vue du lancement ou du traitement d'une opération de paiement électronique. »

-L'article 352 du code numérique stipule que : « *Quiconque aura utilisé des données à caractère personnel ou des informations confidentielles communiquées dans le but de détourner des fonds publics ou privés, sera puni d'une peine de servitude pénale de cinq à dix ans et d'une amende de cinquante millions à cent millions de Francs congolais. »*

Le point commun pour ces deux dispositions sus-évoquées est l'interdiction d'utilisation données à caractère personnel par un tiers dans le but de porter atteinte aux intérêts pécuniaires.

Lorsque les SRM et les FSN procèdent à l'enregistrement de l'identité des abonnés, personnes physiques ou morales cela confère à ces dernières une identité numérique associée aux numéros téléphoniques des cartes Sim. Ainsi tout acte réalisé sur la carte Sim est présomptueusement attribué au titulaire dûment reconnu par sa SRM ou son FSN. Il sied cependant de préciser qu'il s'agit-là d'une preuve réfragable, pour laquelle l'on peut apporter une preuve contraire.

En effet, l'utilisateur d'une carte Sim peut ou ne pas être le titulaire bien que présomptueusement chaque Carte Sim soit souvent enregistrée sous l'identité de son utilisateur qu'il soit personne physique ou morale.

C'est pourquoi tout titulaire d'une carte Sim qui s'en est dépossédé involontairement (par vol du téléphone, par hameçonnage, phishing, perte etc.) est tenu d'obligation légale de le dénoncer auprès de sa SRM ou son FSN aussi dans la même optique de prendre des mesures de précaution afin d'éviter tout accès à son identification électronique , c'est ce que soutient sans ambage l'article182 du code numérique qui dispose que : *« Le titulaire d'un moyen d'identification électronique est tenu de prendre toutes les mesures nécessaires pour le garder sous son contrôle exclusif afin de prévenir le vol, la perte ou la divulgation. Dans ce cas, le titulaire doit immédiatement révoquer le moyen d'identification électronique. »*

Ces dispositions, d'une part préviennent les tiers de toute atteinte à l'identité numérique d'autrui pour ne pas nuire à leurs intérêts pécuniaires et d'autre part elles invitent les abonnés de prendre des mesures de précaution afin de prévenir ces atteintes en évitant tout comportement nuisible contre leurs intérêts pécuniaires.

Au total, à propos des abonnés, la carte Sim représente valablement leur identité numérique, l'absence de sa protection peut engendrer plusieurs contentieux mettant en cause leurs droits patrimoniaux en ce sens que la carte SIM peut constituer non seulement un véritable porte-monnaie électronique pour les abonnés mais aussi elle peut contenir des biens numériques qui leur valent fortune tels que les unités pour la communication, les forfaits internet, etc.

Ainsi ,la ratio legis de ces dispositions sus-evoquées visent directement protéger les valeurs d'ordres patrimoniaux, quantifiables en argent. D'autres dispositions défendent des valeurs non évaluables pécuniairement tel qu'abordé dans le sous-point suivant.

❖ **Valeurs d'ordres extrapatrimoniaux :**

Dans le langage du domaine de la communication les « données d'identification » sont contenues dans la notion des « données personnelles » tel que l'ateste l'article 4 de la loi relative aux télécommunications et aux technologies de l'information et de la communication ainsi libellé au point 37 *: « Données à caractère personnel : toute information relative à une personne physique identifiée ou identifiable directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique. »*

L'article 183 du code numérique fournit des exemples relatifs aux données à caractère personnel en ces termes :

« Les catégories suivantes sont considérées comme données personnelles.

Il s'agit notamment :

1. des données d'identification personnelle notamment prénom, nom, post-nom, date et lieu de naissance, âge, état civil, numéro d'identification nationale, document officie d'identité en cours de validité ou toute autre donnée biométrique notamment photographie, enregistrement sonore, image, empreintes digitales et iris.

2. des données de correspondance : coordonnées téléphoniques, adresses physique, postale et électronique;

3. des données professionnelles : statut, emploi occupé, employeur, rémunération ;

4. des données de facturation et de paiement: montant et historique des factures, état de paiement, relances, soldes de paiement, date de prélèvement;

5. des coordonnées bancaires : code banque, numéro de compte et de la carte bancaire, nom / adresse / coordonnées de la banque, références de transactions

6. des données sur des personnes morales de droit public ou privé faisant apparaitre les données personnelles;

7. des données sur la situation familiale;

8. des données concernant des décisions de justice. »

Tous ces détails fournis par l'article 183 du code numérique contiennent des éléments que peut

regorger les identifiants d'une carte SIM ou du moins ce qu'elle peut contenir, en occurrence :

1) les données d'identification personnelle notamment prénom, nom, post-nom, date et lieu de naissance, âge, etc., prélevés à partir de la carte d'identité de l'abonné. Ainsi, quiconque qui se fait passer frauduleusement pour titulaire d'une carte SIM porte indirectement atteinte au nom qui est un droit extrapatrimonial légalement protégé car faisant partie intégrante d'identité dont l'incrimination est prévue et sanctionnée par l'article 69 de la loi n° 87 /010 du 1er août 1987 portant code de la famille qui condamne l'usurpation du nom.

Pour que la responsabilité pénale de l'agent soit engagée, il faut que cette usurpation du nom d'un tiers soit volontaire et continue, en s'en attribuant frauduleusement et dolosivement dans le but de semer la confusion[16].

2) Les données de correspondance : coordonnées téléphoniques, adresses physique, postale et électronique.

La carte SIM est une véritable boite à lettre pour les abonnés et dont l'accès par une tierce personne mal intentionnée est très possible s'il y a moindre négligence dans le chef de SRM et/ou de l'abonné.

En effet, de nombreuses applications et comptes en ligne sont liés à des adresses électroniques ou à des numéros de téléphone mobile. Souvent, ces applications et comptes utilisent des messages textes pour authentifier l'identité d'une personne. Lorsqu'une personne tente de se connecter, un message texte contenant un code unique est envoyé à son téléphone mobile. Le titulaire du compte a besoin de ce code pour accéder à ses services en ligne.

Une fois que le fraudeur s'empare du compte de téléphone mobile de la victime, il a accès à ce code. En utilisant ce renseignement, il peut prendre le contrôle des comptes en ligne d'une victime ou demander que les mots de passe soient réinitialisés ou modifiés, verrouillant ainsi l'accès pour la victime. Le fraudeur peut accéder aux SMS, aux comptes des médias sociaux (Facebook, Whatsapp, Instagram, etc.), de courriel ou de tout autre compte lié au numéro de téléphone mobile de la victime.

Le secret de correspondance est un droit extrapatrimonial qui est garanti pour tout citoyen en RD Congo et dont la violation est prévue et sanctionnée par l'article 73 du Décret du 30 janvier 1940 tel que modifié et complété par la Loi n° 15/022 du 31 décembre 2015 modifiant et complétant le Décret du 30 janvier 1940 portant code pénal, *In JO. RDC, numéro spécial du 29 février 2016.*

En appréciant les préjudices souvent subis par la victime lors de violation de son secret, force est de comprendre qu'ils affectent plus ses droits extrapatrimoniaux tel que droit à l'intimité, à la dignité; à la réputation car le secret violé provoque chez la victime un dommage moral (et parfois matériels[17]). En principe toute violation de l'intimité renvoie automatiquement à l'idée de la vie privée.

Le concept de vie privée mérite d'être précisé, car il n'existe à date aucune définition légale. Historiquement, ses origines philosophiques remonteraient au IVe siècle avant Jésus-Christ, époque où Aristote faisait déjà la différence entre les deux aspects de la vie que sont d'une part la vie imbriquée dans la sphère publique, appelée *« polis »*, associée à la politique, et d'autre part son opposé, la vie relative à la sphère privée, 1'*« oikos »,* qui se ramène à la vie domestique [18].

Avec le vent des libertés individuelles du XV IIIe siècle, le concept évoluera encore et sera progressivement intégré dans les textes de lois. Mais c'est avec le développement des TIC (photographie, presse, télécommunications, Internet, etc.) que le concept dévoilera toute son importance, invitant le législateur à intervenir pour le préciser.

Sur le terrain, c'est la doctrine qui a pris les devants, notamment à travers les écrits des avocats américains Samuel Warren et Louis Bandeis qui, dans un article paru en décembre 1890, définissaient le concept de vie privée comme le « droit d'être laissé tranquille[19].»

Toutefois la plupart de législateurs dans le monde sont enclins à circonscrire la notion de la vie privée dans le domaine de la correspondance et de droit à l'image alors qu'il existe d'autres aspects concernés par la vie privée, le secret de sa vie affective, familiale etc.

En somme, la « vie privée » comme le concept même l'indique, renvoie à tout ce qui est sensé n'est pas être à la porté de tiers, en occurrence le secret de correspondance dont la ratio legis est la protection de la vie privée. Sa garantie, en ce siècle de NTIC, est étroitement conditionnée à la sécurité dont bénéficieraient les abonnés de SRM via leurs cartes SIM.

[16] Voire B.C. NYANGEZI, *les infractions de A à Z*, 1ere Édition, Laurent Nyangezi, Kinshasa, 2011, pp.588-589

[17] Par exemple la violation de secret de fabrication d'une entreprise peut se répercuter sur son chiffre d'affaire.

[18] Voir DeCew, Judith, « Privagy », Stanford Engyclopedia of Philosophy Arsbins, www.plato.stanford.edu/archives/spr2015/entries/privacy, cité dans « vie privée »consulté le 30 Juillet 2024 à 23h23

[19] En anglais, *« The right to be let alone »* : Warren, Samuel et Brandeis, Louis, « The Riht privacy », Harvard Law Review,n°5,15décembre1890,htn://groups.csail.mit.edu/mac/classes /6805/articles/privacy/privacy_brand_war Zhtml, cité dans « Vie privé », Wikipédia. Org/ wiki/ Vie-privée consulté le 30 Juillet 2024 à 23h52

De ce qui précède, il sied de retenir que la carte SIM incarne bel et bien l'identité numérique des abonnés de SRM et même des FSN. Tout acte attentatoire contre cet outil expose la victime aux préjudices tant matériels que moraux. La riposte législative s'est inscrite dans la même perspective, en protégeant les valeurs d'ordres patrimoniaux et extrapatrimoniaux tel que vérifié dans les commentaires de la ratio legis.

Du reste, les bonnes intentions du législateurs tel que étalées ci-haut, contiennent-elles effectivement et effacement ce phénomène nouveaux d'usurpation d'identité via carte SIM ? Une diagnostique des ressources de protection s'impose donc dans la seconde partie de cette réflexion.

2. De la diagnostique des enjeux de protection d'identité des abonnés

Au-delà des bonnes intentions du législateur, cette partie s'attardera à analyser les limites des ressources que l'État congolais a mises à sa disposition pour protéger l'identité des abonnés des SRM via carte SIM. Il s'agit d'interroger les failles législatives (2.1) et les failles institutionnelles (2.2.)

2.1. De la faille d'inadaptation législative de protection

2.1.1. De l'anachronisme des normes de protection

L'anachronisme renvoie au caractère de qui est anachronique, c'est le fait d'attribuer quelque chose à une époque qui ne lui appartient pas. Dans le cas d'espèce cela renvoie à l'ideé d'une chose qui est devenue inadaptée à cause de l'évolution technologique.

En effet, toutes les lois faisant référence à l'obligation d'identification des abonnées des SRM, plus singulièrement l'arrêté interministériel fixant les conditions de souscription à l'abonnement téléphonique en République Démocratique du Congo, font allusion à l'identification à partir des cartes d'identité du moins pour les personnes physiques.

Il s'avère que ce prédécédé d'identification éprouve aujourd'hui beaucoup de faiblesses du fait que les délinquants ne realisent pas souvent assez de gymnastiques pour accomplir leur dessein criminel . Cette porte d'acces est occassionée principalement par le fait que l'État congolais, juste après le régime de Mobutu, n'a jamais doté ses citoyens de cartes d'identité. Les cartes d'électeurs qui jouent provisoirement ce rôle ne protègent pas d'une manière satisfaisante à cause de sa fragilité en matière de preuve observable notamment dans les cas suivants :

1) La non clarté de l'image photo de la carte : en fait les cartes d'électeurs des dernières élections ont fait objet des critiques exacerbés du point de vue qualité. D'abord imprimée en noir blanc, ensuite ne reflétant pas réellement l'image du titulaire, en fin les écrits s'y effacent si facilement. Au regard de cette situation, le criminel peut l'exploiter à son avantage à des fins infractionnelles. Aussi le vrai titulaire peut être privé d'accès à un service sollicité à la SRM tel qu'élargir son compte Money Mobile.

2) Le duplicata des cartes d'électeurs est souvent reçus avec beaucoup de réserve par les agents des SRM surtout lorsque l'abonné désire swapper sa carte SIM contenant beaucoup d'argent, unités ou forfaits internet. Cette réserve maniériste au nom de la protection des intérêts de l'abonné peut se convertir à une source d'insécurité en ce sens qu'il ne sera privé de répondre notamment à ses besoins pécuniaires tout en disposant l'argent dans sa porte-monnaie électronique que représente la carte SIM.

3) A défaut des cartes d'électeurs, les pièces d'identités plus fiables demeurent les passeports. Malheureusement nombreuses gens n'en disposent pas à cause non seulement de sa lourde procédure d'acquisition mais surtout encore de sa tarification très élevée.

De ce qui précède, la carte d'électeur demeure la pièce d'identité pour la majorité des citoyens congolais, sauf exception. Malheureusement, elle expose son titulaire aux multiples actes infractionnels pour des raisons sus-évoquées. Aussi lorsqu'une carte SIM est perdue,contenant des biens numeriques de valeur valeureuse, la pièce d'identité originale est souvent exigible à l'abonné concerné par la perte, dans le but de protéger ses intérêts pécuniaires[20].

C'est là où trop protéger peut tuer le droit de l'abonné car lui imposer l'obligation de s'identifier dans ce contexte-là reviendrait à lui exiger à déterminer le sexe de l'ange, étant donné qu'il n'est plus en possession de sa pièce d'identité originale[21].

Eu égard à cet état de chose, il s'impose d'envisager un autre nouveau procédé d'identification qui résoudrait les problèmes supra-évoqués.

2.1.2. Plaidoyer pour un nouveau procédé d'identification

Il n'est plus important de démontrer que l'enregistrement numérique des cartes d'électeur comme celui des autres pièces jouant rôle de d'identification en RDC, est un procédé très fragile en matière de protection de l'identité leur titulaires en ce sens qu'elles peuvent facilement faire objet de contrefaçon en vue de réalisation des crimes.

Aussi, en cas de leur perte, les abonnés sont confrontés à une lourde gymnastique de fournir la preuve de leur droit de propriété sur leurs cartes SIM et par ricochet sur tous les biens numériques qu'elles

[20] Renseignements fournis concordamment par Mrs Serge KANYUNYU et Mme SARA KAVIRA, respectivement agents chez la SRM Airtel à Goma et Kinshasa.

[21] Idem

peuvent contenir tel que l'argent électronique, les unités d'appels, les forfaits internet, etc.

C'est dans cette perspective qu'un nouveau procédé d'identification doit être envisagé en vue de résoudre la faille législative due à l'inadaptation des normes d'identification qui se limite jusqu'ici à l'enregistrement des éléments d'identification se retrouvant sur les cartes d'identité des abonnés en occurrence le nom, lieux de résidence, date et lieu de naissance, la nationalité, etc. La possibilité d'usurper ces éléments à des fins criminelles pousse à plaider pour l'identification biométrique.

Le législateur congolais n'a pas clairement défini ce qu'est une l'identification biométrique, il s'est contenté d'une définition énumérative à l'article 183 du code numérique qui stipule que *« (.) les données d'identification biométrique comprennent notamment la photographie, l'enregistrement sonore, images, empreintes digitales, iris. »*

A défaut d'une définition légale satisfaisante, un regard judicieux tourné vers la doctrine permet d'avoir accès à cette définition plus riche qui rapporte que l'identification biométrique « comprend tout un ensemble de technologies et procédés de reconnaissance, d'authentification et d'identification des personnes à partir de certaines de leurs caractéristiques physiques ou comportementales[22]. »

Il est donc question d'enregistrer à partir des outils technologiques les caractéristiques physiques de l'être humain comme l'exprime même le sens littéral du mot «biométrie » qui veut dire « mesure de l'être humain.» Pour la plus part de cas l'on vise les organes qui distinguent une personne des autres ou ceux-là qui font de la personne un être unique par rapport aux autres tel que les empreintes digitales, la reconnaissance de l'iris et faciale.

Ce procédé d'identification biométrique des abonnés de SRM requiert une constellation d'avantages tant au niveau des particuliers qu'au niveau de l'État qu'on peut résumer à quatre points :

1) L'identification biométrique est une garantie efficace contre l'usurpation d'identité.

En fait, la reconnaissance des empreintes digitales, de l'iris ou la reconnaissance faciale n'ont pas leur pareil pour établir le lien entre nos identités physiques et digitales**.** L'authentification biométrique aide ainsi à prévenir l'usurpation d'identité en permettant à une personne souhaitant accéder à un compte ou à un appareil de prouver qu'elle est bien qui elle prétend être. De même, les personnes qui présenteraient au Shop d'une SRM avec les pièces d'identité de leurs victimes en se faisant passer pour ces dernières n'auront plus cette possibilité par le fait que leur identité biométrique ne pourrait jamais correspondre à celle de leurs victimes.

À ce propos, Francis Galton (cousin de Darwin) renchérit que la probabilité de trouver deux empreintes digitales semblables est d'une chance sur 64 milliards même chez les vrais jumeaux (homozygotes). C'est pour cela que l'empreinte digitale est devenue un élément indissociable de l'identité[23].

2) L'identification biométrique écarte la problématique de la lourdeur de la preuve lors de la perte de la pièce d'identité et de la carte SIM

Comme déjà évoqué supra, les agents des SRM se réservent souvent de la demande de leurs abonnés consistant à swapper une carte SIM perdue qui contient des biens numériques de valeur surtout lorsque l'identité est prouvée par un duplicata ou une attestation de perte des pièces. Cette prudence de la part des SRM vaut son pesant d'or par le fait que les OPJ fournissent ces attestations sur base d'une simple déclaration sans qu'elle ne soit confrontée pratiquement à une vérification. En conséquence les SRM n'y font pas foi dans le but de protéger leurs abonnés, cette protection qui peut faire souffrir les intérêts pécuniaires d'un abonné de bonne foi. Par contre l'identification biométrique l'exonère de l'obligation de fournir sa pièce d'identité pour accéder au service sollicité.

3) **Pour les SRM l'identification biométrie offre également un avantage essentiel par rapport aux technologies traditionnelles :** la rapidité et la fluidité avec laquelle l'authentification ou l'identification peuvent être réalisées, d'un simple geste de la main ou littéralement d'un seul coup d'œil[24]**.**

En effet, le remplissage manuel de la fiche d'identification et l'enregistrement numérique de ces données d'identification s'avèrent être une procédure si longue pour les SRM comparativement aux enregistrements d'empreinte digitale, de l'iris, de la reconnaissance faciale ou leur vérification. Un simple clic sur l'appareil, tous les renseignements sur la personne apparaissent.

4) **Pour l'État, l'identification biométrique facilite la prévention des crimes et les enquêtes judicaires**.

Elle contribue donc tant soi peu à la sécurité et au maintien de l'ordre public en ce sens qu'elle facilite efficacement l'identification d'un criminel recherché en

[22] Disponible sur https://www.idemia.com/fr/biometrie , consulté le 10 Avril 2024 à 15h07

[23] Disponible sur https//www.thalesgroup.com/fr/europe/france/dis/gouvernement/inspiration/biometrie

Consulté le 11 Avril 2024 à 9h05

[24] Disponible sur https://www.idemia.com/fr/biometrie , consulté le 10 Avril 2024 à 15h07

apportant une précision non équivoque sur sa personne. Une pratique s'est déplorée dans l'identification traditionnelle, celle consistant pour les SRM d'enregistrer l'abonné sous l'identité d'un autre.

Cela est fréquent surtout lors d'un achat d'une carte SIM préenregistrée qui confère automatiquement à l'utilisateur l'identité de la personne sous laquelle la carte SIM est préenregistrée. C'est une situation délicate pouvant semer de confusion sur l'identité du criminel pendant les enquêtes judicaires si l'un de ces deux abonnés auraient commis un acte illégal. De toute évidence, l'identification biométrique demeure un procédé par excellence pour pallier cet état de chose car son enregistrement impose aux SRM la présence physique de leurs abonnés, ce qui peut déjà vider en amont toute confusion sur l'identification de ces derniers, fait qu'on peut apprécier comme un facteur d'une prévention efficace contre toute atteinte à l'identité.

Somme toute, l'indentification biométrique défie le mieux que possible le criminel de l'ère numérique par son adaptation au dégrée de sa « temibilita »[25]. En faire une exigence légale sous peine de sanction pour sa violation, résoudrait tant soi peu toutes les préoccupations autours des actes infractionnels contre la carte SIM qui représente l'identité de son titulaire ainsi que ses intérêts patrimoniaux et extrapatrimoniaux, cibles finales du criminel.

2.2. De la faille d'insuffisance législative de protection

Au-delà des normes préexistantes en matière de protection d'identité des abonnés des SRM, il se manifeste encore un besoin accru de les renforcer avec des dispositions textuelles visant une protection plus efficace. Ce besoin est récurrent d'une part en ce qui est la lutte contre la prolifération des cartes SIM (2.2.1) et d'autre part la nécessité des normes plus sévères pour non-respect d'identification (2.2.2.)

2.2.1. De la lutte contre la prolifération des cartes SIM

Nos investigations sur terrains nous ont conduit à un constat amer, celui d'identifier un phénomène qui peut servir de voie à la criminalité de tout genre, hormis celle de actes attentatoires aux cartes SIM. Ce phénomène est ici qualifié de prolifération des cartes SIM. In concreto, il s'agit des ventes hors normes des cartes Sim aux abonnés d'une SRM au su ou non de celle-ci et dont la conséquence logique est la détention illimitée des cartes SIM par leurs usagers.

La prolifération des cartes SIM est engendrée par deux pratiques observées dans les activités commerciales des SRM :

1) Il s'est observé de 2023 à nos jours la pratique de vente des forfaits internet mensuels contenus dans une carte SIM qu'on livre sans enregistrement à l'acheteur .Cela viole l'obligation légale d'identification, pourtant ces cartes SIM sont dotées de toutes les fonctionnalités pour correspondre[26].

Si cette carte SIM est utilisée à des fins infractionnelles, il se poserait un problème d'identification du criminel, un aspect non négligeable car le succès d'une enquête judiciaire en dépend dans une certaine mesure.

2) Une autre pratique est celle d'une possibilité pour les abonnés de se procurer d'un nombre illimité d'une carte SIM chez une même SRM. De toute évidence, cette pratique n'est imbibée d'aucune illégalité en vertu d'un principe cher en Droit qui déclare que *« Tout ce qui n'est pas interdit est autorisé »*, inspiré de la Déclaration Universelle de Droit de l'homme disposant que : ***«*** *La loi n'a le droit de défendre que les actions nuisibles à la société. Tout ce qui n'est pas défendu par la loi ne peut être empêché, et nul ne peut être contraint à faire ce qu'elle n'ordonne pas. »*

Cette disposition est à son tour le corollaire du principe de la légalité des délits et des peines qui veut qu'il n'y ait pas de crime ni de peine sans qu'une loi les prévoie. Dans cette perspective le silence du législateur congolais est à interpréter comme une autorisation tacite d'une pratique dont la non incrimination peut représenter un potentiel danger contre l'ordre public.

De bonne heure, les législateurs sous d'autres cieux en ont pris conscience, telle qu'en République du Cameroun le nombre des cartes SIM est limité pour les abonnés des SRM. En effet, le DECRET N° 2015/3759 fixant les modalités d'identification des abonnés et des équipements terminaux des réseaux de communications électroniques dispose à son article 4 ce qui suit :

« (1) Une personne physique ne peut détenir plus de trois (03) modules d'identité d'abonné par opérateur. (2) Toute demande d'un nombre de modules d'identité d'abonné supérieur au nombre mentionné à l'alinéa 1 ci-dessus, est soumise à l'autorisation préalable de l'Agence en charge de la régulation des communications électroniques, à la diligence de l'opérateur. »

De même qu'au Rwanda l'acquisition des cartes SIM est limitée en nombre pour les abonnés de chaque SRM tel que soutenu par le Règlement N°004/R/ICTIRURA/2018 du 26/04/2018 régissant

[25]La « temibilita » est un concept dont la paternité est attribuée à Garofalo désignant la quantité de mal qu'on peut redouter de la part d'un criminel ; en d'autres termes, sa capacité criminelle. Ce terme se traduit parfois par ceux de périculosité, de dangerosité, de redoutabilité.

[26] Interview réalisé sous anonymat auprès des consommateurs des services des Sociétés de Réseaux Mobiles Airtel et Africel ainsi que leurs revendeurs.

l'enregistrement des cartes SIM au Rwanda à son l'article 20 qui dispose ce qui suit :

« Limitation du nombre de cartes SIM La limite de la propriété de la carte SIM sous chaque titulaire de licence est la suivante: 1) Trois (3) cartes SIM sous une seule Carte d'identité 2) Une Carte SIM(1) sous un seul passeport.

Cependant le maximum de cartes SIM autorisées pour chaque abonné ne doit pas dépasser six (6) Cartes SIM. Si pour des raisons valables, il y a besoin de carte SIM supplémentaires, l'abonné doit demander l'autorisation auprès de l'autorité de régulation. »

En fait, si les législateurs des autres États ont incorporé ces dispositions dans leur arsenal juridique, ce qu'elles justifient d'un certain intérêt ou bien fondé, qualifié tantôt de « ratio legis » dans les lignes précédentes. Tout en gardant l'idée de la lutte contre la prolifération des cartes SIM dont la solution s'avère être les lois obligeant leur usage limité en nombre, ces détails visent démontrer combien cela contribue tant soi peu à la politique de prévention des criminalités facilitées par l'avènement des NTIC en générale le manque de protection des cartes SIM en particulier qui ouvrent voie aux atteintes graves contre l'identité des abonnés mettant ainsi en péril leur intérêts tant patrimoniaux qu'extrapatrimoniaux.

De ce qui précède, l'absence des sanctions pour des violations implicites des normes d'identification et l'absence d'incrimination pour des pratiques potentiellement dangereuses sont à la base de prolifération des cartes SIM, un phénomène que le criminel peut exploiter à son avantage en troublant l'ordre public et en mettant péril les intérêts des particuliers. C'est à ce niveau que l'intervention de l'autorité de régulation doit s'affirmer pour une protection plus efficace et plus effective.

2.2.2. Du rôle de l'autorité de régulation dans la protection

Le principe de la légalité concerne non seulement les faits infractionnels et les sanctions y afférentes, mais également les institutions et services de l'État qui ne peuvent exister ab nihilo. C'est la loi qui prévoie leur création, leurs missions ainsi que leurs animateurs etc. Eu égard à ce principe, ce paragraphe présentera la référence textuelle qui consacr

Les missions de l'**A**utorité de **R**égulation de **P**oste et de **T**élécommunications au **C**ongo (ARPTC), en vue d'analyser son rôle dans la prévention des actes attentatoires à l'identité via carte SIM et par ricochet le rôle de l'ARPTC dans la protection des abonnés des SRM.

L'article 1er de la loi n° 014-2002 du 16 octobre 2002 portant création de l'Autorité de régularisation de la poste et des télécommunications dispose ce qui suit :

« *Il est institué, en République démocratique du Congo, un organe indépendant de régulation de la poste et des télécommunications dénommé, Autorité de régulation de la poste et des télécommunications du Congo, A.R.P.T.C. en sigle. L'Autorité de régulation de la poste et des télécommunications du Congo est une personne morale de droit public dotée de la personnalité civile.* »

La disposition sous examen fait principalement allusion à l'autorité de « régulation », entre les mains de qui se concentrent toutes les missions qui seront analysées infra. Ainsi connaitre ce qu'elle est, s'avère impérieux pour mieux comprendre ses missions légales.

Plusieurs définitions gravitent autour de la notion de « régulation », chacune selon le domaine touché par celle-ci . Selon la sociologie politique le terme de régulation prend un sens plus général. Il regroupe l'ensemble des règles et des institutions qui permettent la vie en société en garantissant un certain ordre public, un certain niveau de paix sociale; En droit public français, elle s'exprimerait par la notion classique de police administrative[27].

La régulation constitue alors l'ensemble des opérations consistant à recevoir des règles, à en superviser l'application, ainsi qu'à donner des instructions aux intervenants et régler les conflits entre eux lorsque le système de règles est perçu par eux comme incomplet ou imprécis[28].

Quant à la présente disposition, l'expression « autorité de régulation » dans le secteur des télécommunications renvoie in concreto au service public de l'État dont le rôle est celui d'une part de veiller sur l'application des règles régissant ledit secteur en vue d'y maintenir l'ordre public et la paix sociale par une politique claire de prévention des crimes et d'autre part de maintenir un équilibre économique optimal en contrôlant par exemple la concurrence entre les SRM et en protégeant les consommateurs de leurs services et produits contre tout acte dolosif . Ces détails explicatifs se rapportent donc concomitamment à la notion classique de police administrative et l'interventionnisme étatique dans la vie économique. Avec cette modeste lumière apportée sur l'expression « autorité de régulation » il est plus aisé de déterminer et de comprendre les missions dévolues à l'ARPTC prévues à l'article 3 de la même loi sous examen.

En substance, ce prescrit de l'article 3 reprend l'idée du rôle de la police administrative qui est censé définir une politique d'anticipation criminelle en vue garantir l'ordre publique, la paix sociale et par ricochet l'intérêt général tel que le stipule le point notamment le point « *i* » en ces mots : « *assurer la continuité du service et protéger l'intérêt général*.»

[27] A-S. MESCHERIAKOFF, *Droit public économique, PUF, Paris, 1996, p.23*

[28] B.MARAIS, Droit *public de la régulation économique*, Presses de sciences PO et Dalloz, Paris, 2004, p.484.

Aussi, en plusieurs sous-points l'article 3 martèle sur l'idée du rôle régulateur de l'État dans vie économique où son interventionnisme est clairement défini au sous-point «*l*» qui stipule que l'ARPTC a également pour mission de *« protéger sur le marché des postes et télécommunications, les intérêts des consommateurs et des opérateurs en veillant à l'existence et à la promotion d'une concurrence effective et loyale et prendre toutes les mesures nécessaires à l'effet de rétablir la concurrence au profit des consommateurs. »*

L'interventionnisme étatique dans le secteur économique étant hors sujet à cette réflexion, la préoccupation majeure demeure cependant celle de vérifier dans la pratique le dégrée auquel l'ARPTC contribue in globo à la garantie de l'intérêt général en protégeant l'identité des abonnés via cartes SIM.

Les SRM demeurent des partenaires incontournables pour l'ARPTC étant donné qu'elles représentent les champs d'action pour cette dernière. C'est au travers les activités des SRM que l'ARPTC peut dans le maintien de l'ordre publique et de la paix sociale, en administrant les activités de ce secteur les STC posent des actes au quotidien qui peuvent contribuer au succès ou à l'échec de la mission de l'État de garantir l'intérêt général.

En effet, « la notion d'intérêt général est, aujourd'hui, autant un concept du droit qu'un *topos* rhétorique. Elle est censée désigner l'ordre public, l'intérêt du peuple ou bien la priorité des décisions administratives sur les intérêts privés, sectoriels, les droits individuels et les contrats entre particuliers.»[29]. Dans cette perspective, l'État peut imposer aux particuliers, certaines restrictions affectant leur liberté, celle de ne pas agir à leur guise en vue de prévenir tout comportement liberticide. Éviter les comportements qui violent les libertés des autres est une obligation morale et juridique qui s'impose erga omnes, valable à toutes personnes, qu'elles soient physiques ou morales.

Les SRM étant de la catégorie des personnes morales de droit privé sont aussi concernées par l'interdiction des comportements liberticides qui méritent un contrôle de la part de l'autorité régulatrice de leur secteur, l'ARPTC.

L'obligation légale qui semble avoir plus connu de succès en termes de l'effectivité est celle de l'identification des abonnés à cause du mécanisme mis en place par les SRM consistant à rendre inopérationnelle toute carte SIM si elle n'est pas identifiée lors de son achat. Ce mécanisme purement technique prive momentanément le réseau à son utilisateur s'il jusqu'à ce qu'il se fasse identifier numériquement à sa carte SIM moyennant sa carte d'identité.

Malheureusement d'autres comportements illégaux se sont invités dans les activités commerciales des SRM qui fragilisent ce mécanisme technique mise en place pour obliger les abonnés à se faire identifier. En effet, comme déjà évoqué supra, certaines SRM vendent des cartes SIM pre-identifiées au nom des autres abonnés ce qui engendre comme conséquence l'incohérence d'identité entre l'utilisateur et la personne enregistrée dans le système. Etant donné que l'utilisateur est censé être également la personne enregistrée, sauf preuve contraire, il se pose déjà un sérieux problème de violation de l'identité de la personne enregistrée.

Cela est souvent possible lors que les cartes d'électeurs sont perdues ou lorsque leurs photocopies sont jetées par leurs propriétaires après avoir sollicité un service nécessitant une identification au préalable tel que les banques, les Shop-Money, etc. Alors les revendeurs des SRM recourent à ces procédées pour vite vendre car le nombre écoulé des cartes SIM représente déjà un gain et pour eux-mêmes et pour la SRM (.)[30]

Parfois ils recourent également aux cartes d'identité de leurs membres de familles, amis et connaissance pour activer vite écouler les cartes SIM. Le comportent est motivé par le gout du lucre qui anime tout opérateur économique[31].

Pour éviter cette pratique fourbe, l'article 2 al.3 de l'arrêté interministériel n°25/CAB/VPM/MIN/ INTERSEC/024/2015 fixant les conditions de souscription à l'abonnement téléphonique en République Démocratique du Congo interdit l'identification par procuration qui consiste ici pour un porteur d'une pièce d'identité appartenant à autrui ,de la faire enregistrer de la part de son titulaire.

En fait, la ration legis de cette disposition légale vise éviter l'usurpation d'identité numérique par une personne qui se serait procurée illégalement une carte d'identité d'autrui. Cependant il y a lieu d'exprimer le regret à deux niveaux :

1) Au niveau des SRM qui de part de leur qualité,elles sont censées protéger les intérêts de leurs abonnés en respectant les normes régissant leur secteur en prévoyant tout éventuel crime. Mais ce sont elles qui violent implicitement la loi.

2) Au niveau de l'ARPTC, bras séculier de l'État, police et arbitre, elle n'est finalement qu'un gendarme sourd-muet, au gourdin laxiste, à cause de la

[29] J.CHEVALLIER, « L'intérêt général dans l'administration française », *Revue internationale des sciences administratives*, 1975, vol. XLI, n° 4, p. 325-350.

[30] Propos recuillis de Mastajabu Samuel ,revendeur des produits de SRM airtel à Goma

[31] Renseignements concordants fournis par Samy MASTAJABU et Benjamin AMINI, respectivement les revendeurs des produits des SRM Airtel et Africel à Goma.

complaisance dont elle fait visiblement montre face aux violations des normes qui regissent son secteur au lieu de sanctionner sévèrement ses assujettis (SRM) en ce sens que l'impunité est le bouillon favorable de criminalité.

Aussi, reprochée d'être un « service fantôme », l'ARPTC n'a jamais pu décentraliser ses services dans toutes les provinces et villes de la RDC, elle est installée seulement à Kinshasa la capitale[32]. Comparativement aux autres institutions de l'État, sa visibilité fait défaut. S'il existerait du moins un endroit bien localisable proche de la population pour dénoncer les antivaleurs qui gangrènent le secteur de la télécommunication. Pour cela elle doit disposer des infrastructures comme tous les autres services de l'État (bâtiments, matériels du bureau, engins roulants, etc) pour jouer fidèlement son rôle.

Conclusion générale

Cette modeste réflexion sur « les enjeux et défis de protection d'identité des abonnés via carte sim en RD Congo » a révélé qu'on ne saurait nier qu'une protection effective et efficace de l'identité des abonnés via carte sim doit son succès à plusieurs acteurs. Comme les engrenages d'une machine, grands ou petits, leur taille importe peu, ce qui compte, est que chacun incarne fidèlement son rôle pour que la machine fonctionne à merveille. Il en est de même pour l'État congolais et les SRM. L'apport de chaque prestataire est d'une importance sans mesure pour la sécurité de tous.

Ainsi donc, à la lumière de ce qui précède, les recommandions suivantes sont à considérer pour une sécurité plus efficace et effective en faveur des abonnés des SRM :

Au niveau de l'État :

1) Le législateur doit édicter des lois spéciales adaptées aux enjeux et aux défis qui entourent de protection d'identité des abonnés via carte SIM, la solution demeure l'identification biométrique qui permet de singulariser davantage chaque abonné de SRM en réduisant considérablement les risques de tomber victime d'usurpation d'identité qui peut porter atteinte aux droits patrimoniaux et extrapatrimoniaux d'une personne.

Aussi, pour celui qui a perdu sa carte d'identité contenant les biens numériques de valeur, ça ne vaudra plus la peine de lui imposer l'impossible gymnastique de fournir la preuve de sa propriété étant donné que les organes de son corps peuvent faciliter l'identification en occurrence par l'empreinte digitale, la reconnaissance faciale, etc.

Quant aux normes préexistantes il faut y ajouter de sanctions à cause du rôle intimidant de la peine. En effet, une interdiction sans sanction peut être un facteur de l'ineffectivité d'une norme comme cela a été constaté à propos de celles qui régissent l'identification des abonnés.

2) Au niveau de l'ARPTC, elle doit divorcer avec toute attitude de complaisance à l'égard de ses assujettis, les SRM, en les sanctionnant plus sévèrement selon les peines prévue pour l'infraction par elles commises, surtout que la responsabilité pénale des personnes morales et leurs sanctions sont déjà envisageables en droit congolais. La visibilité de l'ARPTC peut aussi favoriser l'effectivité et l'efficacité de son rôle de régulation dans le secteur de la télécommunication. En effet,sa reputation de service fantôme du à l'absence d'infrastructure (bâtiment, engins roulant) et à son absence sur toute l'étendue du pays excepté Kinshasa. Résoudre ces deux défis rendra son pouvoir bien affirmi pour indiguer les antivaleurs du domaine.

3) Au niveau des SRM, en tant que partenaires incontournables de l'ARPTC, elles doivent moderniser leurs équipements et infrastructures pour faciliter les enquêtes, -elles doivent renforcer la performance de leurs agents par des formations spécialisées dans le domaine technologique, -elles doivent être affables à la coopération avec la justice ou toute autre institution étatique et collaborer ensemble quotidiennement pour la prévention des crimes, -elles doivent se surpasser de leurs intérêts lucratifs lorsqu'il s'agit de dénoncer leurs abonnés impliqués dans les activités criminelles, -en fin, elles doivent développer du professionnalisme dans la gestion quotidienne de leurs services, ce qui permettra d'éviter les maladresses qu'on leur a toujours reprochées et dont peuvent profiter les criminels.

BIBLIOGRAPHIE

I. Ouvrages

1. A-S. MESCHERIAKOFF, *Droit public économique, PUF, Paris, 1996*

2. B.MARAIS, Droit *public de la régulation économique*, Presses de sciences PO et Dalloz, Paris, 2004

3.Dictionnaire Universel, Hachette Edicef ,5e éd. 2008

G. CORNU, Association Henri Capitant, *vocabulaire juridique*, Paris 10e éd. PUF, 2014, *v «* identité. »

4.V. Gautron, *La Fin de la singularité du modèle français de prévention de la délinquance*, AJ pénal 2007

5.C.KAKULE KALWAHALI, *Droit pénal général*, Edition Blessing, Kampala, Janvier 2017

6. Voire B.C. NYANGEZI, *les infractions de A à Z*, 1ere Édition, Laurent Nyangezi, Kinshasa, 2011

II.Sources Legislatives

[32] Propos recueillis du magistrat Claver KAHASA à propos de la coopération de la justice avec l'ARPTC

1. Loi n° 20/017 du 25 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication

2. Arrêté interministériel n°25/CAB/VPM/MIN/ INTERSEC/024/2015 fixant les conditions de souscription à l'abonnement téléphonique en République Démocratique du Congo

3. Loi n° 18-019 du 9 juillet 2018, relative aux systèmes de paiement et de règlement-titres (J.O.RDC., 23 juillet2018, n° spécial, col. 53)

4. Loi n° 87 /010 du 1er août 1987 portant code de la famille

5. Loi n° 15/022 du 31 décembre 2015 modifiant et complétant le Décret du 30 janvier 1940 portant code pénal,

6. Ordonnance loi 23-010 du 13 Mars portant code du numerique

7. Règlement n°004/R/ICTIRURA/2018 du 26/04/2018 régissant l'enregistrement des cartes SIM au Rwanda

8. DECRET n° 2015/3759 fixant les modalités d'identification des abonnés et des équipements terminaux des réseaux de communications électroniques au Cameroun ,

9. loi n° 014-2002 du 16 octobre 2002 portant création de l'Autorité de régularisation de la poste et des télécommunications

III.REVUES

1. J.CHEVALLIER, « L'intérêt général dans l'administration française », *Revue internationale des sciences administratives*, 1975, vol. XLI, n° 4,.

III.Sources internet

1. J. DJOGBENOU**,** *La cybercriminalité : enjeux et défis pour le Bénin*, disponible sur http://www.capod.org

2. « Carte Sim, les formats », htps:/lwyy, hten.frl blog

3. Encyclopédie libre, « Axiologie » disponible sur Axiologie — Wikipédia (wikipedia.org)

4. Identification des abonnés de réseaux de communications électroniques : quelle approche de protection des données dans un cadre légal insuffisant ? - Digital Business Africa

5. DeCew, Judith, « Privagy », Stanford Engyclopedia of Philosophy Arsbins, www.plato.stanford.edu/archives/spr2015/entries/privacy, cité dans « vie privée » En anglais, *« The right to be let alone »* : Warren, Samuel et Brandeis, Louis, « The Riht privacy », Harvard Law Review,n°5,15décembre1890,htn://groups.csail.mit.edu/mac/classes /6805/articles/privacy/privacy_brand_war Zhtml, cité dans « Vie privé », Wikipédia. Org/ wiki/ Vie-privée

V.Interview

1. Avec les agents des SRM Airtel,Vodacom et Orange

2. Les revendeurs des produits airtel et orange

3. Les abonnees de SRM Airtel,Vodacom Orange et Africell