tic&société

Vol. 10, N° 1 | 2016
Contrôle social, surveillance et dispositifs numériques

La régulation des usages des TIC en Côte d'Ivoire : entre identification et craintes de profilage des populations

Jean-Jacques Maomra BOGUI et N'Guessan Julien ATCHOUA

Éditeur
Association ARTIC

Édition électronique
URL : http://ticetsociete.revues.org/1983

Référence électronique
Jean-Jacques Maomra BOGUI et N'Guessan Julien ATCHOUA, « La régulation des usages des TIC en Côte d'Ivoire : entre identification et craintes de profilage des populations », *tic&société* [En ligne], Vol. 10, N° 1 | 1er semestre 2016, mis en ligne le 24 octobre 2016, consulté le 07 novembre 2016. URL : http://ticetsociete.revues.org/1983

La régulation des usages des TIC en Côte d'Ivoire : entre identification et craintes de profilage des populations

Jean-Jacques Maomra BOGUI et N'Guessan Julien ATCHOUA

Introduction

1 Depuis les années 1990, l'insertion sociale des technologies numériques et leur appropriation par les citoyens sont devenues un enjeu important pour le développement et la démocratisation des États africains. Chéneau-Loquay (2011) fait remarquer dans cette perspective que « les TIC sont un secteur majeur de la croissance récente d'une nouvelle économie informelle dans les villes africaines ».

2 Cependant, malgré la bonne santé de l'économie liée aux télécommunications et technologies de l'information et de la communication (TIC), le développement de l'usage d'Internet occasionne également de nombreuses menaces sur le rayonnement économique de plusieurs pays africains et leur image à l'extérieur en raison du développement important des arnaques réalisées à l'aide des outils numériques (téléphone cellulaire et Internet) aussi bien à l'intérieur des pays qu'au plan international. Cette situation va être le prétexte d'une importante campagne d'identification des usagers des technologies numériques dans différents pays africains (Côte d'Ivoire, Niger, Cameroun, etc.) en vue de réguler les activités dans le cyberespace et permettre sa sécurisation. Dans la présente étude, nous nous sommes particulièrement intéressés au cas de la Côte d'Ivoire, dont la campagne d'identification des usagers des TIC s'est achevée le 31 décembre 2012 avec un taux de pénétration de leur usage de 85,43 % pour 19,8 millions d'abonnés selon l'Agence de régulation des télécommunications de Côte d'Ivoire (ARTCI, 2012).

3 La nécessité pour les décideurs ivoiriens de freiner l'expansion de ces détournements d'usage, facteurs d'insécurité et de détérioration de l'image du pays (Bogui, 2010), a suscité la prise de dispositions en vue de réguler le cyberespace ivoirien au risque de participer au contrôle social d'un « espace public fragmenté » (Miège, 1995). L'identification en 2012 des abonnés aux services des réseaux de communication mobiles par l'application du « décret n° 2011-476 du 21 décembre 2011 portant identification des abonnés des services de télécommunications ouverts au public », l'érection de structures de lutte contre la cybercriminalité (PLCC) ainsi que l'implication de la police scientifique dans l'opération sont, entre autres, les mesures prises par l'État de Côte d'Ivoire pour assurer la régulation des usages des TIC dans le pays.

4 Cette politique de régulation qui a connu une phase de sensibilisation, d'identification et de répression, entraîne néanmoins des interrogations sur les enjeux politiques et économiques inavoués du processus d'identification des abonnées au mobile et à Internet et sur la place accordée à la préservation de la vie privée du citoyen dans un processus de surveillance et de contrôle des usages des TIC.

5 Nombreuses sont les études qui, depuis au moins deux décennies, s'intéressent au potentiel des TIC comme vecteur de développement économique, social et humain en Afrique. En effet, depuis l'avènement des technologies numériques, un discours antagoniste s'est développé dans le milieu universitaire entre les chercheurs qui perçoivent les nombreux usages totalement inédits observés plus particulièrement dans l'usage de la téléphonie mobile (*mobile commerce*, *mobile banking*, etc.) comme la preuve de la capacité de ces outils à sortir les pays du tiers-monde du sous-développement (Loukou, 2013) et ceux qui mettent l'accent sur les limites de cette thèse (Alzouma, 2008 ; Kamga, 2006). Le potentiel de ces technologies à favoriser l'émergence de sociétés plus démocratiques a été également souvent mis en avant (Kiyindou, 2010, 2012). Gingras explique à ce propos que :

> « les caractéristiques des réseaux électroniques, comme l'accès à l'information, l'interactivité, la numérisation et la transmission à haut débit suscitent un optimisme fondé sur l'idée que pourront être réalisés deux des plus chers idéaux de la démocratie qui concernent directement la sphère publique : la transparence et l'agora » (2009, p. 216).

6 Cependant, le potentiel de contrôle et de surveillance de ces technologies numériques qui fait régulièrement débat, notamment depuis la récente affaire Snowden[1] en Occident, est encore très peu abordé dans le contexte africain. Notre article ambitionne de combler cette lacune à travers la contextualisation de ce phénomène mondial.

7 En effet, la surveillance s'est intensifiée ces dernières années dans nos sociétés contemporaines avec le développement des TIC. Elle exerce de nos jours une telle emprise sur le quotidien des citoyens qu'il est pratiquement impossible d'y échapper. Lyon (2001, p. 1) traduit bien cette situation en ces termes : « Everyday life is subject to monitoring, checking, scrutinizing. It is hard to find a place, or an activity, that is shielded or secure from some purposeful tracking. [...] ».[2]

8 Bien que cet article se présente en premier lieu comme une réflexion théorique sur la question du contrôle social et de la surveillance générés par l'adoption des dispositifs numériques en Afrique, il s'appuie également sur des informations recueillies grâce à une recherche qualitative réalisée à travers des entretiens semi-directifs auprès de quelques-uns des principaux acteurs chargés de la régulation du cyberespace en Côte d'Ivoire. Cette méthode et les techniques d'entretien semi-directif suscitées sont apparues comme les

plus adaptées à notre objectif de recherche. En outre, le peu d'intérêt accordé à la question de la surveillance numérique dans la recherche universitaire et dans le débat sociopolitique en Côte d'Ivoire au moment de nos investigations a constitué une entrave à l'obtention d'informations clés sur cette question qui apparaissait comme un sujet tabou. Les entretiens exploratoires de types semi-dirigés ont pu être néanmoins réalisés en 2013 et 2014 auprès d'un corpus de 20 participants constitués d'acteurs et de responsables de structures étatiques ou privées chargées de la régulation du cyberespace en Côte d'Ivoire. Il s'agit de responsables de la direction de l'informatique et des traces technologiques (DITT) de la police scientifique ivoirienne, de l'Agence de régulation des télécommunications de la Côte d'Ivoire (ARTCI), ainsi que de responsables et agents de cellules d'identification des six opérateurs de téléphonie mobile et fournisseurs d'accès Internet (Orange, MTN, Moov, Koz, Green et Café Mobile) que compte le pays. Il s'est agi de recueillir auprès de ces participants leur avis sur le mode opératoire du processus d'identification des abonnés au mobile et à Internet, sur les difficultés rencontrées pendant le processus, sur les enjeux économiques et politiques de cette initiative, sur les mécanismes mis en place pour assurer le respect de la vie privée des citoyens.

9 Au total, les données recueillies au cours de cette enquête réalisée par le canal d'un guide d'entretien ont permis, en plus des explorations documentaires, d'obtenir des résultats intéressants qui ont contribué à notre réflexion théorique.

10 Cet article se structure en trois parties. La première partie est consacrée à quelques considérations théoriques sur les enjeux de la surveillance dans nos sociétés contemporaines et sur le potentiel de contrôle et de surveillance des technologies médiatiques ; la seconde partie traite des enjeux économiques du processus d'identification des usagers des TIC en Côte d'Ivoire ; enfin, la troisième et dernière partie s'intéresse aux enjeux politiques de l'identification des usagers des TIC en Côte d'Ivoire.

Quelques considérations théoriques

Foucault et la métaphore du panoptique

11 La métaphore du panoptique a été régulièrement utilisée ces dernières années pour décrire les formes de surveillance qui se sont développées dans nos sociétés contemporaines. Cependant, bien que ce cadre théorique ait été pendant longtemps considéré comme pertinent, les nouvelles caractéristiques des technologies numériques ont mené plusieurs chercheurs à repenser la question du renforcement de la surveillance à l'ère de ces outils numériques (Deleuze, 1990 ; Haggerty et Ericson, 2000 ; Ball, 2005 ; Leclercq et Isaac, 2013).

12 C'est dans son ouvrage intitulé *Surveiller et punir* paru en 1975 que M. Foucault a développé la métaphore du panoptique. L'approche de Foucault s'inspire du modèle architectural de la prison panoptique du XVIII^{e} siècle inventée par J. Bentham et qui peut également s'appliquer à différents établissements d'enfermement (usines, écoles, etc.). Selon Ottoviani (2003), dans cette configuration, « le pouvoir est une sorte de présence absente, une virtualité, puisqu'on ne peut jamais savoir si l'on est effectivement surveillé à tel ou tel moment, mais il est cependant doté d'effets réels ». Comme l'indique Foucault (1975, p. 235), « celui qui est soumis à un champ de visibilité, et qui le sait, reprend à son compte les contraintes du pouvoir. [...] Il devient le principe de son propre

assujettissement ». Le panoptique pour Foucault (1975, p. 240) est une figure de technologie politique qui peut s'appliquer à divers domaines.

13 La volonté des autorités ivoiriennes de sortir tous les internautes de ce pays de l'anonymat à la suite d'une campagne médiatique particulièrement vive en faveur de l'identification de tous les usagers d'Internet en Côte d'Ivoire peut faire apparaître le cyberespace comme un dispositif panoptique. Le but de la manœuvre, comme l'ont confirmé les responsables de la lutte contre la cybercriminalité en Côte d'Ivoire au cours de nos entretiens semi-dirigés, est de faire en sorte que, se sachant désormais identifiés et donc sous surveillance, les usagers du cyberespace dans ce pays soient emmenés à s'autodiscipliner.

14 Pour Leclercq et Isaac (2013, p. 13) :

> « Foucault met ainsi en évidence une articulation entre les processus matériels et physiques de surveillance, et les mécanismes sociocognitifs qui conduisent à l'intériorisation de cette surveillance par les sujets ».

15 Le panoptisme est perçu par Foucault comme l'" un des traits spécifiques aux technologies politiques modernes d'asservissement, la figure moderne des disciplines » (Ragoucy, 2010, p. 49). Pour Foucault, la discipline est une « force positive d'incitation et d'orientation » ; elle est « une fonction normalisatrice » (Ottaviani, 2013). En fin de compte, le panoptique « illustre les rapports de pouvoir quotidiens, diffus dans la société, qui vont bien au-delà de la conception architecturale du panoptique » (Leclercq et Isaac, 2013, p. 14) dans la mesure où, selon Deleuze (1990), il avait conscience de la brièveté du modèle des sociétés de surveillance qu'on pourrait considérer comme transitoire.

L'approche deleuzienne et la société de contrôle

16 Selon Deleuze (1990), on a vu depuis l'époque classique se succéder trois types de société, à savoir la société de souveraineté, la société disciplinaire et la société de contrôle. Il observe une concordance entre ces différents types de société et l'évolution de la nature des techniques utilisées. Ainsi, les grands progrès observés dans le domaine de l'informatique seraient à l'origine de cette société de contrôle. Cette situation s'expliquerait par l'évolution d'un système économique de moins en moins concentré. Cette évolution va entraîner la mise en œuvre de nouveaux dispositifs de surveillance et de contrôle.

17 Pour lui, les milieux d'enfermement disciplinaires laissent progressivement la place à des « formes ultra-rapides de contrôle à l'air libre. [...] Ce qui compte ce n'est pas la barrière, mais l'ordinateur qui repère la position de chacun, licite ou illicite, et opère une modulation universelle » (Deleuze, 1990). Comme le souligne Lyon :

> « [...] Humans are surrounded, immersed, in computing and networked technologies from dawn to dusk and in every conceivable location. Not only is the employee able to access the building or the computer terminal only with a coded key, all environments are either hardwired or wirelessly able to sense where people are, what they are doing and where they are going. Even "wilderness" hikers have global positioning system (GPS) devices to indicate where they are at any given moment » (2007, p. 1)[3].

18 Dans une analyse comparative des caractéristiques entre le système disciplinaire (Foucault) et la société de contrôle (Deleuze) effectuée par Leclercq et Isaac (2013, p. 18), il ressort, entre autres, que si le principe de la société de surveillance est de constituer des moules normalisateurs des comportements humains, dans la société de contrôle le

principe est la modulation (variation d'un instant et d'un lieu à l'autre). Les dispositifs de surveillance dans l'approche foucaldienne se caractérisent par la visibilité permanente des corps, la normalisation et le dressage alors que dans l'approche deleuzienne le contrôle se fait à « l'air libre » (computation des traces codées). La nouvelle politique d'identification des usagers du cyberespace ivoirien décidée par les autorités de ce pays peut ainsi laisser percevoir la volonté de mettre en place un dispositif de contrôle des citoyens plus en phase avec l'approche deleuzienne d'" assemblage de surveillance » ou « rhizomique ». Cette décision augure la mise en place progressive d'une société où les technologies numériques permettent un contrôle qui ne nécessite pas une visibilité permanente de l'individu.

19 Plusieurs auteurs anglo-saxons tels que Haggerty et Ericson (2000) et Ball (2005) vont s'inspirer de l'idée d'" assemblage de surveillance » et de la métaphore du « rhizome[4] » développée par Deleuze et Guattari (1980) pour expliquer le système de surveillance à l'œuvre dans nos sociétés contemporaines marquées par un développement important de nouvelles technologies numériques :

> "This assemblage operates by abstracting human bodies from their territorial settings and separating them into a series of discrete flows. These flows are then reassembled into distinct "data doubles" which can be scrutinized and targeted for intervention » (Haggerty et Ericson, 2000, p. 606)[5].

20 En effet, avec certaines technologies telles que les GPS ou les cartes à puce, la surveillance ne nécessite plus de contact visuel comme dans le système disciplinaire foucaldien. L'homme est quelque peu déshumanisé. Il doit cohabiter avec un « double numérique » qui permet à un agent de surveillance d'avoir accès à une multitude d'informations sur sa vie :

> « Data doubles circulate in a host of different centres of calculation and serve as markers for access to resources, services and power in ways which are often unknown to its referent » (Haggerty et Ericson, 2000, p. 613)[6].

21 La surveillance par assemblage ou rhizomique facilite une vision d'ensemble et un regard suffisamment puissant pour être capable d'atteindre les profondeurs de l'intimité de l'individu.

22 Toutefois, on peut relever que dans le contexte actuel où l'usage quotidien des technologies numériques devient inéluctable pour les citoyens, tout le monde peut à la fois surveiller et être victime de la surveillance. La surveillance devient de plus en plus privée ; elle se transforme même en divertissement, ce qui entraîne une forme d'indifférence face à son emprise.

L'État, les entreprises et les dispositifs de surveillance

23 Les informations personnelles des citoyens sont aujourd'hui plus faciles à acquérir grâce au réseau Internet (connaissances de l'identité, des habitudes de navigation, de consommation, etc.). Selon Gingras (2009, p. 219) :

> « L'amélioration de la gestion sert d'argument parapluie pour l'introduction des technologies médiatiques ; parmi les avantages ciblés, on note une augmentation de la rapidité et de l'efficacité des services, la simplification des rapports avec l'État et une meilleure prise en compte des besoins des clientèles grâce à leur connaissance accrue ».

24 Certains auteurs parlent également de profilage de la population qui se définit selon Mattelart et Vitalis, 2014, p. 5) comme :

> « [...] une forme de contrôle indirect des individus à partir de l'exploitation des informations prélevées sur eux. Du livret ouvrier aux registres de police et aux fichiers manuels, jusqu'à l'apparition de l'Informatique puis de l'Internet, cette forme de contrôle n'a cessé de se perfectionner et de s'étendre. [...] Des forces de l'ordre à la banque, des services de renseignement au marketing, en passant par l'institution scolaire et les services psychomédicaux, peu de secteurs d'activité y échappent ».

25 Dans leur ouvrage intitulé *The Surveillance-Industrial Complex : A Political Economy of Surveillance* (Ball et Snider, 2013), les auteurs examinent les liens entre le capital et l'État néolibéral dans la promotion, l'émergence et la croissance de la société de la surveillance. Dans une approche de l'économie politique qu'ils définissent comme l'interconnexion des processus sociaux, politiques et économiques (Ball et Snider, 2013, p. 1), ces auteurs considèrent que la lutte contre le terrorisme a donné aux gouvernements et aux entreprises privées en Occident l'opportunité d'accroître le contrôle social et de faire du profit. On assisterait ainsi à un accès sans précédent aux données personnelles des individus glanés dans le secteur privé, de même qu'à un renforcement de partenariat public-privé pour le financement de la production de nouveaux dispositifs de surveillance (Ball et Snider, *ibid.*). Une intensification du contrôle aux frontières dans un climat de méfiance et de peur entretenu au sein de la population légitime cette situation. Cependant, la lutte contre le terrorisme ne peut tout expliquer, car l'accès aux données personnelles des citoyens est aujourd'hui une véritable mine d'or pour les entreprises. On peut sans doute considérer la mission d'identification des usagers des technologies numériques confiée aux opérateurs de téléphonie mobile et des services Internet par l'État de Côte d'Ivoire dans le cadre de la lutte contre la cybercriminalité comme un exemple de mise en place de partenariat public-privé dans le contexte ivoirien en vue de renforcer la surveillance des usagers du cyberespace dans ce pays. Ce partenariat qui renforce l'accès de ces entreprises privées aux données personnelles des citoyens conduit à des interrogations sur l'usage que ces entités commerciales pourraient en faire.

26 Au moment où nous rédigeons cet article, nous apprenons qu'un recours collectif vient d'être déposé contre la compagnie de télécommunication Bell au Canada pour violation de la vie privée en rapport avec un programme de publicité ciblé[7]. En effet, comme le soulignait Gandy (1993), on assiste depuis quelques décennies pour des besoins de stratégies marketing à ce qu'il qualifie de tri panoptique, une surveillance de la consommation au détail. Les données de consommation sont recueillies et analysées par des moyens technologiques, ce qui permet aux entreprises de faire des offres ciblées à divers catégories et segments de clients. Fuchs (2011) montre dans un article intitulé « *Web 2.0, Prosumption, and Surveillance* » comment, au mépris de la vie privée, une compagnie comme Google accumule des profits par la marchandisation des données personnelles des utilisateurs auprès des annonceurs. Dans son article, Fuchs met l'accent sur le service Google Buzz qui fait partie de l'empire Google de la surveillance économique. Ce service rassemble des données sur le comportement et les intérêts des utilisateurs afin de les stocker, de les évaluer et de les vendre à des annonceurs publicitaires.

27 Comme on peut le constater, les enjeux économiques reliés à la surveillance des usagers des TIC sont très importants pour le monde de l'entreprise en Occident. L'accès aux données personnelles et leur vente constituent une activité lucrative pour les entreprises opérant dans le domaine du numérique. On peut légitimement s'interroger sur ce qu'il en est dans le contexte des pays en développement.

Enjeux économiques du processus d'identification des usagers des TIC en Côte d'Ivoire

Le marché des TIC en Côte d'Ivoire et en Afrique : le succès remarquable de la téléphonie mobile

28 Selon une étude[8] publiée par GSMA[9], l'Afrique subsaharienne est le « leader mondial » en ce qui concerne « la croissance et l'impact de la téléphonie mobile ». Entre 2007 et 2012, le nombre d'abonnés au téléphone mobile en Afrique subsaharienne a augmenté de 18 % en moyenne chaque année. Cela constitue la meilleure performance au monde. En 2013, on dénombre 253 millions d'abonnés mobiles uniques et 502 millions d'abonnements (cartes SIM uniques ou numéros de téléphone) contre 105,2 millions et 165,6 millions respectivement en 2007. Selon les estimations de GSMA, en 2017, le sous-continent devrait compter 346 millions d'utilisateurs uniques, soit un taux de pénétration de 37,6 %, contre à peine 14,6 % en 2007, ce qui constituera une progression de vingt points en une décennie.

29 L'industrie mobile représente à ce jour en Afrique 3,3 millions d'emplois et contribue à plus de 6 % du PIB de l'Afrique subsaharienne, contre 4 % en Amérique latine et à peine 1,4 % dans la région Asie-Pacifique. En 2012, les entreprises du secteur mobile ont apporté 21 milliards de dollars aux caisses des gouvernements de la région. La contribution du secteur devrait doubler d'ici à 2020 pour représenter 6,6 millions de salariés et 42 milliards de dollars de recettes publiques.

30 Plus de 20 millions de personnes sont abonnées au téléphone mobile en Côte d'Ivoire au premier trimestre 2014[10], ce qui équivaut à un taux de pénétration de 83,5 %. Les abonnés prépayés représentent plus de 99 % des utilisateurs. Le chiffre d'affaires global généré par le marché de la téléphonie mobile en Côte d'Ivoire est passé d'un peu plus de 15 milliards de francs CFA (environ 23 millions d'euros) en 1997 à environ 190 milliards de francs CFA (environ 290 millions d'euros) au premier trimestre de l'année 2014.

31 En 2014, selon l'ARTCI, 94 % des parts du marché sont détenus par trois des six opérateurs en activité. Il s'agit d'Orange-CI (36,53 %), MTN (35,82 %) et Moov (21,82 %). Ces trois entreprises sont respectivement des filiales des groupes français France Télécom, sud-africain MTN international et des Émirats arabes unis Etisalat.

32 La compagnie Orange-CI, qui est le leader incontesté du marché des télécommunications en Côte d'Ivoire, pèse à elle seule, avec 8,8 millions d'abonnés, environ 3 % du produit intérieur brut (PIB) ivoirien et 50 % du chiffre d'affaires global généré par le secteur des télécommunications en Côte d'Ivoire, selon son directeur général. Au niveau du cybercommerce, 4 millions d'achats ont été effectués en Côte d'Ivoire en 2014, et une grande partie de ces achats aurait été effectuée par le service de *mobile banking* de la compagnie : « Aujourd'hui, nous avons 3,5 millions d'abonnés au service Orange Money sur lequel il y a une transaction de 6 milliards de francs CFA (12 millions de dollars US) par jour. » [11] À titre de comparaison, on peut relever que la domination de cette multinationale (Orange) du marché des télécommunications est encore plus impressionnante dans certains pays de la sous-région. On note plus de 67 % des parts de marché au Sénégal[12] et plus de 53 % au Mali[13].

La cybercriminalité et ses conséquences sur l'économie en Côte d'Ivoire et en Afrique

33 Malgré son faible nombre d'internautes au milieu des années 2000 (24 millions, soit 2,6 % du total mondial), l'Afrique devient un terrain d'action important pour la cybercriminalité qui a pris de l'ampleur sur le continent au cours de cette période. Les pertes attribuées à la cybercriminalité ont été évaluées, en 2007, à près de 200 milliards de dollars US, une valeur en forte hausse par rapport aux chiffres de 2003 qui étaient d'à peine 20 milliards d'euros (ATCI, 2008). Selon les chiffres de la Plateforme de lutte contre la cybercriminalité en Côte d'Ivoire (PLCC), entre 2009 et le premier semestre de 2013, le pays a subi « un préjudice financier d'environ 26 milliards de francs CFA (environ 40 millions d'euros) ». Les compagnies de télécommunication et plus précisément les fournisseurs d'accès Internet (FAI) font partie des grandes victimes du phénomène de la cybercriminalité, car, sur certains sites Internet de transactions commerciales en Occident, les adresses IP de ces compagnies sont sur des listes noires (Bogui, 2010).

34 Le gouvernement ivoirien devant les conséquences de cette dérive qui touche l'économie ivoirienne en plein cœur et porte atteinte au développement du pays va décider à l'instar d'autres pays de la sous-région (Sénégal, Niger, etc.) de prendre les mesures idoines pour y mettre fin par l'adoption de disposition en vue de renforcer la surveillance et le contrôle des usagers du mobile et d'Internet en Côte d'Ivoire.

35 Selon le diagnostic porté par les autorités ivoiriennes en 2008, plusieurs facteurs favorisaient l'essor de la cybercriminalité. Il s'agit de l'absence de cadre juridique approprié, de l'absence de politique d'identification des abonnés, de l'absence de politique d'identification des usagers Internet dans les cybercafés (70 % des internautes d'Abidjan, selon une étude réalisée par le Cires[14] en 2008), de l'absence de culture de cybersécurité, de la mauvaise prise en charge des cas de cyberescroquerie par la police nationale, de l'absence de structure chargée de la sécurité informatique. Pour remédier à cette situation, en 2008, un plan d'action basé sur les cinq piliers (la sensibilisation, les mesures législatives et réglementaires, les mesures organisationnelles, le renforcement des capacités, la coopération internationale) définis par l'Union internationale des télécommunications (IUT) sur la stratégie de cybersécurité est élaboré.

36 Bien que, selon les autorités ivoiriennes, le marché de la cybercriminalité soit encore estimé à environ 22 milliards de FCFA (33,5 millions euros), grâce aux actions de sensibilisation menées dans le cadre du plan d'action pour la cybersécurité élaboré en 2008, le phénomène est maintenant largement connu du grand public et des décideurs politiques. L'évolution du cadre réglementaire et législatif a mis fin à l'impunité des cyberarnaqueurs. En 2012, on dénombrait 4 265 plaintes reçues et traitées, 176 cyberescrocs condamnés à des peines de prison ferme. La campagne d'identification de tous les abonnés à Internet et au téléphone mobile a permis de mettre fin à l'anonymat des usagers des technologies numériques.

37 Ce processus d'identification qui constitue un élément essentiel de la stratégie de surveillance et de contrôle du cyberespace en Côte d'Ivoire a été perçu par les citoyens ivoiriens comme une véritable révolution dans un pays où jusqu'à cette date le secteur informel jouait un rôle prépondérant dans l'accès aux TIC. Cette décision a ainsi été à la base de nombreuses interrogations des citoyens quant aux réelles intentions du

gouvernement et les conséquences de ces décisions sur la protection de leur vie privée et leur liberté d'action dans le cyberespace.

Enjeux économiques et le pouvoir de surveillance des succursales

38 L'identification présentée comme un moyen efficace de faciliter la régulation des usages des TIC permettra à l'État de Côte d'Ivoire, selon des informations recueillies auprès d'un responsable de l'ARTCI, de maîtriser le nombre des abonnés et le flux des communications. Elle constitue une voie d'ouverture sur d'autres formes d'observations sur l'économie des TIC en Côte d'Ivoire. Ainsi, le gouvernement ivoirien devrait être en mesure de vérifier grâce au pouvoir de contrôle que vont lui permettre les résultats de cette campagne d'identification certaines déclarations des entreprises opérant dans ce juteux secteur des télécommunications sur les transactions qui se font dans le cyberespace ivoirien.

39 On peut tout de même s'interroger sur la décision de l'État de Côte d'Ivoire de confier cette campagne d'identification aux opérateurs de téléphonie mobile et d'Internet. Selon une étude du cabinet Deloitte (2015), une classe moyenne se forme en Afrique et celle-ci souhaite consommer. Cependant, pour les entreprises qui souhaitent investir en Afrique, l'opportunité sera belle, à condition de bien comprendre les demandes de cette nouvelle société de consommation. Selon cette même étude, les consommateurs africains sont de plus en plus connectés[15] et ce niveau élevé de connexion à l'Internet mobile constitue un point clé pour les compagnies qui se tournent vers eux. Il faut rappeler que l'Afrique est, toujours selon Deloitte, le leader mondial dans le domaine du paiement mobile. En effet, l'accès aux données personnelles des clients est aujourd'hui un élément essentiel des stratégies marketing des entreprises (Gandy, 1993 ; Fuchs, 2011), comme nous l'avons rappelé dans la première section de cet article. On peut donc se demander comment le gouvernement ivoirien compte procéder pour s'assurer que toutes les données personnelles des clients recueillies au cours de cette période d'identification ne soient pas utilisées à d'autres fins par ces entreprises. À cette question, nous n'avons pu obtenir de réponses formelles de l'ARTCI. Cette mission d'identification confiée à ces entreprises qui sont pour la plupart des succursales de multinationales peut ainsi apparaître comme un cadeau du gouvernement ivoirien à leur égard. Elle peut être classée dans la lignée des partenariats publics-privés, qui se sont développés en Occident au lendemain des attentats du 11 septembre 2001 sur les questions de sécurité, et qui ont permis la croissance d'une impressionnante économie de la surveillance (Ball et Snider, 2013). Elle est également le reflet de l'influence qu'exercent les multinationales sur les gouvernements africains et de la place incontournable dont elles bénéficient dans l'économie de ces pays.

Enjeux politiques du processus d'identification des usagers des TIC en Côte d'Ivoire

Politique d'identification et surveillance de l'espace public numérique

40 Comme le souligne Ceyhan (2006), « l'identification et la surveillance ne sont pas des pratiques récentes, elles existent depuis la constitution des regroupements humains ».

Selon sa définition, l'identification est « le processus d'assignation, d'attestation, de certification d'une identité reconnaissable au sein d'un groupe ou d'une communauté au moyen de critères relativement stables », tandis que la surveillance consiste en « l'observation, le suivi et l'examen des comportements, des déplacements, des itinéraires, des relations d'une personne », ainsi qu'en « la collecte et le traitement des informations liées à ces actes ». Ces pratiques qui ne sont pas neutres font partie des techniques de pouvoir et de gouvernement de la vie des individus. Ces techniques de surveillance peuvent ainsi être considérées comme un dispositif disciplinaire (Foucault, 1975).

41 L'identification est devenue une condition légale de l'utilisation des TIC en Côte d'Ivoire. Outre l'identification des abonnés, celle des usagers (notamment dans les cybercafés d'où 70 % des internautes ivoiriens ont accès à Internet) est un élément essentiel de cette politique.

42 Bien que la légitimité des actions déployées pour lutter contre les nombreux détournements de l'usage des TIC peut difficilement être contestée, dans le contexte d'un État comme la Côte d'Ivoire qui sort progressivement de plus d'une décennie de crise politico-militaire et qu'on pourrait qualifier de « démocratie en construction », le processus d'identification des usagers des TIC suscite néanmoins des interrogations chez bon nombre de citoyens sur les motivations réelles de l'État ivoirien à faire de cette opération une priorité.

43 L'opération d'identification ne cache-t-elle pas la volonté du gouvernement ivoirien de pouvoir exercer un contrôle plus strict sur cet espace public numérique qui jusque-là lui échappait ?

44 Il nous semble intéressant de relever qu'une étude intitulée *Les Enjeux éthiques d'Internet en Afrique de l'Ouest : Vers un modèle éthique*[16] réalisée plus d'une décennie avant le début de ce processus d'identification (en 1999) par le CRDI[17] et publiée en 2002 montre qu'à l'inverse des citoyens des autres pays d'Afrique de l'Ouest où l'étude s'est déroulée, « les Ivoiriens interrogés sont plus sensibles au fait qu'Internet pourrait être utilisé par le pouvoir à des fins de surveillance » (Brunet, Tiemtoré et Vettraino-Soulard, 2002, p. 61).

45 L'interpellation de blogueurs par la Direction de la surveillance du territoire (DST) dans le cadre de la diffusion des opinions sur le drame des festivités du nouvel an 2013[18] et les arrestations opérées sur la base de message SMS dans le cadre des opérations de ratissage contre les présumés coupables d'attaques armées contre les symboles de l'État entre 2010 et 2013 renforcent ce sentiment de certains citoyens qui, à l'issue de la campagne d'identification, perçoivent encore plus qu'avant les technologies numériques comme un instrument de contrôle et de surveillance de leurs activités dans le cyberespace. En effet, cette régulation permet également à l'État ivoirien de réaffirmer son autorité dans un espace public numérique qui semblait échapper à son contrôle. Ainsi, selon les résultats de nos enquêtes sur le terrain, une collaboration se développe entre les services de la police (police judiciaire et police scientifique) qui reçoivent les plaintes et saisissent la justice qui, en cas de besoin, a recours à l'ARTCI qui sollicite les opérateurs de téléphonie mobile et de services internet pour obtenir des informations sur les usagers suspectés de comportements délictueux dans le cyberespace.

La suspicion générale et les mesures législatives

46 Ces craintes de citoyens seront d'ailleurs confirmées au cours du processus d'identification des usagers des TIC. Selon les agents recenseurs des fournisseurs d'accès Internet et des opérateurs de téléphonie mobile, une forte résistance de certains citoyens a pu être observée pendant l'opération de recensement (refus de présenter une pièce d'identité, par exemple) en raison des traumatismes multiformes sur la vie quotidienne des habitants après les affrontements armés qui se sont substitués aux verdicts des urnes de la présidentielle de 2010.

47 La violation de fait des identités individuelles à travers l'enregistrement du numéro de téléphone, la présentation de la carte d'identité, la prise d'image photographique de la pièce d'identité, l'indication du lieu d'habitation et l'attribution par les opérateurs à chaque abonné d'un nouveau numéro secret stocké dans la carte SIM qui a la particularité de l'identifier et qui sont des modes de contrôle et de surveillance peuvent constituer les éléments de telles réfractions à l'identification dans un espace public « sociologiquement sensible » (Proteau, 2002). De l'aveu même d'un responsable de la Direction de l'informatique et des traces technologiques (DITT) de la police scientifique de la Côte d'Ivoire, la tâche des agents recenseurs qui étaient des employés d'entreprises privées a été difficile, car plusieurs individus se sont présentés avec de fausses cartes d'identité afin d'éviter de décliner leur vraie identité, et donc de se soustraire à la surveillance et au contrôle étatique. Notre enquête sur le terrain nous a permis de nous rendre compte que certains de ces clients ont été en mesure de faire enregistrer leur numéro de téléphone sur l'identité d'autres abonnés.

48 L'identification apparaît ainsi chez bon nombre de citoyens ivoiriens comme une opération de surveillance et de contrôle de leurs activités dans le cyberespace, et donc d'entrave aux libertés individuelles dans la consommation des nouveaux médias numériques. L'inquiétude générée par le climat général d'insécurité sociopolitique entraîne des craintes nourries par des présomptions d'espionnage à partir de l'identité déclinée.

49 Une information émanant de la presse africaine stipule qu'à six mois des élections présidentielles d'octobre 2015 en Côte d'Ivoire, certains opposants au régime en place redoutaient d'avoir été mis sur écoute par les services de renseignements de l'État ivoirien et, pour cette raison, ils évitaient d'aborder des questions de fonds et de stratégie au téléphone. Ce type d'informations relatives à la mise sous écoute des citoyens et des opposants est très récurrent dans ce pays, malgré les assurances de certains diplomates occidentaux en poste à Abidjan sur l'absence de capacités techniques et technologiques opérationnelles pouvant permettre aux autorités ivoiriennes de pratiquer des écoutes massives des opposants. Ces derniers prendraient tout de même des précautions pour y échapper. Ainsi, pour les conversations importantes, certains préféreraient par exemple utiliser des téléphones abonnés à des compagnies occidentales (américaines ou françaises) en mode *roaming* à Abidjan, tandis que d'autres utiliseraient des numéros de téléphone non abonnés à leur nom[19] dans une compagnie ivoirienne.

50 Il paraît opportun de signaler que le gouvernement ivoirien, à la suite de cette opération d'identification des abonnés, a jugé nécessaire de proposer une « loi sur la protection des données à caractère personnel ». En mai 2013, le parlement ivoirien a adopté cette loi qui présente des innovations majeures en matière de protection des données à caractère

personnel en clarifiant sous la tutelle de l'ARTCI toutes les procédures de déclarations et d'octroi des autorisations. Elle détermine les responsabilités des auteurs du traitement de ces données et apporte enfin des avancées conséquentes, telles que la reconnaissance d'un « droit à l'oubli numérique », le droit à l'opposition et au refus du profilage, le droit à la portabilité des données personnelles et la clarification des règles relatives au recueil du consentement et à l'exercice des droits.

Conclusion

51 Le détournement des usages des TIC et le désordre social qu'il implique ont conduit plusieurs pays africains à procéder, par des moyens divers, à l'identification des abonnés aux services d'Internet et du téléphone mobile. Ces États entendent ainsi s'inscrire dans le principe d'une politique de régulation sociale apparue comme une exigence internationale et un préalable à l'usage des TIC perçus comme des outils de développement.

52 Les pays africains n'auront donc pas lésiné sur les moyens financiers et médiatiques pour parvenir à corriger le dysfonctionnement avéré dans les usages des technologies numériques que constitue le phénomène de la cybercriminalité. Cette régulation leur assure, sous le prétexte de créer les conditions requises pour un usage plus sécurisé des TIC dans les pays respectifs, le contrôle et la surveillance des usagers.

53 À l'instar donc des pays occidentaux, la question des libertés individuelles ou même celle de la préservation de la vie privée des citoyens usagers de ces réseaux de communication mobiles et d'Internet restent posées dans ce contexte de surveillance du consommateur déjà traumatisé par des conflits sociopolitiques et militaires.

54 Ce sont les enjeux économiques et politiques de la régulation des usages des TIC en Afrique en général, en Côte d'Ivoire en particulier, qui se trouvent au centre des préoccupations de cette étude. À travers des investigations qualitatives auprès de structures en charge du contrôle des usages des TIC (ARTCI, police scientifique-DITT), des opérateurs de téléphonie mobile et Internet ainsi que des fouilles documentaires, nous avons pu noter qu'en Côte d'Ivoire également « la soif d'indépendance » dans les usages des TIC est un véritable « cratère d'illusion ». Comme le souligne Assange et *al.* (2013), sur les méthodes de surveillance des usagers des TIC, les États africains qui ne disposent pas encore de moyens sophistiqués en matière de surveillance numérique parviennent par le canal de multinationales à contrôler leurs citoyens sous les auspices d'une collaboration inter-États.

55 Le profilage des populations, à travers l'argument d'une quête de sécurité sociale et numérique, est une réalité qui mérite, en Afrique également, une attention particulière. Cependant, si la lutte contre les escrocs du Net a été au départ le prétexte légitime pour combler le besoin pour certains gouvernants de discipliner et de contrôler le débat sociopolitique dans l'espace public numérique, on peut tout de même constater que la montée du terrorisme en Afrique avec les récents attentats de Bamako (Mali) en 2014 et de Ouagadougou (Burkina Faso) en 2015 a eu pour corolaire, comme dans les pays occidentaux, un regain d'intérêt pour la surveillance et le contrôle des usagers du cyberespace à travers une politique d'identification des abonnés (Togo, Mozambique, etc.). On note même qu'un pays comme le Kenya, qui a déjà été victime de plusieurs attaques terroristes, a demandé à ces voisins (l'Ouganda, le Rwanda et le Burundi) de

procéder à l'identification de leurs abonnés afin de renforcer la sécurité dans cette région. La nécessité d'accroître le contrôle et la surveillance des usagers du cyberespace en Afrique devient ainsi une question plus que jamais d'actualité.

BIBLIOGRAPHIE

ALZOUMA G., 2008. « Téléphone mobile, Internet et développement : l'Afrique dans la société de l'information ? », *Tic&société*, vol. 2, n° 2, ticetsociete.revues.org/488, dernière consultation le 5 mars 2016.

ASSANGE J., APPELBAUM J., MÜLLER-MAGUHN A. et ZIMMERMANN J., 2013, *Menaces sur nos libertés, comment Internet nous espionne, comment résister*, Paris, Robert Laffont.

BALL K., 2005, « Organization, Surveillance and the Body: Towards a Politics of Resistance », *Organization*, vol. 12, n° 1, pp. 89-108.

BALL K. et Snider L., 2013, *The Surveillance-Industrial Complex : A Political Economy of Surveillance*, Londres, Routledge.

BOGUI J.-J., 2010, « La Cybercriminalité, menace pour le développement », *Afrique contemporaine*, n° 234, 2010/2, Bruxelles, De Boeck université, pp. 155-170.

BONJAWO J., 2002, *Internet : Une chance pour l'Afrique*, Paris, Karthala.

BRUNET P., TIEMTORÉ O. et VETTRAINO-SOULARD M.-C., 2002, *Les Enjeux éthiques d'Internet en Afrique de l'Ouest : Vers un modèle éthique*, Presses de l'université Laval/L'Harmattan/CRDI.

CEYHAN A., 2006, « Enjeux d'identification et de surveillance à l'heure de la biométrie », *Cultures & Conflits*, n° 64, conflits.revues.org/2176, dernière consultation le 5 mars 2016.

CHÉNEAU-LOQUAY A., 2011, « Rôle joué par l'économie informelle dans l'appropriation des TIC en milieu urbain en Afrique de l'Ouest », *Les Cahiers de NETSUDS*, Sociétés africaines de l'information, http://revues.mshparisnord.org/netsuds/index.php?id=219, dernière consultation le 5 mars 2016.

DELEUZE G., 1990, « Post-scriptum sur les sociétés de contrôle », *L'Autre Journal*, n° 1, https://infokiosques.net/imprimersans2.php3?id_article=214, dernière consultation le 5 mars 2016.

DELEUZE G. et GUATTARI F., 1980, *Capitalisme et schizophrénie 2 : Mille plateaux*, Paris, Les Éditions de Minuit.

DELOITTE, 2015, « La Consommation en Afrique : Le Marché du XXIe siècle, Deloitte SAS, http://www2.deloitte.com/content/dam/Deloitte/fpc/Documents/secteurs/consumer-business/deloitte_consommation-en-afrique_juin-2015.pdf, dernière consultation le 5 mars 2016.

FOUCAULT M., 1975, *Surveiller et punir*, Paris, Gallimard, collection « Tel ».

FUCHS C., 2011, « Web 2.0, Prosumption, and Surveillance », *Surveillance & Society*, vol. 8, n° 3.

GANDY O. H., 1993, *The Panoptic Sort: A Political Economy of Personal Information,* Boulder, Westview Press.

GINGRAS A.-M., 2009, *Médias et démocratie : Le Grand Malentendu*, 3e édition revue et augmentée, Québec, Presses de l'université du Québec.

HAGGERTY K. D. et ERICSON R. V., 2000, « The Surveillant Assemblage », *British Journal of Sociology*, vo. 51, n° 4, pp. 605-622.

KAMGA O., 2006, « Un exemple de développement dans le contexte africain : L'Appropriation de la téléphonie mobile en Côte d'Ivoire », *in Place et rôle de la communication dans le développement international*, sous la direction de J.-P. LAFRANCE, A.-N. LAULAN et C. RICO DE SOTELO, Québec, Presses de l'université du Québec, pp. 105-122.

KIYINDOU A., 2012, « Technologies de l'information et de la communication et démocratie en Afrique », *in Usages et pratiques des publics dans les pays du Sud. Des médias classiques aux TIC,* actes du colloque interdisciplinaire d'Agadir (Maroc), sous la direction de A. AMSIDDER, F. DAGHMI et F. TOUMI, pp. 85-91.

KIYINDOU A., 2010, *TIC et développement socio-économique en Afrique : enjeux et pratiques,* Paris, Lavoisier.

LECLERCQ-VANDELANNOITTE A. et ISAAC H., 2013, « Technologies de l'information, contrôle et panoptique : Pour une approche deleuzienne », *in Systèmes d'information et management*, vol. 18, n ° 2, pp. 9-36.

LOUKOU A. F., 2013, « Les Techniques d'information et de communication (TIC) et l'évolution de l'économique africaine : vers une hybridation des activités », *in Les Enjeux de l'information et de la communication,* n° 14/1, pp. 103-116, lesenjeux.u-grenoble3.fr/2013/Loukou/index.html, dernière consultation le 5 mars 2016.

LYON D., 2007, *Surveillance Studies: An Overview*, Cambridge, Polity.

LYON D., 2001, *Surveillance society: Monitoring Everyday Life*, Buckingham & Philadelphia, Open University Press.

MATTELART A. et VITALIS A., 2014, *Le Profilage des populations : Du livret ouvrier au cybercontrôle,* Paris, La Découverte.

MIEGE B., 1995, « L'Espace public : perpétué, élargie et fragmenté », *L'Espace public et l'emprise de la communication*, sous la direction de I. PAILLART, Grenoble, Ellug, pp. 163-175.

OTTAVIANI D., 2003, « Foucault – Deleuze : de la discipline au contrôle », *in Lectures de Michel Foucault : Foucault et la philosophie volume 2*, Lyon, ENS Éditions, pp. 59-73, http:// books.openedition.org/enseditions/1217?lang=fr, dernière consultation le 5 mars 2016.

PROTEAU L., 2002, *Passions scolaires en Côte d'Ivoire : École, État et société*, Paris, Karthala.

RAGOUCY C., « Le Panoptique et 1984 : confrontation de deux figures politiques d'asservissement », *Psychanalyse*, 2010/2, n° 18, pp. 45-58.

NOTES

1. Edward Joseph Snowden est un informaticien américain, ancien employé de la CIA et de la NSA, qui a révélé les détails de plusieurs programmes de surveillance de masse américains et britanniques.

2. « La vie quotidienne est l'objet de surveillance, de contrôle, d'examens minutieux. Il est difficile de trouver un endroit ou une activité, protégée où à l'abri d'un repérage constant. » (notre traduction)

3. « Les humains sont entourés, plongés dans l'informatique et les technologies en réseaux du matin au soir, dans tous les endroits imaginables. Non seulement de l'employé doit accéder à son lieu de travail ou à son terminal informatique avec une clé codée, mais tous les environnements en réseau câblés ou sans fils permettent de savoir où sont les gens, ce qu'ils font et où ils vont. Même les randonneurs 'sauvages' peuvent être repérés grâce au système de localisation par satellite (GPS) qui permet de savoir où ils se trouvent à tout moment. » (notre traduction)

4. « Le rhizome connecte un point quelconque avec un autre point quelconque, et chacun de ces traits ne renvoie pas nécessairement à des traits de même nature » (Deleuze et Guattari, 1980, p. 31).

5. « Cet assemblage s'opère en extrayant les corps humains de leur fixations territoriales et en les répartissant en une série de flux distincts. Ces flux sont ensuite rassemblés en différents 'doubles numériques' qui peuvent être minutieusement examinés et ciblés en cas d'intervention. » (notre traduction)

6. « Les doubles numériques circulent dans plusieurs différents centres de calcul et servent de marqueurs pour l'accès aux ressources, les services et le pouvoir d'une manière le plus souvent inconnue de son référent. » (notre traduction)

7. Voir www.droit-inc.com/article15159-750M-reclames-a-Bell-dans-un-recours-collectif-pour-violation-de-la-vie-privee, page consultée le 07/10/2016.

8. Rapport *Économie mobile en Afrique subsaharienne 2013*, publié en 2013.

9. Association qui regroupe 800 opérateurs mobiles à travers le monde.

10. ARTCI, 2014, *Données statistiques. Premier trimestre : Internet – fixe –mobile*.

11. Conférence de presse du directeur général d'Orange-CI tenu le 14 avril 2015, http://news.abidjan.net/h/549103.html, page consultée le 07/10/2016.

12. Rapport trimestriel sur le marché des télécommunications au Sénégal, ARTP, 2015.

13. Voir www.orange.com/fr/A-propos/Presence-mondiale/Orange/pays/Bienvenue-chez-Orange-Mali, page consultée le 07/10/2016.

14. Centre ivoirien de recherches économiques et sociales.

15. Selon le rapport du cabinet Deloitte, on prévoit qu'environ 30 % de la population africaine (334 millions de personnes) aura accès à une connexion par Smartphone.

16. BRUNET P., TIEMTORÉ O. et VETTRAINO-SOULARD M.-C., 2002, *Les Enjeux éthiques d'Internet en Afrique de l'Ouest : Vers un modèle éthique*, Presses de l'université Laval/L'Harmattan/CRDI, 2002.

17. Centre de recherches pour le développement international.

18. Au cours des festivités du nouvel an 2013, une bousculade dans le public a fait plusieurs dizaines de morts. Plusieurs heures après l'événement, aucune information n'a été diffusée dans les médias d'État, pourtant de service public, avant le communiqué officiel du gouvernement. C'est à travers les réseaux sociaux qu'aux premières heures de la journée plusieurs témoignages mettant en cause la police nationale chargée de sécuriser cette manifestation ont été communiqués au public.

19. Afrikipresse : « Présidentielle ivoirienne : les opposants à Ouattara redoutent des mises sous écoute téléphonique » www.afrikipresse.fr/politique/presidentielle-ivoirienne-les-opposants-a-ouattara-redoutent-des-mises-sous-ecoute-telephonique, mise en ligne le 18 avril 2015, page consultée le 07/10/2016.

RÉSUMÉS

La volonté de plusieurs États africains de freiner l'expansion des détournements dans l'usage des technologies numériques (arnaques, cyberescroquerie) a suscité la prise de dispositions en vue de la régulation des activités dans le cyberespace. L'identification des abonnés des services des réseaux de communication mobile et d'Internet observée dans ces pays depuis au moins 2012 est l'une des principales mesures prises dans ce sens. Cependant, cette politique de régulation qui a connu une phase de sensibilisation, d'identification, mais aussi de répression, suscite des interrogations sur la préservation de la vie privée du citoyen dans un processus de surveillance de l'usage des TIC. Cette étude s'intéresse aux enjeux de la régulation des usages des TIC en Afrique à partir du cas ivoirien, où les méthodes utilisées pour endiguer la cybercriminalité laissent apparaître des craintes de profilage des populations.

The desire of many African states to curb diversions in the use of digital technologies (scams, Internet fraud) has sparked making initiatives to regulate activities in cyberspace. To this end, one of the major steps taken in these countries since at least 2012 has been the identification of subscribers to mobile communication networks and the Internet. However, this regulatory policy that has experienced a phase of awareness, identification, but also repression, also raises questions about how to protect the privacy of citizens while monitoring the use of ICT. This study examines the challenges of regulating ICT use in Africa with the example of the Ivory Coast where the methods used to curb cybercrime raise fears of profiling people.

El deseo de muchos Estados africanos para frenar la expansión de la malversación de fondos en el uso de las tecnologías digitales (estafadores, fraude cibernético) provocó haciendo los arreglos para la regulación de las actividades en el ciberespacio. La identificación de los abonados de redes de comunicaciones móviles y servicios de Internet observadas en estos países desde al menos 2012 es una de las principales medidas adoptadas en esta dirección. Sin embargo, esta política de regulación que vio una fase de sensibilización, identificación, sino también la represión, plantea interrogantes acerca de la preservación de la privacidad de los ciudadanos en el proceso de control de la utilización de las TIC. Este estudio se centra en los temas de la regulación de los usos de las TIC en África de Costa de Marfil, si los métodos utilizados para frenar la delincuencia informática revelan los temores de perfiles de población.

INDEX

Palabras claves : control, identificación, el delito cibernético, la vigilancia, el perfil
Mots-clés : régulation, identification, cybercriminalité, surveillance, profilage
Keywords : monitoring, security, cybercrime

AUTEURS

JEAN-JACQUES MAOMRA BOGUI

Jean-Jacques Bogui est enseignant-chercheur à l'université Félix-Houphouët-Boigny, à Abidjan (Côte d'Ivoire) et professeur associé à l'université du Québec, à Montréal (Canada). Il est affilié à plusieurs groupes et centres de recherche canadiens (GRICIS et GERACII), français (MICA) et ivoiriens (CERCOM). Ses intérêts de recherche portent sur les enjeux sociaux, politiques et économiques de l'intégration et de l'usage des technologies numériques dans les pays en voie de développement et l'internationalisation des communications.

N'GUESSAN JULIEN ATCHOUA

Dr N'Guessan Julien ATCHOUA est enseignant-chercheur en communication politique à l'université Félix-Houphouët-Boigny, à Abidjan. Membre du Centre d'études et de recherches en communication (CERCOM) à Abidjan et de l'Association francophone pour le savoir (ACFAS) au Québec (Canada), il s'intéresse, dans ses investigations scientifiques, aux mutations de l'espace public en rapport avec les médias et la vie politique en Côte d'Ivoire.