La cybercriminalité, menace pour le développement
Les escroqueries Internet en Côte d'Ivoire

Jean-Jacques Bogui

La participation des pays africains à la société de l'information est présentée comme un défi majeur. Ainsi, les télécommunications ont connu un développement important en Afrique ces dernières années. En Côte d'Ivoire, par exemple, ce secteur a engendré des investissements cumulés de près de 1,5 milliard d'euros en dix ans. Cependant, malgré la bonne santé de l'économie liée aux TIC, l'apparition et l'ampleur du phénomène des escroqueries *via* Internet (surtout dans le milieu de la jeunesse) sont une véritable menace pour le développement de ce pays.

Mots clés : Cybercriminalité – TIC – Internet – Développement – Jeunesse

En Côte d'Ivoire, un ministère dédié aux NTIC[1] a été créé en août 2002 afin de favoriser le développement de ce secteur au potentiel important. D'autre part, un schéma directeur stratégique des NTIC et de la mise en œuvre de ses principaux projets a été adopté par le gouvernement en 2002. Depuis lors, on peut relever la numérisation complète du réseau de télécommunications et la couverture du territoire national avec près de 2 000 kilomètres de fibre optique. Selon le ministère ivoirien chargé du développement des NTIC, au moins un million de personnes se connectent tous les jours à Internet dans ce pays[2]. Sur les dix dernières années, le secteur a engendré des investissements cumulés de près de 1 000 milliards de FCFA (près d'un milliard et demi d'euros).

Cependant, malgré la bonne santé de l'économie liée aux technologies de l'information et de la communication, le développement de l'usage d'Internet occasionne de nombreuses menaces sur le rayonnement économique du pays et son image à l'extérieur. En effet, au début de l'année 2008, les fournisseurs d'accès Internet (FAI) ont constaté que le nombre de courriers électroniques

Jean-Jacques Bogui est enseignant-chercheur et consultant en sciences de l'information et de la communication au CERCOM (université de Cocody-Abidjan) et au MICA-GRESIC (université Michel de Montaigne-Bordeaux 3).

indésirables (ou spams), dont l'objectif est d'escroquer le destinataire, a atteint des proportions trop importantes. Devant la prolifération de ces courriels disséminés à partir de la Côte d'Ivoire, de nombreux pays africains ont sollicité les autorités ivoiriennes afin que des mesures soient prises pour endiguer ou à défaut maîtriser le phénomène. La non-résolution de ce problème pourrait avoir pour conséquence l'interdiction de l'accès à leurs sites aux internautes vivant en Côte d'Ivoire.

« La cybercriminalité s'est amplifiée avec le développement de l'Internet, pour atteindre des proportions inquiétantes. » Tel est le constat de certains des participants de la première conférence régionale sur la cybersécurité, dans la capitale politique de la république de Côte d'Ivoire. Malgré son faible nombre d'internautes (24 millions, soit 2,6 % du total mondial), l'Afrique est devenue un terrain d'action important pour les cybercriminels. Selon Sylvanus Kla, directeur général de l'ATCI (Agence de télécommunication de Côte d'Ivoire), la délinquance informatique est en nette augmentation sur le continent. Les pertes attribuées à la cybercriminalité ont été évaluées, en 2007, à près de 200 milliards de dollars (près de 158 milliards d'euros), une valeur en forte hausse par rapport aux chiffres de 2003 qui étaient d'à peine 20 milliards d'euros. Nous souhaitons montrer l'ampleur des problèmes soulevés par le détournement de l'usage d'Internet en Côte d'Ivoire. Il s'agira notamment de décrire comment une technologie présentée par les agences onusiennes comme la solution à tous les maux dont souffre le continent africain est en passe de devenir un obstacle au développement économique de ce pays.

Notre étude a demandé deux approches méthodologiques. La première a consisté à constituer un corpus d'articles de presse (presse ivoirienne et française) et d'émissions de chaînes de télévision (françaises et belges) sur le sujet. L'exploitation du corpus nous a permis de recueillir de nombreux témoignages de cybercriminels, de victimes, d'agents des forces de l'ordre chargés de lutter contre le fléau et du personnel de l'ATCI, qui a fait de l'arrêt de la progression de ce phénomène son principal objectif pour les prochaines années. Nous avons également recueilli auprès de cette agence une quantité importante de documents. Notre seconde approche méthodologique nous a conduit à enquêter à l'aide d'un guide d'entretien auprès de la direction générale de l'ATCI, organe chargé de la régulation des télécommunications en Côte d'Ivoire, qui se trouve selon la volonté du gouvernement ivoirien au cœur de la lutte contre ce fléau. Nous avons donc eu un entretien avec un représentant de la direction générale de l'ATCI qui nous a permis d'obtenir des informations concernant le profil des cybercriminels, le type de cybercriminalité observé dans le pays, les méthodes

1. Nouvelles technologies de l'information et de la communication.
2. Discours du ministre chargé des NTIC à l'occasion de l'ouverture des journées nationales des technologies de l'information et de la communication (JNTIC), le 19 mai 2009 à Abidjan.
3. Par la suite nous réaliserons des enquêtes plus approfondies auprès des jeunes internautes.
4. Émission de télévision *66 minutes*, « Internet : les as de l'escroquerie », M6, 25 février 2009.
5. www.consumerfraudreporting.org

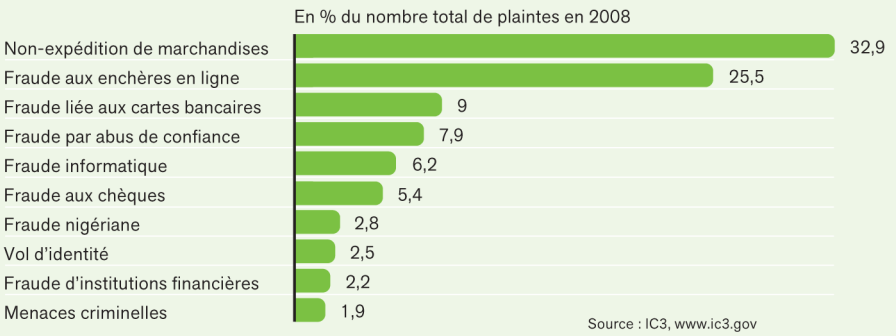
les plus utilisées par ces personnes, l'ampleur du phénomène et la stratégie de l'ATCI pour lutter contre cette infraction. La confrontation des informations obtenues au cours de notre entretien avec celles que nous a fournies notre corpus nous a permis une première approche[3] de ce phénomène et de ses conséquences pour la société ivoirienne.

La cybercriminalité : un phénomène mondial

Près de 4 000 plaintes ont été recensées en 2008 par les autorités policières françaises contre les cybercriminels basés en Côte d'Ivoire[4]. Cependant, les autorités françaises sont persuadées que la majorité des victimes ne portent pas plainte, ce qui signifie qu'il devrait y en avoir beaucoup plus. Toutefois, pour l'ATCI, il n'y a pas que les Français à être victimes de ces escrocs des temps modernes. Les Ivoiriens sont eux-mêmes très nombreux à souffrir de ce phénomène. Les plaintes viennent également de toutes les parties du monde : États-Unis, pays du Golfe, Madagascar, etc.

Une comparaison de ces statistiques avec celles de l'Internet Crime Complaint Center (IC3), organisation spécialisée dans la recension des délits commis *via* Internet et travaillant en partenariat avec le Federal Bureau of Investigation (FBI) des États-Unis, nous montre que les méthodes utilisées par les cybercriminels résidant en Côte d'Ivoire sont assez marginales à une échelle internationale. La méthode nigériane, de loin la plus pratiquée dans ce pays, qui consiste à contacter par courrier électronique des milliers de personnes en leur inventant des histoires les plus invraisemblables, ne représente que 2,8 % des plaintes déposées sur les dix principales catégories d'arnaques *via* Internet dénoncées en 2008 par ce rapport. Les principales arnaques étant de loin la non-livraison de marchandises achetées sur des sites Internet et les fausses ventes aux enchères en ligne, avec respectivement 32,9 % et 25,5 % de plaintes[5]. Si la majorité des plaintes recensées proviennent de victimes américai-

La fraude nigériane, trois plaintes sur cent aux États-Unis



Atelier de cartographie de Sciences Po, 2010

nes (92,4 %), l'IC3 reçoit également des plaintes de pays comme le Canada, le Royaume-Uni, l'Australie, l'Inde et la France.

Cette organisation a recensé 275 284 plaintes en 2008 et 66,1 % des auteurs de ces arnaques étaient originaires des États-Unis. Dans le classement des dix premiers pays en nombre d'arnaqueurs établi par cette organisation, les États-Unis venaient largement en tête (66,1 %) suivis du Royaume-Uni (10,5 %) et du Nigeria (7,5 %). On retrouve également aux sixième et septième rangs, derrière le Canada (3,1 %) et la Chine (1,6 %), deux autres pays africains, l'Afrique du Sud (0,7 %) et le Ghana (0,6 %). Trois pays européens terminent ce classement, il s'agit de l'Espagne (0,6 %), l'Italie (0,5 %) et la Roumanie (0,5 %). Ces statistiques prouvent que nous avons bien affaire à un phénomène mondial. Cependant, dans un pays en voie de développement comme la Côte d'Ivoire, les conséquences de ce phénomène peuvent être particulièrement dramatiques.

La cybercriminalité en Côte d'Ivoire

Depuis quelques années, le développement de l'usage d'Internet est assez impressionnant dans la capitale économique de la Côte d'Ivoire. Plus aucun quartier d'Abidjan n'est laissé pour compte dans cette volonté d'inclusion numérique, et les grandes villes de province également découvrant progressivement le Net. Les cybercafés ne sont plus ces endroits « étranges » réservés à une caste d'initiés. Tout le monde veut désormais être « connecté », avoir son adresse électronique, ses amis virtuels vivant souvent dans les pays développés, qui restent la référence absolue pour une jeunesse qui s'interroge sur son avenir au pays.

Entre ces jeunes gens qui passent leurs journées devant l'ordinateur en quête de l'âme sœur et ces étudiants qui espèrent trouver une bourse d'étude ou une université pour poursuivre leurs études loin du pays, en Occident de préférence, on trouve une autre catégorie d'individus pour qui l'usage d'Internet est devenu un nouveau moyen d'obtenir de l'argent facilement, sans trop d'effort, c'est le nouveau business à la mode : l'escroquerie *via* Internet, également qualifiée de « cybercriminalité ».

Le terme de cybercriminalité a été inventé à la fin des années 1990, au moment où Internet se répandait en Amérique du Nord. Un sous-groupe des pays du G8[6] fut formé suite à une réunion à Lyon afin d'étudier les nouveaux types de criminalité encouragés par, ou migrant vers Internet. Ce « groupe de Lyon » employait alors le terme de « cybercriminalité » pour décrire, de manière relativement vague, tous les types de délits perpétrés sur Internet ou les nouveaux réseaux de télécommunications dont le coût chutait rapidement (Perrin,

6. Groupe des sept pays les plus industrialisés au monde, auxquels il faut ajouter la Russie. Il est composé de l'Allemagne, le Canada, les États-Unis, la France, la Grande-Bretagne, l'Italie, le Japon et la Russie.

7. www.interieur.gouv.fr

8. Consultante spécialisée en matière de vie privée et politique d'information. Coordinatrice de la recherche pour le projet « Anonymity » à l'université d'Ottawa. Elle est également membre de l'Electronic Privacy Information Centre (EPIC) de Washington et travaille avec d'autres organismes internationaux au Canada et dans le monde.

2005). Pour le ministère français de l'Intérieur, la cybercriminalité représente l'ensemble des infractions pénales qui se commettent sur le réseau Internet (*Ibid.*). Il s'agit notamment des fraudes à la carte bleue (utilisation par autrui sans votre consentement), vente par petites annonces ou aux enchères d'objets volés ou encaissement de votre paiement sans livraison de votre marchandise, diffusion d'images pédophiles, de méthodes pour se suicider, de recettes d'explosifs ou d'injures raciales, diffusion auprès de vos enfants de photographies pornographiques ou violentes[7].

Selon Stéphanie Perrin[8], la cybercriminalité se caractérise par trois aspects : d'abord, le nouveau crime consistant à pirater, s'introduire ou espionner les systèmes informatiques d'autres personnes ou organisations ; ensuite, les cas dans lesquels le crime est ancien mais le système nouveau, comme dans les tentatives d'escroquerie par Internet. Les arnaques commerciales existent depuis toujours, les arnaques téléphoniques depuis des décennies, et nous avons aujourd'hui les arnaques par Internet. Il en va de même pour la pornographie et le non-respect du copyright ; enfin, l'enquête, dans laquelle l'ordinateur sert de réservoir de preuves indispensables pour que les poursuites engagées dans le cadre de n'importe quel crime aboutissent. Ce qui autrefois était consigné sur le papier a toutes les chances d'être aujourd'hui consigné sous forme numérique, et peut être détruit ou chiffré à distance (*Ibid.*).

Le second aspect est assurément le plus répandu en Côte d'Ivoire, au point de faire l'objet de nombreux articles dans la presse locale et étrangère. Cette dernière n'hésite plus à envoyer des reporters dans le pays pour remonter la filière de ces cybercriminels qui, à partir d'Abidjan, font énormément de victimes à travers le monde. Mais qui sont ces escrocs des temps modernes ?

Le profil des cyberescrocs. La majorité de ces escrocs du Net est issue des milieux défavorisés de la capitale économique ivoirienne. On retrouve parmi eux des étudiants, des élèves, des chômeurs, et même quelques jeunes travailleurs qui veulent arrondir leur fin de mois. En général, même s'ils n'appartiennent pas à de gros réseaux mafieux internationaux comme les Nigérians qui sont également nombreux à sévir depuis Abidjan, ils sont tout de même très bien organisés en petits réseaux (trois ou quatre personnes). Selon la police ivoirienne, l'arrestation d'un membre du réseau permet le plus souvent de démanteler tout le réseau. D'après l'agence de régulation des télécommunications en Côte d'Ivoire, la majorité de ces arnaqueurs est âgée de 12 à 25 ans. Ils sont donc très jeunes pour la plupart et travaillent le plus souvent pour leur propre compte. Selon l'ATCI, les premiers réseaux de cybercriminels sont arrivés du Nigeria. Ils fuyaient la répression orchestrée contre cette activité illicite. En effet, le Nigeria se donne les moyens juridiques de lutter contre ce type de délit grâce aux dispositions de la section 419 de leur code pénal. C'est ainsi que se type d'arnaque est appelé depuis quelque temps « scams 419 » ou « fraudes 419 ».

Cependant, très vite on va assister à une contagion des jeunes Ivoiriens, au point qu'aujourd'hui la jeunesse estudiantine et scolaire s'adonne de plus en

plus à cette pratique criminelle. De nombreux jeunes fréquentant les cybercafés sont envieux du train de vie que mènent ces cyberescrocs et se mettent donc, à leur contact, à apprendre les méthodes utilisées pour escroquer les occidentaux. Pour beaucoup d'adeptes de cette pratique, cette activité a commencé comme un jeu, mais très vite, face à l'ampleur du gain (de 500 à 30 000 euros selon les témoignages recueillis), le jeu s'est transformé en gagne-pain. Les cybercafés, dont le nombre ne fait que croître à Abidjan et dans les grandes villes du pays, sont le lieu de prédilection pour l'exercice de cette activité. Ces endroits sont donc devenus des zones sans interdit car les gérants n'ont pour seule préoccupation que leur recette journalière. On peut également relever que devenir cyberescroc ou cyberarnaqueur n'est pas le seul danger auquel les jeunes usagers du Net sont confrontés dans les cybercafés ivoiriens : l'accès à des images pornographiques est également très courant.

Les cybercriminels opérant sur le territoire ivoirien sont très nombreux à parler avec fierté de leur activité dans les médias nationaux et étrangers, quelques fois même à visage découvert comme s'ils n'avaient pas conscience de la gravité des actes qu'ils commettent. Il ressort des témoignages des escrocs qu'Internet est devenu pour eux le moyen le plus aisé de se faire de l'argent. Ils sont nombreux à estimer que leurs victimes, surtout lorsqu'elles sont françaises ou occidentales, sont riches, ce qui leur fait penser que leur délit n'est pas si grave. « Les blancs ont toujours de l'argent, donc, nous, on en prend un peu » affirmait un cyberescroc dans les médias. C'est même quasiment un jeu passionnant. Une sorte de revanche des « petits africains » pauvres sur les riches occidentaux qui les méprisent. Une des victimes françaises, dont l'histoire fut relatée dans la presse ivoirienne, a même reçu ce message très évocateur : « Tu viens de rembourser le prix de la traite négrière que vos ancêtres nous ont infligée » (Doumbia, 2008).

S'il est difficile d'avoir des statistiques irréfutables sur le nombre d'adeptes de cette pratique, on peut tout de même affirmer sans risque que le nombre de jeunes escrocs ivoiriens sur Internet est devenu suffisamment important pour que les autorités politiques de ce pays sortent de leur léthargie (absence de lois, de répression policière, de campagne de sensibilisation, etc.) et demandent à l'ATCI (agence de régulation des télécommunications) de leur proposer une batterie de mesures pour endiguer le phénomène. C'est ainsi que l'ATCI va mettre en place un programme d'action pour la cybersécurité reposant sur cinq piliers dont le premier est la sensibilisation. À partir de l'année 2008, on assiste à l'organisation de plusieurs manifestations (séminaires, forums et conférences) sur le sujet de la cybersécurité afin d'emmener les autorités politiques et

9. Parmi les manifestations les plus marquantes, on peut citer le forum national sur la cybersécurité, organisé les 18 et 19 juin 2008 en collaboration avec l'Internet Society Chapitre Côte d'Ivoire et la conférence régionale africaine sur la cybersécurité organisée du 18 au 20 novembre 2008 à Yamoussoukro en partenariat avec l'Organisation internationale de la francophonie (OIF) et l'Union africaine (UA).
10. L'agence a participé à la mise en place d'une équipe pour proposer une stratégie nationale de cybersécurité et un texte de loi contre la cybercriminalité en collaboration avec la police nationale, la société civile, les fournisseurs d'accès Internet et le ministère de tutelle.
11. En argot ivoirien, « se chercher » signifie « se débrouiller ».

la population ivoirienne à prendre conscience de la nécessité d'un cyberespace sécurisé[9]. Les quatre autres piliers du programme de l'agence concernent la réglementation[10], la veille technologique, la formation et la coopération internationale. Cependant, ce pays reste encore dans l'attente d'une loi contre ce type de criminalité.

La pratique de la cybercriminalité en Côte d'Ivoire. En général, deux méthodes sont le plus souvent utilisées par les cyberescrocs ivoiriens. La première consiste à se rendre sur des sites de rencontres pour échanger avec des Européens ou des Européennes en mal d'amour. On affiche des photos volées sur le Net à des personnes qu'on ne connaît pas, très belles de préférence, ou alors on peut utiliser des complices. Souvent, des jeunes filles, contre un certain pourcentage sur le futur gain, acceptent de servir d'appât. Elles s'installent devant la caméra en faisant semblant d'écrire à leur correspondant virtuel, alors qu'en réalité à côté de ces belles créatures est assis le cyberescroc qui utilise le clavier pour faire la conversation. Le témoignage de Souleymane, un cyberarnaqueur ivoirien, diffusé dans la presse ivoirienne confirme l'efficacité de cette méthode. Selon lui, c'est pour « se chercher[11] » qu'ils commettent de tels actes. Grâce à l'un de ses amis, il est entré en contact avec trois occidentaux en se faisant passer pour trois femmes différentes. À l'issue d'une communication assidue, en complicité avec des jeunes filles présentes dans des cybercafés, il a reçu successivement de leurs « amants » 500, 800 et 1 500 euros. « Dès que la communication est établie entre le Blanc et toi, tu peux lui faire la promesse de venir chez lui en produisant de faux passeports et de faux visas qu'on lui expédie à travers Internet afin qu'il participe au voyage » affirmait Isidore, un autre adepte de cette pratique (Doumbia, 2008).

La « méthode nigériane » est la plus répandue. On envoie des courriels et l'on espère que quelques personnes crédules mordront à l'hameçon et paieront. En général, les adresses électroniques sont récupérées sur le Net, notamment sur les listes de diffusions qui circulent, sur les forums de discussions ou les newsgroups. Certains logiciels permettent de récolter automatiquement les adresses e-mail publiées sur le Net. Dans le panorama des inventions les plus habituelles de ces escrocs du Net on peut citer : l'argent d'un héritage bloqué dans une banque, un succès à une loterie à laquelle on n'a jamais participé, une demande d'amitié d'une personne inconnue en vue d'une éventuelle relation amoureuse, une demande d'aide d'une personne fictive rencontrée sur Internet, le règlement d'un achat effectué en ligne, etc.

De nombreux cyberarnaqueurs manient à merveille les outils informatiques et notamment les logiciels favorisant les retouches de photos. Leur dextérité est telle que même des auxiliaires de justice n'arrivent pas toujours à déceler la faille. L'histoire de ce jeune français, qui avait pourtant pris la précaution de consulter une avocate, est édifiante. Cette histoire, relayée par la chaîne de télévision française M6 qui a interrogé les parents de cette victime d'une filière de cybercrarnaqueurs nigérians basée à Abidjan, permet de prendre encore plus

la mesure de la capacité de nuisance de ces malfaiteurs. En effet, la victime avait été contactée par un courrier électronique dans lequel il était mentionné qu'un de ses parents éloignés l'invitait à retirer un héritage d'un montant extrêmement important déposé dans une banque ivoirienne. L'infortuné, convaincu de l'existence de cette fortune imaginaire, va s'endetter pour honorer les frais bancaires et honoraires d'huissier proportionnels au montant à percevoir, pour finalement se rendre compte qu'il s'agissait d'une arnaque. Criblé de dettes (près de 400 000 euros), il se retrouve en prison. L'avocate qu'il avait contactée pour authentifier les documents qui lui ont été envoyés n'y avait vu aucune anomalie.

Dans ce type d'escroquerie, la première démarche consiste à fournir à la victime l'adresse électronique d'un faux auxiliaire de justice (avocat, notaire, huissier). Quand la victime contacte l'usurpateur, ce dernier lui demande de lui faire parvenir de l'argent pour l'ouverture d'un compte en Côte d'Ivoire ou l'argent sera déposé. Puis, ce seront des frais pour l'ouverture d'un compte bancaire off shore, et pour finir, s'il ne se rend toujours pas compte de la supercherie, on l'invitera à prendre contact avec « l'avocat » de la banque qui lui demandera de payer des frais d'envoi de la somme correspondant à 10 % ou 20 % du montant. Bien évidemment, cet argent n'arrivera jamais dans le compte bancaire de la victime. Comme on peut le constater, ces escrocs ont une assez bonne connaissance du monde de la finance. Il faut également souligner le rôle que jouent des agents véreux des compagnies de transferts d'argent dans ces réseaux. En effet, grâce à des complices introduits dans ces agences, les cybercriminels peuvent récupérer leur gain sans avoir besoin de présenter une pièce d'identité, ce qui est pourtant formellement exigé par la loi.

Outre les individus, les religions et les entreprises sont elles aussi victimes de ce phénomène. En effet, les cybercriminels n'hésitent plus à créer des sites Internet en se faisant passer pour des associations religieuses à la recherche de financement pour la construction d'édifices religieux tels que les mosquées et les églises. Ils prennent le soin d'expédier aux éventuels donateurs des photos de vieux édifices religieux délabrés, en demandant une aide financière en vue de leur réhabilitation, ou des photos d'églises ou de mosquées en construction pour lesquels ils auraient besoin d'aide pour l'achèvement des travaux. Une fois l'argent expédié, ils attendent une période donnée avant d'expédier une photo qui présente un autre édifice religieux flambant neuf pour prouver leur bonne foi. « Cela accroît la confiance entre les escrocs et ces associations, qui n'hésitent plus à mettre la main à la poche, pensant qu'ils ont affaire à une association qui œuvre pour le bien-être de leur religion », affirme un adepte de cette pratique. Dans les entreprises ivoiriennes, selon l'ATCI, de nombreuses plaintes sont formulées contre une nouvelle catégorie de cybercriminels qui, à l'aide de photos falsifiées, tentent d'extorquer de l'argent à de hauts responsables d'entreprises en les menaçant de publier sur le Web des photos pouvant compromettre leur réputation.

Selon le témoignage d'un ex-escroc du Net, cette activité permettait à son réseau d'amasser en moyenne 1 000 à 2 000 mille euros par jour, ce qui est

une somme extrêmement importante quand on sait que le salaire minimum dans ce pays n'excède pas 60 euros. S'il est difficile d'établir une moyenne des gains, on peut néanmoins affirmer, en recoupant les nombreux témoignages, que ceux-ci peuvent aller de 500 euros à plus de 30 000 euros par mois selon les périodes. Ces sommes permettent à ces escrocs de vivre une vie de rêve : « Avec ce qu'on gagne on vit bien pendant des mois » disait un cybercriminel.

Depuis peu de temps, le phishing ou « l'hameçonnage », une autre catégorie d'escroquerie sur Internet, qui désigne métaphoriquement le procédé criminel de vol d'identité par courriel, a fait son apparition. Il s'agit d'« aller à la pêche de renseignements personnels dans un étang d'utilisateurs Internet sans méfiance. Pour l'Office québécois de la langue française, l'hameçonnage peut être défini ainsi : « Envoi massif d'un faux courriel, apparemment authentique, utilisant l'identité d'une institution financière ou d'un site commercial connu, dans lequel on demande aux destinataires, sous différents prétextes, de mettre à jour leurs coordonnées bancaires ou personnelles, en cliquant sur un lien menant vers un faux site Web, copie conforme du site de l'institution ou de l'entreprise, où le pirate récupère ces informations, dans le but de les utiliser pour détourner des fonds à son avantage » (Serres et Cluzeau, 2008).

Conséquences de la cybercriminalité en Côte d'Ivoire

La cybercriminalité est devenue en Côte d'Ivoire, en l'espace de quelques années, un véritable problème de société. Après le début de l'intégration de l'Internet au milieu des années 1990 dans la société ivoirienne, marquée entre autres par une sorte de fascination de la jeunesse et la multiplication des cybercafés, l'heure est maintenant au désenchantement, voire à la crainte. En effet, l'usage des TIC, encouragé par les autorités politiques, connaît assurément des déviations dangereuses. Cependant, avant de nous appesantir sur les conséquences de ce détournement de l'usage des nouvelles technologies, il nous semble important de nous attarder quelque peu sur la notion d'usage.

Comme l'écrivent Philippe Breton et Serges Proulx, selon les contextes d'analyse et les cadres théoriques mobilisés, la notion d'usage, qui est par ailleurs assez complexe, renvoie à un continuum de définitions, allant du pôle de la simple « adoption » (achat, consommation, expression d'une demande sociale en regard d'une offre industrielle) au pôle de l'« appropriation » (Breton et Proulx, 2002, p. 255). Concernant ce dernier cas, ils considèrent qu'on peut parler d'« appropriation » lorsque trois conditions sociales sont réunies. Premièrement, il s'agit pour l'usager de démontrer un minimum de maîtrise technique et cognitive de l'objet technique. Deuxièmement, cette maîtrise devra s'intégrer de manière significative et créatrice aux pratiques quotidiennes de l'usage. Troisièmement, l'appropriation ouvre des possibilités de détournements, de contournements, de réinventions ou même de participation directe des usagers à la conception des innovations (*Ibid.*, p. 255-256).

Les usages d'Internet détournés à des fins d'escroquerie par une certaine catégorie d'usagers en Côte d'Ivoire sont assurément la conséquence du développement de la cyberescroquerie. L'ampleur de ce phénomène, comme nous l'avons relevé, a des conséquences extrêmement néfastes pour la Côte d'Ivoire et son économie. En effet, ce phénomène de la cybercriminalité pose au moins trois grands problèmes : le premier concerne l'image du pays et des citoyens ivoiriens à l'extérieur qui ne cesse de se dégrader ; ce qui est la conséquence du second problème : les difficultés d'ordre économique, car les entreprises et les hommes d'affaires ivoiriens, victimes de cette triste image, éprouvent d'énormes difficultés à profiter des avantages du cyberespace dans leurs activités avec des partenaires étrangers ; enfin, le troisième problème est d'ordre éducationnel car les cybercriminels sont très jeunes.

La Côte d'Ivoire et les Ivoiriens sont devenus eux aussi des victimes de la cybercriminalité, car de nos jours, avec l'amplification de ce phénomène, l'image du pays, déjà peu reluisante depuis la crise politico-militaire qu'il a connu de septembre 2002 à mars 2007[12], est davantage écornée. Les nombreux reportages des médias étrangers sur l'ampleur de la cybercriminalité en Côte d'Ivoire ne sont pas faits pour l'améliorer. Il circule même sur Internet un « guide contre les escroqueries de la Côte d'Ivoire ». Les menaces de certains pays de la sous-région ouest-africaine d'interdire l'accès à leurs sites aux internautes naviguant depuis la Côte d'Ivoire[13] confirment cette image dégradante. Les Ivoiriens, vivants à l'étranger, qui dénoncent cette situation, sont nombreux à souffrir d'une image si négative que ce détournement de l'usage d'Internet donne de leur pays et de leurs concitoyens. Inévitablement, cette situation a des répercussions sur la bonne marche de l'économie ivoirienne.

La cybercriminalité et l'économie ivoirienne. Les hommes d'affaires ivoiriens sont nombreux à souffrir des conséquences du développement de la cybercriminalité en Côte d'Ivoire, de nombreux témoignages dans les médias ivoiriens l'attestent. Il devient quasiment impossible pour eux de faire des affaires avec des opérateurs économiques étrangers sur le Net. En effet, à l'évocation de leur lieu de résidence, leurs correspondants préfèrent rompre tout contact, certains ont même été victimes de propos injurieux (Doumbia, 2008). La Côte d'Ivoire est aujourd'hui, par la faute des cybercriminels, un pays à haut risque. Fiché par les autorités européennes, ce pays n'est plus fiable, et est inscrit sur la liste rouge des pays à ne plus fréquenter « électroniquement ». Selon Didier Kla[14],

12. Le 19 septembre 2002 une tentative de coup d'État avortée se transforme en rébellion. Cette situation aura pour corollaire la partition du pays en deux jusqu'à la signature d'un accord de paix à Ouagadougou (Burkina Faso) le 4 mars 2007.

13. République de Cote d'Ivoire (2008).

14. Président de l'Internet Society-Côte d'Ivoire (ISOC-CI), www.isoc.ci

15. Avis juridique prononcé par un mufti, un ouléma ou un faqîh dans la religion musulmane.

16. Ouestafnews (2008).

17. Conseiller technique chargé des NTIC à l'ATCI.

une fatwa[15] à l'échelle mondiale est même lancée pour interdire des achats en ligne à partir de ce pays. Dès lors que vous êtes repéré comme étant un ressortissant ivoirien, désireux de faire des achats en Europe à partir de la Côte d'Ivoire, le vendeur vous ferme automatiquement ses portes. Il affirme que de nombreuses plaintes sont déposées contre la Côte d'Ivoire à travers l'Europe, et que ce pays risque non seulement une exclusion du cyberespace dans les prochaines années, mais également une exclusion à tout moment du commerce international (Doumbia, 2008). Outre les pays européens, le gouvernement indien a lui aussi mis en garde ses ressortissants contre les agissements d'escrocs basés en « Afrique de l'Ouest » et qui arnaquent les ressortissants indiens. Le bureau d'information du gouvernement indien dresse une liste de sept pays ouest-africains, dont la Côte d'Ivoire, à partir desquels agissent ces escrocs[16]. Selon Abraham Djekou[17] les premières entreprises victimes de ce phénomène sont les fournisseurs d'accès Internet (FAI) de Côte d'Ivoire, car en raison des nombreuses plaintes, elles sont « blacklistées ». Autrement dit, lorsque leurs adresses IP sont reconnues sur certains sites, les transactions sont bloquées.

Les conséquences de la cybercriminalité sur l'économie ivoirienne sont donc désastreuses, ce qui témoigne de l'importance de la confiance dans le monde virtuel. « Tout système d'échange commercial ne peut exister sans une confiance qui agit comme la force qui scelle la relation vendeur-client et influence l'orientation à long terme de cette relation » (Bergadaa, Graber, Muhlbacher, 1999). Gilles de Chezelles considère que la confiance est indispensable dans les échanges commerciaux ou comportant un échange de l'une ou de l'autre des parties. Selon lui, si « dans le monde réel de nombreux critères objectifs et subjectifs nous permettent, par exemple, de nous assurer de l'identité de notre correspondant, de son lieu de travail, de son appartenance à une entreprise ou une administration. Le problème auquel nous sommes maintenant tous confrontés est que, très souvent, ces critères ne sont pas utilisables "en l'état" dans le cadre des échanges dématérialisés » (de Chezelles, 2007). D'où la nécessité d'avoir recours à des « tiers de confiance », car la confiance dans les échanges électroniques ne peut se limiter à des dispositifs techniques. C'est également une question de droit, d'identification du correspondant, de psychologie... En d'autres termes, si l'accès à certaines technologies peut faciliter le développement d'échanges commerciaux entre les entrepreneurs ivoiriens et d'éventuels partenaires étrangers, en l'absence d'un climat de confiance, ces dispositifs techniques ne pourront favoriser aucun développement économique. Cependant, hormis les chefs d'entreprises, une autre catégorie d'Ivoiriens est victime de l'expansion de ce phénomène : la jeunesse.

Conclusion

En définitive, les problèmes de criminalité et d'insécurité s'adaptent à l'évolution de la société, avec les technologies de l'information et de la communication. On assiste juste à une modernisation des méthodes et les mêmes maux

demeurent : le vol, les arnaques, la pédophilie… Les institutions étatiques ivoiriennes, comme pour les anciennes formes de délits, doivent donc exercer leurs fonctions régaliennes. L'ATCI, dont la principale raison d'existence est la régulation des télécommunications, n'aurait certainement pas eu l'obligation de se trouver en première ligne dans cette guerre pour la sécurisation du cyberespace en Côte d'Ivoire si ces institutions jouaient le rôle qui leur est dévolu.

Alors que les gouvernants ivoiriens et les médias nationaux et internationaux interprètent ce phénomène comme une volonté des jeunes Ivoiriens d'acquérir facilement de l'argent, on peut s'interroger sur la facilité de cette activité qui demande pourtant un maximum de dextérité en matière d'usage des TIC, de grandes qualités de psychologue et de bonnes connaissances du monde de la finance. Comment se fait-il que la société dans laquelle ils évoluent soit incapable d'exploiter un si grand potentiel, une telle ingéniosité, à des fins plus saines et plus avantageuses pour le développement ? Par ailleurs, n'est-ce pas un désaveu des discours technocentristes des organisations internationales intervenant dans le domaine du développement qui privilégient la plupart du temps un encouragement à une course à l'équipement, tout en négligeant la question fondamentale de l'appropriation des techniques et de la formation aux usages ? Dans bon nombre de pays africains, la politique d'intégration des TIC se limite à offrir l'accès à ces moyens de communication aux citoyens. L'éducation des populations et plus particulièrement de la jeunesse à l'usage de ces nouveaux médias ne devrait-elle pas être une priorité ? Devant le peu de changements apportés au quotidien des populations par ces outils présentés comme la panacée à tous les problèmes du continent africain, ne peut-on pas craindre que ces déviances se multiplient et fassent de ces technologies un nouvel obstacle au développement ?

La crainte ou le désenchantement qu'engendre le développement de l'usage des TIC dans la population est le résultat de la non-anticipation des problèmes de sécurité. Pourtant, le développement de l'usage des TIC reste un défi important pour le pays à l'ère de la mondialisation. Participer à la nouvelle société de l'information est pour les pays africains un enjeu à la fois social, culturel, économique et politique. La nécessité de rompre l'isolement et de développer des synergies par le biais du travail collaboratif, de rénover le système de santé et d'enseignement, ou encore de s'inscrire dans les nouveaux courants d'échanges internationaux aux contenus et aux supports de plus en plus virtuels justifie pleinement cette ambition.

Bibliographie

Bergadaa, M., **Graber**, S. et **Muhlbacher**, H. (1999), « La confiance dans la relation tripartite vendeur-client-entreprise », XV^e congrès de l'Association française de marketing, Strasbourg, mai.

Breton, P., **Proulx**, S. (2002), *L'Explosion de la communication. Introduction aux théories et aux pratiques de la communication*, Montréal/Paris, éditions du Boréal/La Découverte.

Cheneau-Loquay, A. (2000), *Enjeux des technologies de la communication en Afrique*, Paris, Karthala.

Chezelles (de), G. (2007), « La confiance, une nécessité dans un monde virtuel », www.dechezelles.fr

Doumbia, Y. (2008), « La Mafia de la cybercriminalité en Côte d'Ivoire. Qui sont-ils ? Comment opèrent-ils ? », *L'Inter*, jeudi 15 mai.

Hofnung, T. (2008), « Berlines volées : la juge cale à Abidjan », *Libération*, jeudi 19 février.

IC3 (2009), "Internet Fraud. Scam and Crime Statistiques".

Interpol (2008), « Initiative sécurité globale », www.interpol.int

Lascombe, M. (2005), *Le Droit constitutionnel de la V^e République*, Paris, L'Harmattan.

Ouestafnews (2008), « Cybercriminalité : Nigeria, Sénégal, Côte d'Ivoire, Burkina, Ghana, Bénin, Togo "fichés" par les Indiens », mardi 22 juillet, www.ouestaf.com

Perrin, S. (2005), « "Cybercriminalité". Enjeux de mots : regards multiculturels sur les sociétés de l'information », C & F Éditions, 5 novembre.

République de Côte d'Ivoire (2008), « Conférence africaine sur la cybercriminalité », Abidjan, 17 au 20 octobre.

République de Côte d'Ivoire (2008), « Plan de Yamoussoukro sur la cybersécurité », conférence africaine sur la cybersécurité, Yamoussoukro, 18 au 20 novembre.

Serres, D. et **Cluzeau**, A. (2008), « La Cybercriminalité. Les nouveaux enjeux de la protection des données », université de Laval, maîtrise en droit de l'entreprise.

Sociétés de l'information (2009), « Comprendre la dynamique des réseaux », n° 58, avril.

UIT (2004), « L'Afrique, marché où le mobile connaît la plus forte croissance au monde. La technologie du mobile est-elle la clé de l'accès aux TIC en Afrique ? », communiqué de presse, Genève, 26 avril.

UIT (2007), « Guide de la cybersécurité pour les pays en développement », www.itu.int

Wally, K. (2009), « Escroquerie sur Internet. Un reportage scandaleux mettant en cause des Ivoiriens diffusé en France », *Nord-Sud*, jeudi 5 mars.

M6 (2009), « Abidjan, capitale de la débrouille ! », *Enquête exclusive*, 26 avril.

M6 (2009), « Internet : les as de l'escroquerie », *66 minutes*, 25 février.

RTL/TVI (2009), « Les arnaques sur Internet », *Reporters*, 10 avril.

La connexion de l'Afrique au reste du monde : de la pénurie à la surcapacité ?

Le paradoxe des TIC en Afrique réside dans le rapport entre la faiblesse actuelle des connexions technologiques aux réseaux de communications mondiaux et les stratégies récentes de construction d'infrastructures qui conduiront à une surcapacité. Au XXIe siècle, le seul câble sous marin, SAT 3, qui reliait depuis 2003-2004 douze pays de la façade Atlantique à l'Europe et à l'Asie, était en effet utilisé très en deçà de ses capacités (20 % à peine). Certes, les prix de SAT 3 étaient très élevés mais quand on considère le coût de tels projets on ne peut que s'interroger sur leur utilité et sur le gaspillage de ressources qu'ils induisent. Dans les pays desservis, les prix pour la bande passante de SAT 3 allaient de 4 500 à 12 000 dollars par Mbit/s/mois en 2007, soit cinquante fois plus que les prix de la bande passante aux États-Unis, en raison du monopole des membres du consortium[1].

Un pays côtier comme le Sénégal, connecté au câble et dont l'opérateur (national) est partie prenante et en position stratégique, bénéficie d'avantages que ses voisins mauritanien et malien n'ont pas. En 2007, un fournisseur d'accès à Internet (FAI) mauritanien payait presque trois fois plus pour 1 Mbit/s qu'un FAI sénégalais. De même, la Namibie et le Lesotho utilisent toujours des liaisons satellitaires, alors qu'ils ont accès à la fibre mais à des coûts de transit si élevés que la liaison par satellite ne leur revient pas plus cher.

Ces distorsions ne sont plus atténuées par une politique d'équipement à l'échelle régionale comme ce fut le cas pour le réseau mixte (téléphonique et télévision) panafricain Panaftel déployé sur le continent avant la vague libérale. Or, la plupart des pays africains n'ont pas le choix car ils sont dépendants d'un seul fournisseur d'accès international.

Les protestations des FAI ont été unanimes, et celle du Ghana a réussi à faire baisser le prix de la connexion après deux ans de lutte contre l'opérateur national. Avec la mise en service du câble Seacom[2] en Afrique de l'Est, en juillet 2009, les propriétaires de SAT 3 ont baissé les prix de 50 %. Outre la concurrence, une autre manière de faire baisser les prix est d'avoir un accès plus ouvert aux infrastructures de base.

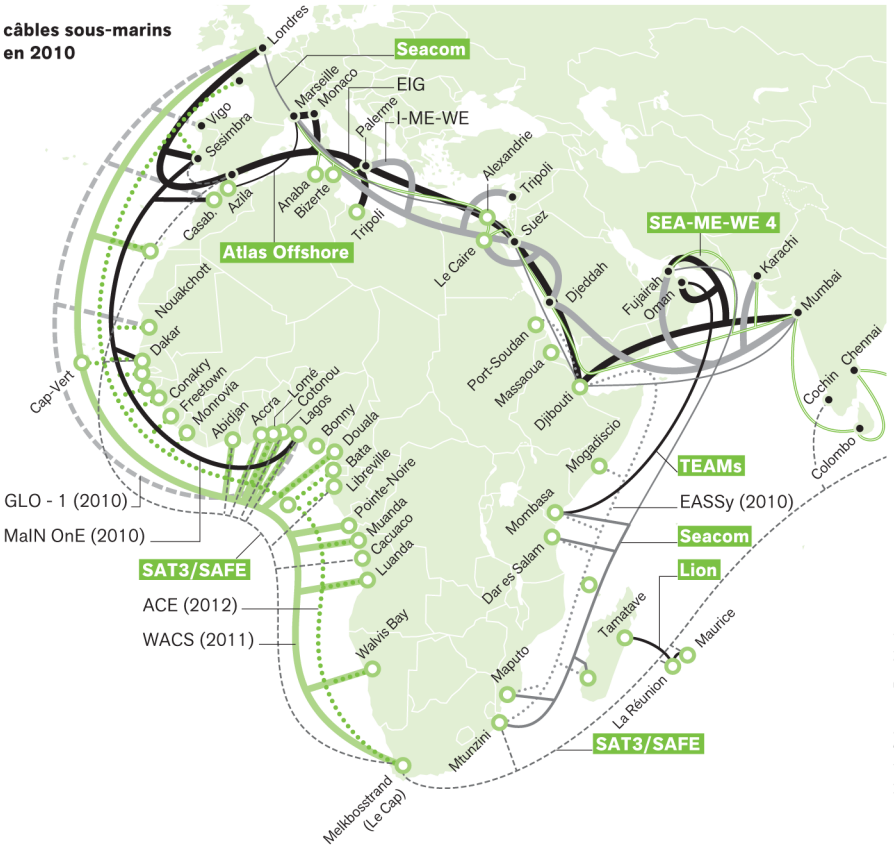
À la suite du SMSI[3], la société civile est devenue un nouvel acteur pour promouvoir l'accès et le service universel. Les grandes ONG comme APC[4] ou PANOS[5] ont exercé un efficace lobbying pour réclamer un accès ouvert aux infrastructures, en particulier là où il y avait un chaînon manquant, le long des côtes de l'Afrique de l'Est. Depuis 2003, un projet existait, l'East African Submarine Cable System (EASSY), qui a fait l'objet d'âpres négociations, en particulier entre l'Afrique du Sud et le Kenya et avec le NEPAD, nouveau partenariat pour l'Afrique. Toutes les parties concernées (gouvernement, experts, régulateurs, société civile, juristes, compagnies de télécommunications et bailleurs de fonds) se sont mises d'accord pour que sa gestion intègre plusieurs principes équitables[6]. EASSY est détenu et géré par un groupe d'opérateurs Africains (92 %) et d'opérateurs internationaux (8 %). La complexité de cette organisation a entraîné beaucoup de retard. En 2010, le câble est en cours de déploiement[7].

En attendant, la surcapacité n'empêche pas des projets concurrents. Le Kenya, acteur principal en Afrique de l'Est, a passé contrat avec d'autres opérateurs, comme sur le projet TEAM, partenariat entre le gouvernement Kenyan et des sociétés privées. Certes, l'accroissement des infrastructures et de l'offre de connectivité peut amener à une remise en cause des monopoles et à une baisse des prix. Mais ce que l'on constate sur le marché des téléphones mobiles ne s'observe pas dans le secteur d'Internet qui continue d'être uniquement soumis aux logiques propres à l'offre. La spirale « vertueuse » qui veut que les opérateurs adaptent leurs services aux utilisateurs et à l'évolution des modalités d'usage des technologies de l'information et de la communication n'a pas encore cours en Afrique.

Annie Chéneau-Loquay

1. Un consortium de trente-six partenaires dont certains gros investisseurs comme France Telecom (12,08 %), Nitel (8,39 %) du Nigéria, TCI, un sous traitant de AT&T (12,42 %) et VSNL (8,93 %), le principal opérateur indien.
2. Seacom est financé par le secteur privé et détenu aux trois-quarts par des Africains. Il devrait aussi fournir la bande sur la base d'un accès ouvert et égal pour tous les opérateurs.
3. Sommet mondial sur la société de l'information (www.itu.int).
4. APC est l'association pour le progrès des communications. « Fondé en 1990, APC est à la fois un réseau international et une organisation à but non lucratif qui croit en un accès libre et ouvert pour tous » (www.apc.org).
5. L'Institut PANOS Afrique de l'Ouest est une organisation non-gouvernementale qui œuvre, par l'information et la communication, « à la construction d'une culture de la démocratie, de la citoyenneté et de la paix » (www.panos-ao.org).
6. Un accès ouvert et non discriminatoire, une propriété collective et équitable de l'infrastructure du réseau à travers la région, la séparation de la propriété de l'infrastructure de celle de son utilisation et un fonctionnement sur le principe d'un recouvrement des coûts mais pas pour faire du profit.
7. À la date du 14 février 2010, Telma (Telecom malagasy) rapporte que l'Île de Batz, le navire en charge de la pose de câble est arrivé à Muntzini en Afrique du Sud. De là, il va entreprendre de rallier les derniers segments du câble, qui arrivera à Tulear en mars selon les prévisions de la société.

Autoroutes numériques autour de l'Afrique



Seacom Câbles en fonction
ACE (2012) Projets (date)

Débits (gigabits) :

- 300 - 500
- 1 000 - 1 500
- 1 500 - 2 500
- 3 000 - 5 200

Source : African Undersea Cables, www.manypossibilities.net/african-undersea-cables, mise à jour avril 2010.

Atelier de cartographie de Sciences Po, 2010

L'impact de la téléphonie mobile sur le développement

Dans les pays en développement, la Banque mondiale est le plus grand investisseur multilatéral dans les TIC. Son action s'accompagne d'un discours qui diffuse au niveau mondial le credo selon lequel les TIC seraient un formidable vecteur de développement des économies du Sud. Une large littérature soutient ce discours. Ces études économétriques montrent qu'il existe un impact positif de la croissance de la téléphonie fixe et de la pénétration de la téléphonie mobile sur les revenus nationaux dans les pays. D'après Guy Zibi d'AfricaNext, une société indépendante de conseil axée sur le secteur des télécommunications, des médias et des technologies (TMT) en Afrique, les recettes des services de télécommunication représentent près de 5 % du PIB des États africains, et celles-ci peuvent aller jusqu'à 7 % dans certains pays. « Un gain de dix points en pénétration de téléphonie mobile entraîne une hausse additionnelle de à 0,6 % pour le PIB/habitants », note Christine Zhen-Wei Qiang. Cela s'explique par les importantes économies de coût de transport engendrées, la création d'emplois (en 2007, près de 3,5 millions de personnes en Afrique travaillaient de manière indirecte dans le secteur des télécommunications). De plus, les opérateurs en télécommunications sont les premiers contributeurs fiscaux. Actuellement, le marché de la téléphonie mobile génère 7 % des recettes fiscales totales en Afrique.

Mais les TIC peuvent-elles échapper à cet éternel problème du développement économique et surtout social, qui fait souvent de l'Afrique un tonneau des Danaïdes ? Les participants au séminaire de Bamako « Internet, passerelle du développement » (2000) avaient bien perçu le problème en demandant que les infrastructures routières, les services postaux, bancaires et sociaux soient améliorés, car à quoi sert de faire du commerce électronique si les produits ne peuvent pas être acheminés ? La téléphonie mobile à haut débit est décrite par l'UIT comme étant la solution pour pallier l'absence d'infrastructures en oubliant la nécessaire synergie entre les réseaux, et que le rôle des infrastructures dans le développement d'un pays est crucial. Renoncer à avoir une infrastructure stable au sol et passer par la voie des airs, c'est oublier que la fibre optique est le meilleur vecteur pour le haut débit et aussi qu'une interconnexion des réseaux est la caractéristique des territoires développés.

Peut-on croire, comme l'a affirmé Joel Selanikio[1] à la BBC, que le téléphone portable pourrait devenir l'ordinateur pour tous dans un futur proche ? Il serait l'outil de communication, le portail pour Internet, le livre scolaire, l'album photo familial, la carte de paiement et de crédit, la radio et bien d'autres choses si les adaptations nécessaires sont réalisées (Selanikio, 2008).

La question du développement des TIC en Afrique est à considérer dans toutes ses dimensions interreliées : des stratégies des opérateurs internationaux à celles des fournisseurs de service et des usagers locaux. Mais dans ce jeu d'acteurs, l'État a un rôle éminent à jouer. Choix techniques, financiers, modes de régulations, répartition territoriale sont de son ressort, même si les petits pays aux marchés étroits ont moins de marges de manœuvre. Les différences constatées dans le développement du réseau et des usages entre les pays africains tiennent plus encore à la volonté politique des États qu'aux stratégies des firmes ou à l'aide internationale.

Annie Chéneau-Loquay, Nicolas Courtin

1. Joel Selanikio est un physicien cofondateur de DataDyne.org, une start-up qui crée des logiciels en *open source* pour la santé publique et le développement international.

Bibliographie

Lee, S., **Levendis**, J., **Gutierrez**, L. (2009), "Telecommunications and Economic growth. An Empirical Analysis of Sub-Saharan Africa", Universitad del Rosario, Facultad de Economia, Working Papers, n° 64.

Selanikio, J. (2008), "Technology. The invisible Computer Revolution", *BBC News*, 17 janvier.

Sridhar, K.S., **Sridhar**, V. (2004), *Telecommunications Infrastructure and Economic Growth. Evidence from Developing Countries*, National Institute of Public Finance and Policy, Working Papers 04/14.

World Bank (2009), "Information and Communications for Development. Expending Reach and Increasing Impact", Washington.

Zhen-Wei Qiang, C. (2009), "Mobile Telephony. A Transformation Tool for Growth and Developement", *Private Sector & Development*, n° 4.

Zibi, G. (2009), "The African Mobile Phone Market. Beyong the Boom Phase, Between the Promise and Uncertainty of Maturity", *Private Sector & Development*, Proparco's magazine, n° 4, novembre.