



## Praxis de la communication mobile : enjeux et défis pour la sécurité des données privées

---

Carlin MBUNDANI WATALU<sup>1</sup> et Godfrey BENTH NGOYI<sup>2</sup>

Université de Kinshasa, République Démocratique du Congo

[godfrey.benth@unikin.ac.cd](mailto:godfrey.benth@unikin.ac.cd)

**Résumé :** Il est question dans cet article d'évoquer quelques enjeux et défis en matière de sécurité de nos données personnelles dans l'usage de téléphone devenu un outil par excellence de la modernité. Ainsi donc, l'étude va d'abord s'appesantir sur le clone qui accentue l'insécurité dans la confidentialité des données personnelles (privées). L'article comporte deux parties : la clarification des concepts et les enjeux & défis pour la sécurité des données, hormis l'introduction et la conclusion.

**Mots-clés :** Communication, Mobile, Sécurité, Données, Clonage, Logiciel, RAM.

### Praxis of mobile communication: issues and challenges or the security of private data

**Abstract :** This article looks at some of the issues and challenges relating to the security of our personal data when using the telephone, which has become a tool par excellence of modernity. So the study will first focus on the clone, which accentuates insecurity in the confidentiality of personal (private) data. The article is in two parts: clarification of the concepts and the issues and challenges for data security, apart from the introduction and conclusion.

**Keywords :** Communication, Mobile, Security, Data, Cloning, Software, RAM.

### Introduction

Au 21<sup>ème</sup> siècle, la gestion de nos vies passe par le numérique à travers lequel nous contrôlons nos comptes bancaires, payons factures, analysons notre système immunitaire de santé, surveillons à distance nos ménages et communiquons avec nos proches, travaillons même à distance et tant d'autres. L'observation est sans appel, les enfants et des adultes sont quasiment tous exposés aux écrans 6 à 12 heures par jour. Nos smartphones sont aujourd'hui une concentration de toutes nos données personnelles et autres. Cela constitue une seconde vie. Donc la vie numérique. Le contrôle de la vie numérique dépend premièrement de la nature d'informations stockées et deuxièmement ledit contrôle nous échappe, car actuellement nous sommes exposés à la compétition des algorithmes. Nous passons au simple terminal d'échange d'information et de

---

<sup>1</sup> MBUNDANI WATALU Carlin est licencié en Sciences de l'Information et de la Communication, Chercheur en multimédia. Apprenant au DEA à l'Université de Kinshasa, Faculté des Lettres et Sciences Humaines, au Département des SIC.

<sup>2</sup> BENTH NGOYI Godfrey est Chercheur en NTIC et Multimédia, Assistant à l'Université de Kinshasa et Apprenant au DEA/DES en Sciences de l'Information et de la Communication.

stockage des données à une sphère de suivi de traces pour une exploitation commerciale ou d'espionnage. Une attention particulière sera retenue dans la problématique du clonage de nos smartphones. A quoi est-ce – que nous sommes ou seront exposés une fois que notre smartphone est cloné ?

## 1. Clarification des concepts

### 1.1. Communication humaine, homme – machine, communication mobile et clonage

#### - Communication humaine

La communication humaine est un phénomène social dans lequel l'individu agit de façon rationnelle. Pour J. CAELEN et J. COURAZ (2019 :140), « la communication relève d'une "tentative d'ajustement" où l'on doit ajouter au transport de l'information, le jeu des rôles et des actes par lesquels les interlocuteurs se reconnaissent comme tels, agissent comme tels et fondent ainsi des communautés linguistiques dans un monde humain ».

Cette définition résulte elle-même de nombreux ajustements car beaucoup de disciplines se sont intéressées à la communication humaine. Les cognosciences retiennent de la communication les aspects liés à la perception, à l'action et au raisonnement du point de vue de l'individu. Ainsi, la philosophie s'intéresse à cet individu placé en situation de communication. Sur un plan intentionnel, l'ethnoscience pose par contre la communication dans une perspective sociale : les individus agissent dans un cadre normalisé selon des règles et des conventions qui sont socio-culturellement bien définies. Quant aux technosciences, elles visent à intégrer la machine dans un univers de « communication humaine » dans plusieurs directions : soit dans une perspective de machine médiatrice- canal entre des interlocuteurs humains, soit dans une perspective virtualisante, la machine anime ou simule le monde virtuel, soit encore dans une perspective opérante et là, la machine s'insère dans le processus même de la communication pour devenir l'un des partenaires dans la communication et participer à la résolution d'un problème ou d'une tâche selon J. CAELEN et J. COURAZ (2019 : 258). Dans ce dernier cas, elle est assujettie à comprendre pour participer et collaborer au mieux à la tâche de l'utilisateur.

#### - Communication Homme - Machine

Le terme communication homme-machine pourtant couramment employer, semble abusif : la machine n'est pas un être social, n'a pas d'intention ni de culture. Elle ne peut pas agir sur le monde réel et on ne peut pas lui dire : « peux-tu fermer la porte s'il te plaît ? ». Elle n'a de prise que sur son propre monde. De fait, la machine procure des outils, des moyens d'accès, pour réaliser une tâche ou permet de partager des données, un logiciel, avec d'autres humains pour travailler de manière collaborative dans un même environnement informatique. Elle se présente donc chaque fois comme un intégrateur. Sa fonction de communication se résume à la manière de présenter des informations

ou de comprendre des instructions. Cette fonction se situe dans une relation opérateur-tâche où la machine a un rôle collaboratif (Joëlle COUTAZ, 1990 : 16). Mais c'est ici que surgit le paradoxe car pour assumer ce rôle, elle doit avoir des capacités qui lui permettent de comprendre les processus actionnels et dialogiques de l'utilisateur qui puissent la rendre artificiellement sociale pour être au minimum « conviviale ». Pour ce faire, « la machine devrait donc posséder : (1) La connaissance de l'opérateur, (2) La connaissance du domaine de la tâche, (3) des représentations d'elle-même (pour s'adapter), (4) les règles de l'intervention pédagogique (aides, guides, exemples), (5) les règles du dialogue (principes de négociation, de coopération, de réactivité, etc.), (6) les règles de comportement social, et bien sûr tous les processus inférentielle mettant en œuvre ces connaissances, voire même des capacités de compréhension du langage naturel, etc. ».

Les différentes étapes par lesquelles la machine, partant des instructions produites par un interlocuteur humain, tente de les comprendre en les replaçant dans un cadre actionnel et dialogique pour générer des réponses sous forme d'actions après avoir planifié ses réponses en fonction des contraintes interactionnelles. Ces étapes sont planifiées généralement par un composant logiciel appelé contrôleur de dialogue. L'interaction homme-machine doit s'appuyer sur une ergonomie d'harmonisation des moyens de communication que sont : écran, clavier, voix, image, etc. De manière générale, il vaut mieux entrer des données : nombres, noms (de fichiers par ex.) au clavier (pour des raisons de fiabilité et de taille de vocabulaire), les opérations de mouvements fins réglage de taille de fenêtre, déplacements, pointage à la souris et ne garder pour la communication orale que des commandes de niveau élevé, par exemple "ouvrir un fichier sur le lecteur interne " équivalente à une longue séquence de "clics" sur les menus. Dans le cas de la réponse orale pour des messages d'aide, de demande de confirmation ou de renseignements complémentaires, etc. le problème est exactement symétrique : certains messages sont mieux captés par l'oral que par le texte écrit (messages d'alerte notamment, commentaires, aides).

#### - Communication mobile

La téléphonie mobile, ou téléphone cellulaire est un moyen de communication, plus précisément de radiocommunication, c'est-à-dire la transmission de la voix et de données à l'aide d'ondes radioélectriques entre une station de base qui peut couvrir une zone de plusieurs dizaines de kilomètres de rayon et le téléphone mobile de l'utilisateur ([www.google.com](http://www.google.com)). La communication mobile est à la fois une communication qui se fait entre deux ou plusieurs protagonistes, et aussi une communication entre les machines, entre

pilones et téléphones. Elle s'effectue par la volonté humaine et exige au départ avoir un numéro de contact.

### 1.2. *Le clonage*

Le clonage est un dispositif digital qui enregistre nos trajets, nos comportements, nos likes, nos commentaires, nos photos qui sont stockées sur internet et dans les réseaux sociaux ([www.commentcamarche.com](http://www.commentcamarche.com)). Nos données de santé, nos battements de cœur sont enregistrés sur des data centers. Cela se fait via la reconnaissance faciale, par empreinte digitale ou vocale généralement pour s'identifier. Ceci permet de créer une personne numérique jumelle à nous. Une fois que son smartphone est cloné, cela revient à dire que l'on a une vie qui est gérée par une tierce personne dont l'existence est ignorée, signale J. MONTAGUT (2008 : 121).

Notre smartphone sait énormément de choses sur nous, à la fois dans le monde virtuel d'Internet et dans le monde physique réel (déplacements, habitudes, paramètres biologiques, etc.). La liste de nos applications est aussi porteuse de sens puisque celles-ci correspondent à nos centres d'intérêt et besoins. Un smartphone peut donc fournir de nombreuses données personnelles qui font vivre tout un écosystème ([www.theconversation.com](http://www.theconversation.com)). Donc, le concept de clonage a fait sa transition jusqu'au monde du numérique à l'aide des terminaux tels que le téléphone (smartphone) et l'ordinateur. Tout terminal numérique est exposé à une forme de clonage dont la source peut être sans traces dépendamment à la performance de code du programmeur informatique A. CARON et L. CARONIA, (2005 : 19). Que dire de plus, car plus nous avançons numériquement, plus la guerre de code ou des algorithmes devient intense. Le smartphone concentre beaucoup de données personnelles saisies par l'utilisateur. Mais, il en génère également au travers des capteurs et interfaces de communication dont il est doté. A chaque appel téléphonique ou SMS, utilisation d'un navigateur Web ou d'une application, des traces de ces activités sont créées ([www.celltrackingapps.com](http://www.celltrackingapps.com)). Un sms, peut aider à vider votre compte bancaire. Le cybercriminel tente nous arnaquer par sms. La dématérialisation des données de nos téléphones est devenue le mode de paiement préféré.

## 3. **Les enjeux et défis**

La technologie nous a beaucoup rapproché. Les smartphones nous ont donné la possibilité de communiquer avec des personnes du monde entier et nous offrent une foule d'autres fonctionnalités. Cependant, il y a toujours un revers de la médaille : avec l'essor de la technologie, l'on perd son intimité avec une possibilité d'être écouté en tout lieu et en tout temps. L'une des façons de le

faire est d'activer à distance le microphone d'un téléphone portable pour écouter les appels à distance et suivre les conversations et l'environnement immédiat de la personne. Certes, le système d'exploitation iOS d'Apple met en œuvre des vérifications dynamiques : lorsqu'une application est exécutée pour la première fois, si elle a besoin d'une autorisation particulière, l'utilisateur reçoit un message avec une explication lui permettant de l'accorder ou non. Par la suite, l'utilisateur peut changer d'avis et avoir une vision globale des autorisations accordées dans un panneau de contrôle facile à trouver.

Pour le système d'exploitation Android de Google, pendant longtemps l'utilisateur n'a eu d'autre choix que d'accepter en bloc toutes les autorisations demandées sans quoi les applications ne pouvaient être installées. Heureusement, avec la venue de l'Android 6, Google a inclus un mécanisme d'autorisation dynamique, mais les informations de contrôle demeurent éparpillées, difficiles à trouver et à comprendre. En outre, Google a classé les autorisations en deux catégories : les autorisations normales et les autorisations à risques ; l'utilisateur n'est sollicité que pour les autorisations à risques, les autorisations normales ne comprenant, selon Google, pas beaucoup de risques pour la vie privée et la sécurité de l'utilisateur restant automatiquement accordées lors de l'installation. Or, en recherchant dans les pages destinées aux développeurs Android, on se rend compte que ces autorisations ouvrent, en fait, l'accès à des identifiants techniques stables, c'est-à-dire permettant de tracer les utilisateurs dans la durée et de connaître, par exemple, tous les réseaux wifi auxquels ils se sont connectés. Ces informations sont loin d'être anodines en termes de respect de la vie privée. Enfin, quelques limites communes aux deux systèmes d'exploitation demeurent, notamment l'absence de contrôle du comportement des applications par l'utilisateur, de la composition précise des autorisations, et parfois encore l'absence de collecte explicite du consentement de l'utilisateur.

Les smartphones concentrent beaucoup de données personnelles saisies par l'utilisateur. Mais, il en génère également au travers des capteurs et interfaces de communication dont il est doté : à chaque appel téléphonique ou SMS, utilisation d'un navigateur Web ou d'une application, des traces de ces activités sont créées. Notre smartphone sait donc énormément de choses sur nous, à la fois dans le monde virtuel d'Internet et dans le monde physique réel (déplacements, habitudes, paramètres biologiques...). La liste de nos applications est aussi porteuse de sens puisque celles-ci correspondent à nos centres d'intérêt et besoins. Un smartphone peut donc fournir de nombreuses données personnelles qui font vivre tout un écosystème ([www.theconversation.com](http://www.theconversation.com)).

### 3.1. Quelques logiciels de clonage et leur danger

- Dr. Fone - Transfert de téléphone

Le premier logiciel de clonage de téléphone de notre liste est *Dr.Fone transfert de téléphone*. Il fait partie de la boîte à outils Dr. Fone et offre un moyen rapide et fiable de déplacer vos données d'un appareil à un autre. Ce logiciel de clonage de téléphone portable peut être installé sur votre appareil Mac ou Windows. Ensuite, vous pouvez l'utiliser pour déplacer vos données entre Android, Windows, iOS, et tous les principaux smartphones (supporte plus de 6000 appareils). Par conséquent, Dr. Fone Switch peut être utilisé comme un logiciel de clonage Android ainsi qu'un logiciel de clonage iPhone.

- Outil de clonage de SIM - MOBILedit

Développé par MOBILedit, l'outil de clonage de SIM est essentiellement un ensemble de cartes SIM réinscriptibles qui est utilisé à des fins médico-légales. Bien qu'il puisse également être utilisé comme un logiciel de clonage de téléphone. Il possède de nombreuses fonctionnalités avancées qui permettent de cloner et de copier la carte SIM d'un téléphone sans trop de difficultés. Plus tard, vous pouvez même formater la carte SIM pour supprimer ses données. De cette façon, vous pouvez vous débarrasser de vos contacts d'un appareil existant pour le revendre également.

- Phone Clone - Huawei

Si vous recherchez un logiciel de clonage de téléphone portable rapide et sans fil, vous pouvez également essayer Phone Clone. Cet outil hautement sécurisé et avancé, développé par Huawei Technologies et est disponible gratuitement sur Google Play et iOS App Store. Il prend en charge le transfert sans fil de musique, de photos, de vidéos, d'applications, de paramètres, etc. Même si l'outil a été conçu spécifiquement comme un logiciel de clonage mobile pour les téléphones Huawei, vous pouvez l'utiliser pour déplacer votre contenu d'iPhone à Android et d'Android à Android également.

### 3.2. *Les nouvelles maladies du téléphone mobile*

En dehors de ce danger de clonage, le smartphone nous a amené plusieurs maladies devenues un mode de vie. Ces nouvelles maladies apparaissent avec les téléphones portables intelligents.

- La dépendance au smartphone

La dépendance ou l'addiction au smartphone est un phénomène qui apparaît depuis la large diffusion des smartphones. Il relève, du moins en partie, de la cyberaddiction (*dépendance à Internet*) qui peut se développer, notamment

dans le cadre du nomadisme numérique, ou révèle souvent d'autres addictions<sup>1</sup>. Il peut ajouter à la dépendance au téléphone et à l'information disponible sur l'Internet une autre dépendance, à certains des réseaux sociaux qui se sont développés grâce à l'internet. H. ATLAN et al. (1999 : 54).

«Ce trouble est classé dans les pathologies communicationnelles ; troubles psychologiques entraînant chez le « mobinaute », un besoin excessif, incontrôlable voire obsessionnel d'utiliser un téléphone au point d'y consacrer tant de temps et d'énergie, que l'objet et son utilisation finissent par interférer négativement avec la vie quotidienne, professionnelle ou affective du sujet qui peut développer une anxiété, parfois phobique ou une dépression qui vont indirectement aussi affecter son entourage. Cette dépendance se résout parfois d'elle-même, et dans ce cas, à la différence des dépendances chimiques elle n'entraînerait pas ou peu de séquelles physiques et psychiques pour la santé, affirmation que seules des études épidémiologiques de long terme pourront confirmer.

« Cette nouvelle addiction semble tendre, pour partie au moins, à se substituer à l'addiction à la télévision. Elle touche davantage les jeunes ; selon une étude parue en 2013, 7 % des 50 millions de Sud-Coréens (dans l'un des pays les plus « câblés » au monde), présentent « un risque élevé » d'addiction à l'internet, mais ce taux triple en grimant à près de 20 % chez les adolescents (génération née et ayant grandi avec internet), les étudiants de haut niveau ne sont pas les moins touchés et 240 000 adolescents seraient susceptibles d'être touchés par ce phénomène en Corée rien qu'en 2013. Autant d'utilisateurs potentiellement sujets à des nouveaux troubles. Car si l'on parle souvent de la dangerosité des ondes électromagnétiques pour notre santé, on évoque plus rarement les nouvelles maladies apparues avec l'émergence des téléphones portables. Dépendance, trouble de l'équilibre, problèmes oculaires... Retour sur ces pathologies dont vous souffrez peut-être sans même le savoir ».

- La nomophobie

Comprenez la « no mobile phone phobia », soit la "phobie du non téléphone portable". Il s'agit de l'inquiétude phobique de ne pas pouvoir utiliser son portable : mauvais signal, niveau de batterie insuffisant, difficulté à trouver son téléphone, etc. Autant d'éléments qui peuvent provoquer un stress intense chez certains utilisateurs dépendants. Une pathologie qui rend incapable d'éteindre son téléphone portable ou de ne pas vérifier ses notifications de manière systématique.

- Le cybermalaise

Il s'agit d'un déséquilibre causé par l'utilisation d'applications 3D disponibles sur certains smartphones. Ces applications entraîneraient un décalage entre les mouvements oculaires et les signaux reçus par le système qui contrôle l'équilibre, le cerveau interprétant les mouvements 3D comme des mouvements réels. Un décalage qui peut engendrer troubles oculaires, nausées et étourdissements.

- Le syndrome du téléphone fantôme

Causé par une dépendance au téléphone, ce syndrome se traduit tout simplement par la fausse impression, régulière et répétée, que son téléphone est en train de vibrer. Un syndrome qui peut également être auditif, avec la sensation d'entendre son téléphone sonner quand ce n'est pas le cas. Comme pour la nomophobie, il s'agit souvent d'un signe d'addiction au téléphone qui peut entraîner des comportements compulsifs.

- Le syndrome de l'œil sec

Il s'agit d'une détérioration oculaire liée au fait de fixer des écrans de manière prolongée. Avoir les yeux rivés sur un écran, particulièrement s'il est de petite taille comme celui d'un smartphone peut conduire à une réduction du nombre de clignements de l'œil d'environ un tiers et provoquer une modification de la production de larmes. A terme, cela peut amener à des dommages permanents aux yeux.

- La textonite ou tendinite du pouce

Rédaction de SMS, navigation sur le net : plus de 20 % des utilisateurs déclarent passer entre 2 et 4 heures par jour à pianoter sur leur téléphone. Une pratique qui sollicite beaucoup les articulations de nos doigts et peut avoir pour conséquence une inflammation des tendons et provoquer douleurs et crampes.

- Le "text-neck"

Outre la tendinite du pouce, une autre partie du corps peut être fortement affectée par le "texting" intensif : le cou. C'est ce que certains spécialistes appellent le text-neck ("texto" et "cou" en français) entraînant des douleurs et une raideur au niveau de la nuque et des épaules à force de pencher la tête pour envoyer des SMS, les lire ou naviguer sur Internet.

- L'insomnie causée par la lumière bleue

« Plusieurs études ont démontré les effets de la lumière bleue sur le sommeil. Celle-ci affecte notre horloge biologique basée sur le rythme jour/ nuit. Une exposition excessive aux écrans le soir ou avant le coucher peut entraîner des troubles du sommeil (insomnie ou difficulté à s'endormir). Pour éviter ces



désagréments, il est recommandé de ne pas utiliser les écrans durant l'heure précédant le coucher ».

#### **4. Piste des solutions pour faire face au clone et à des maladies liées au téléphone**

Au vu de ces nombreux désagréments, il est important de réduire son temps passé sur son mobile et d'apprendre à l'éteindre de temps en temps. Car si aujourd'hui, le smartphone est devenu presque indispensable dans l'accomplissement de certaines tâches, il peut aussi nuire à notre santé et à notre bien-être. En ce qui concerne le clone, le geofencing demeure la solution idéale pour limiter l'accès à vos données personnelles. Commençons par le geofencing et à quoi ça sert. Le geofencing ou géorepérage, sa traduction, est une technologie permettant de définir des barrières virtuelles pour un appareil électronique. Aussi appelé gardiennage virtuel, le geofencing est une fonctionnalité d'un programme logiciel ou d'une application permettant de définir des barrières géographiques virtuelles. L'administrateur du logiciel peut définir manuellement ces limites. Lorsque l'appareil sur lequel tourne le logiciel (généralement un smartphone) franchit les barrières virtuelles, en entrant dans la zone ou en la quittant, une alerte est émise. Le géorepérage repose généralement sur le Global Positioning System (**GPS**) ou sur la Radio Fréquence Identification (**RFID**). De nombreuses applications de geofencing incorporent aussi Google Earth pour permettre de définir une barrière géographique à part d'une vue satellite. Certaines applications définissent également les barrières virtuelles en se basant sur la longitude ou la latitude ou alors à partir de cartes basées sur le web.

Nous précisons que les barrières virtuelles peuvent être actives ou passives. Les barrières actives nécessitent qu'une application soit ouverte et que l'utilisateur se connecte à un service. Les barrières passives quant à elles fonctionnent en permanence en arrière-plan, et reposent sur le Wi-Fi ou les données cellulaires plutôt que sur le GPS ou le RFID. Dans le domaine de la communication marketing, le geofencing est également de plus en plus utilisé à tel point qu'un terme spécifique a vu le jour : le géomarketing. Par exemple, il est possible de définir une barrière virtuelle autour d'un magasin. Ainsi, lorsqu'un client potentiel franchit la barrière, il est possible de lui envoyer une offre promotionnelle ou une pub mobile sur son smartphone pour l'inciter à l'achat.

De même, il est possible de délimiter une barrière virtuelle autour d'un magasin concurrent pour proposer aux clients des offres promotionnelles compétitives. Par ailleurs, même si le géorepérage ne permet pas systématiquement de pousser le chaland à l'achat, il est possible d'utiliser cette

technologie pour surveiller le comportement des clients au sein d'un magasin physique, afin de se baser sur ces informations pour élaborer des campagnes marketing plus efficaces.

### **Conclusion**

Il est impératif de chercher des réponses à ces questions car, avec la généralisation du paiement sur smartphone et la multiplication des objets connectés (montres intelligentes, maison intelligente, voitures connectées...), celles-ci s'étendent déjà à d'autres domaines. Après cette étude, les progrès restent donc possibles au regard du respect de la vie privée des utilisateurs de smartphones. D'abord, les utilisateurs eux-mêmes devraient se montrer plus responsables, d'une part en étant conscients que la gratuité totale n'existe pas, quelqu'un doit forcément soutenir financièrement le travail et d'autre part en faisant preuve de plus de vigilance en matière d'autorisation lorsqu'ils installent et paramètrent des applications sur leur smartphone. Par exemple, en suivant des recommandations simples. Ensuite, les autres acteurs de l'écosystème (éditeur du système d'exploitation, développeur, régie publicitaire) gagneraient à être plus transparents vis-à-vis de leurs pratiques ; ils devraient aussi être en mesure de prouver techniquement leur conformité par rapport à la législation.

Enfin, des tiers de confiance typiquement, l'Autorité de Régulation de la Poste et des télécommunications du Congo (ARPTC) devrait pouvoir contrôler ces acteurs même étrangers. D'où la nécessité de justifier l'apport du RAM (Registre d'Appareils Mobile). Ainsi donc, cette réflexion nous permet d'ouvrir des champs de recherche en communication numérique. Il est plus que temps de prendre conscience de l'importance des données privées et d'en limiter l'accès avec des outils souples et appropriés.

### **Références bibliographiques**

- ATLAN, H. et al., 1999, *Le clonage humain*, Paris, Edition du Seuil.
- CAELEN, J. et COURAZ, J., 2009, *Interaction homme-machine multimodale : quelques problèmes*. Bulletin de la communication parlée n°2.
- CARON, A. et CARONIA, L., 2005, *Culture mobile. Les nouvelles pratiques de communication*, Montréal, PUM
- COUTAZ J., 1990, *Interface homme-ordinateur : conception et réalisation*, Paris, Dunod.
- MONTAGUT, J., 2008, *Le clonage*, Paris, Edition Idées reçues.
- [www.celltrackingapps.com](http://www.celltrackingapps.com)
- [www.commentcamarche.com](http://www.commentcamarche.com)
- [www.google.com](http://www.google.com)
- [www.theconversation.com](http://www.theconversation.com)