EUROPEAN DATA PROTECTION SUPERVISOR

Avis 1/2015

La santé mobile

Concilier innovation technologique et protection des données

21 mai 2015

TABLE DES MATIÈRES

RÉSUMÉ

La santé mobile est un secteur en croissance rapide, issu de la convergence entre les soins de santé et les TIC. Il englobe des *applications mobiles* destinées à fournir des services liés à la santé via des dispositifs intelligents, et impliquant souvent le traitement d'informations à caractère personnel relatives à la santé. Les applications de santé mobile traitent également de grandes quantités d'informations relatives au *mode de vie* et au *bien-être*.

Le marché de la santé mobile est compliqué, car de multiples opérateurs publics et privés interviennent simultanément (développeurs d'applis, magasins d'applis, fabricants de dispositifs, publicitaires, etc.) et les modèles économiques qu'ils adoptent évoluent constamment pour s'adapter à une dynamique de changement accéléré. Ils n'en sont pas moins tenus, lorsqu'ils traitent des informations à caractère personnel, de respecter les règles de protection des données et d'assumer la responsabilité de leurs opérations de traitement. De plus, les informations relatives à la santé bénéficient, en vertu de ces règles, d'un niveau de protection très élevé.

Le développement de la santé mobile recèle un potentiel considérable d'amélioration en ce qui concerne les soins de santé et la vie des individus. D'autre part, les mégadonnées ainsi que l'«internet des objets» devraient avoir un impact considérable sur la santé mobile, en raison de la masse d'informations disponibles et de la qualité des conclusions qu'il est possible d'en tirer. Il devrait en découler de nouvelles perspectives pour la recherche médicale, de même qu'une réduction des coûts et une simplification de l'accès des patients aux soins de santé.

D'un autre côté, il est nécessaire de protéger la dignité et les droits fondamentaux des personnes, en particulier les droits au respect de la vie privée et à la protection des données. L'exploitation généralisée des mégadonnées risque de compromettre la maîtrise des utilisateurs sur leurs données à caractère personnel. Cela est dû, en partie, à l'énorme déséquilibre entre les informations limitées dont disposent les personnes et la masse de données auxquelles ont accès les entités qui proposent des produits impliquant le traitement de ces données à caractère personnel.

Nous pensons que les mesures suivantes relatives à la santé mobile seraient significativement bénéfiques au regard de la protection des données:

- le législateur de l'Union devrait s'attacher, dans les mesures politiques futures concernant la santé mobile, à renforcer la responsabilisation et la répartition des responsabilités de ceux qui participent à la conception, à la fourniture et au fonctionnement des applis (notamment les concepteurs d'applis et les fabricants de dispositifs);
- les concepteurs et éditeurs d'applis devraient concevoir des dispositifs et des applications qui renforcent la transparence et le niveau d'information des utilisateurs sur le traitement de leurs données et s'abstenir de collecter plus de données que nécessaire pour l'exécution de la fonction prévue. À cet effet, il conviendrait qu'ils intègrent à la conception des paramètres relatifs au respect de la vie privée et à la protection des données, et qu'ils prévoient leur applicabilité par défaut dans les cas où l'utilisateur ne serait pas invité à définir manuellement ses options de protection des données, par exemple lors de l'installation de l'appli sur son dispositif intelligent;
- les entreprises devraient utiliser les mégadonnées en santé mobile pour des finalités qui soient au service des individus, et s'abstenir d'y recourir pour des pratiques susceptibles de leur porter préjudice, comme le profilage discriminatoire;
- le législateur devrait renforcer la sécurité des données et encourager la mise en œuvre des principes de respect de la vie privée dès la conception et de respect de la vie privée par défaut, grâce à l'ingénierie de la vie privée et au développement de briques et d'outils applicatifs.

Bien que la santé mobile soit un secteur nouveau et en développement, les règles de l'Union en matière de protection des données – en leur état actuel, mais aussi telles que la réforme est appelée à les renforcer – prévoient des garanties pour la protection des données à caractère personnel. D'autre part, nous inviterons l'IPEN (Internet Privacy Engineering Network - réseau d'ingénierie de la vie

privée sur Internet) à tester de nouvelles bonnes pratiques et des solutions innovantes dans le domaine de la santé mobile. Enfin, eu égard à la dimension mondiale du traitement des données dans le cadre de la santé mobile, il est impératif de mettre en place une coopération renforcée entre les autorités de contrôle de la protection des données du monde entier.

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, et en particulier son article 41, paragraphe 2, et son article 46, point d),

A ADOPTÉ LE PRÉSENT AVIS:

I. INTRODUCTION ET CONTEXTE

I.1 L'émergence de la santé mobile - intérêt social et mégadonnées

1. Au début des années 2000, les secteurs des médias, des technologies de l'information et des communications électroniques ont engagé leur convergence, donnant ainsi naissance à un nouvel environnement économique en même temps qu'à de nouveaux besoins réglementaires. De la même façon, aujourd'hui, le secteur de la santé a trouvé de nouveaux gisements de développement et de croissance dans la convergence avec les nouvelles technologies (dispositifs intelligents et applis mobiles liées). Cette combinaison vise fondamentalement à dispenser des soins de santé aux utilisateurs par l'intermédiaire de dispositifs intelligents. Elle est considérée comme un «*nouveau domaine d'activité dont le développement rapide peut contribuer à faire évoluer les soins de santé et à accroître leur qualité et leur efficience*»[1].

2. La convergence entre nouvelles technologies et soins de santé devrait permettre i) d'offrir de meilleurs soins de santé à moindre coût, ii) d'autonomiser le patient (en lui permettant de gérer ses propres soins de santé)[2] et iii) d'assurer un accès plus facile et plus immédiat aux informations et aux soins médicaux en ligne (p. ex. en permettant aux médecins de surveiller leurs patients à distance et de communiquer plus souvent avec eux par courrier électronique).

3. La réalisation de ces objectifs passe par la conception et la distribution de dispositifs mobiles (p. ex. dispositifs informatiques portables) et d'applis fonctionnant sur les dispositifs intelligents des utilisateurs. Ces dispositifs sont en mesure de recueillir, à l'aide de «capteurs», un volume croissant de données à caractère personnel (la capacité de stockage et la puissance de calcul augmentent de façon exponentielle, tandis que les prix baissent), lesquelles peuvent, le cas échéant, faire l'objet d'un traitement ultérieur dans les centres de données des fournisseurs, aux capacités informatiques sans précédent. L'alliance entre utilisation et connectivité généralisées, services à but lucratif souvent proposés à titre gratuit aux utilisateurs (telles les applis mobiles gratuites), mégadonnées et exploration de données, joue un rôle crucial dans la santé mobile, en construisant une image numérique de chacun d'entre nous (la «*quantification de soi*»)[3].

[1] Commission européenne, Livre vert sur la santé mobile, 10 avril 2014, COM(2014) 219 final, complété par un document de travail des services de la Commission [SWD(2014) 135 final].
[2] Cortez, N., «The Mobile Health Revolution?», *University of California Davis Law Review*, vol. 47, p. 1173.
[3] Kelvin Kelly, fondateur de *Wired*, a créé la plateforme *quantifiedself.com* avec le journaliste Gary Wolf, et a contribué à populariser ce concept auprès du grand public.

I.2 Objectif de l'avis

4. Eu égard à l'incidence que le développement de la santé mobile est susceptible d'avoir sur les droits des personnes en matière de respect de la vie privée et de protection des données à caractère personnel, nous avons décidé, de notre propre initiative, d'émettre le présent avis.

5. Son objet est d'attirer l'attention sur les principaux aspects de la protection des données dans le domaine de la santé mobile, qui pourraient aujourd'hui être négligés ou sous-estimés, afin de mieux assurer le respect des dispositions en vigueur en matière de protection des données et d'ouvrir la voie à une application systématique de ces dispositions. Il s'inspire, à cet effet, de l'avis adopté par le groupe de travail «Article 29» sur les applis mobiles installées sur les dispositifs intelligents[4].

6. Il examine également les possibles répercussions de ce nouveau scénario, en mutation rapide, au regard des modifications envisagées dans la proposition de règlement général sur la protection des données («RGPD»).

7. Le présent avis comporte deux sections. La section II met en évidence les principales implications de la santé mobile sur la protection des données. La section III propose des pistes pour l'intégration des exigences en matière de protection des données dans la conception des applis de santé mobile, en insistant sur les nouvelles mesures législatives qui apparaissent à la fois souhaitables et nécessaires pour apporter une réponse efficace aux questions que la santé mobile soulève ou est susceptible de soulever à plus ou moins brève échéance, en termes de dignité, de respect de la vie privée, de protection des données et de droit à l'identité personnelle.

II. LES IMPLICATIONS DE LA SANTÉ MOBILE SUR LA PROTECTION DES DONNÉES

II.1 Les exigences imposées par les règles de l'Union

8. Le respect de la vie privée et la protection des données à caractère personnel constituent des droits fondamentaux au titre des articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne[5]. En outre, la directive «protection des données»[6] et la directive «vie privée et communications électroniques»[7] contiennent des dispositions spécifiques actuellement applicables à la santé mobile. Celles-ci prévoient que tout traitement de données à caractère personnel doit obligatoirement respecter certaines garanties, par

[4] Avis 02/2013 du groupe de travail «Article 29» du 27 février 2013 sur les applications destinées aux dispositifs intelligents (WP 202), disponible à l'adresse http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_fr.pdf.

[5] Sur la différence entre les deux droits fondamentaux consacrés respectivement aux articles 7 et 8, voir les lignes directrices du CEPD relatives à la protection des données dans la réglementation européenne des services financiers, disponible à l'adresse https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Thematic%20Guidelines/14-11-25_Financial_Guidelines_FR.pdf.

[6] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JO L 281 du 23.11.1995, p. 31–50.

[7] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), JO L 201 du 31.7.2002, p. 37–47.

exemple le double impératif selon lequel les informations à caractère personnel ne peuvent être traitées qu'à des fins spécifiques (limitation de la finalité) et ne doivent jamais être transférées vers un pays tiers n'offrant pas un niveau de protection adéquat (transferts internationaux). En particulier, les informations relatives à la santé bénéficient d'un degré de protection plus élevé et ne peuvent faire l'objet d'un traitement que si certaines conditions sont réunies, notamment le consentement spécifique et informé de l'utilisateur[8].

II.2 Définition des types de données traitées en santé mobile

9. La première question à laquelle il convient de répondre est de savoir si les informations traitées dans le contexte de la santé mobile sont des données à caractère personnel relatives à des personnes physiques identifiées ou identifiables et relèvent, en tant que telles, du cadre juridique de la protection des données. Dans l'affirmative, il y a lieu de déterminer, ensuite, si certaines d'entre elles, et lesquelles, doivent être considérées comme des données relatives à la santé d'un individu et sont par conséquent soumises aux règles plus strictes de protection des données applicables à des catégories particulières de données. Cette question est d'autant plus pertinente que le volume d'informations concernant le mode de vie et le bien-être souvent partagé sur les dispositifs intelligents et les applications sociales est important[9].

Les données traitées en santé mobile sont des données à caractère personnel

10. S'agissant de la première question, il y a lieu d'observer que **les données traitées dans le cadre de la sa santé mobile sont, en principe, des données à caractère personnel**, puisqu'elles concernent des personnes physiques identifiées ou identifiables [article 2, point a), de la directive 95/46/CE, ci-après la «directive»].

11. La pseudonymisation et même l'anonymisation[10] ne changent rien, fondamentalement, à la nécessité de mettre en œuvre des garanties de protection des données aux données de santé mobile. **Les données pseudonymes demeurent des données à caractère personnel dans la mesure où elles peuvent être réidentifiées non seulement par le responsable du traitement, mais aussi par des tiers qui les combinent avec des informations externes émanant d'autres sources[11].**

---

[8] L'article 8 de la directive «protection des données» interdit le traitement de catégories particulières (c'est-à-dire «sensibles») de données, notamment celles relatives à la santé, sous réserve de certaines dérogations, qui sont d'interprétation stricte.

[9] Selon le livre vert de la Commission, la santé mobile recouvre «*les pratiques médicales et de santé publique reposant sur des dispositifs mobiles tels que téléphones portables, systèmes de surveillance des patients, assistants numériques personnels et autres appareils sans fil*». Cela englobe notamment «*les applications concernant le mode de vie et le bien-être qui peuvent se connecter à des dispositifs médicaux ou capteurs (p. ex. bracelets ou montres) ainsi que les systèmes de conseil personnalisés, les informations de santé et rappels de prise de médicament envoyés par SMS et la télémédecine pratiquée par communication sans fil*».

[10] Même lorsqu'elles sont considérées comme anonymisées, les données peuvent posséder des caractéristiques intrinsèques conduisant à l'identification d'une personne précise (dans le cas d'une maladie rare, par exemple, lorsque le nombre de patients à l'échelle mondiale est réduit, le risque existe qu'ils soient facilement identifiés).

[11] Voir avis 4/2007 du groupe de travail «Article 29» du 20 juin 2007 sur le concept de données à caractère personnel (WP 136), disponible à l'adresse http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_fr.pdf, et avis 05/2014 du 10 avril 2014 sur les techniques d'anonymisation (WP 216), disponible à l'adresse http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_fr.pdf.

Les données traitées dans le contexte de la santé mobile doivent-elles toutes être considérées comme des données de santé sensibles?

12. S'agissant de la seconde question, dans de nombreux cas, les données traitées dans le domaine de la santé mobile concernent ou révèlent l'état de santé physique (ou mentale) des individus utilisant les dispositifs ou les applis[12], et relèvent donc du régime plus strict de protection des données applicable aux catégories particulières de données (article 8 de la directive). Pour autant, il n'y a pas de réponse simple et définitive à cette question: l'évaluation permettant de déterminer, parmi les données traitées en santé mobile, celles qui constituent des données de santé sensibles ne peut se faire qu'au cas par cas. **Les données relatives au mode de vie et au bien-être sont, en règle générale, considérées comme des données de santé dès lors qu'elles sont traitées dans un contexte médical (p. ex. lorsque l'appli est utilisée sur conseil du médecin) ou que l'on peut raisonnablement déduire des données (en elles-mêmes ou combinées à d'autres) des informations concernant la santé d'une personne, en particulier lorsque la finalité de l'application est de surveiller la santé ou le bien-être de la personne (que ce soit dans un contexte médical ou autre).**

13. Bien que le cadre européen existant en matière de protection des données comporte des dispositions concernant le traitement des données sensibles (dont font partie les données de santé), il ne donne, à l'heure actuelle, aucune définition des données de santé (la situation est différente au niveau des États membres)[13].

14. Le règlement général sur la protection des données (RGPD)[14], en attente d'adoption, définit les «*données concernant la santé*» comme «*toute information relative à la santé physique ou mentale d'une personne, ou à la prestation de services de santé à cette personne*»[15]. Plus intéressante est la liste détaillée, sans pour autant être exhaustive, figurant au considérant 26 du RGPD[16], qui, néanmoins, n'aborde pas expressément la question de savoir si, et dans quelle mesure, les informations concernant le mode de vie et le bien-être rentrent dans le champ des informations relatives à la santé.

---

[12] Les données de santé englobent aussi les documents administratifs comportant des données à caractère personnel relatives à l'état de santé d'une personne. Parmi ces documents figurent les certificats médicaux (p. ex. documents certifiant l'aptitude médicale au travail) et les formulaires concernant les congés maladie ou le remboursement des frais médicaux. Voir lignes directrices du CEPD concernant le traitement des données relatives à la santé sur le lieu de travail par les institutions et organes communautaires, septembre 2009, p. 2.

[13] Pour plus de détails, voir le premier rapport de la Commission européenne sur la mise en œuvre de la directive relative à la protection des données, disponible à l'adresse http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52003DC0265:en:NOT.

[14] COM(2012) 11 final.

[15] RGPD, article 4, point 12).

[16] Le considérant 26 indique que «*les données à caractère personnel concernant la santé devraient comprendre, en particulier, l'ensemble des données se rapportant à l'état de santé d'une personne concernée; les informations relatives à l'enregistrement du patient pour la prestation de services de santé; les informations relatives aux paiements ou à l'éligibilité du patient à des soins de santé; un numéro ou un symbole attribué à un patient, ou des informations détaillées le concernant, destinés à l'identifier de manière univoque à des fins médicales; toute information relative au patient recueillie dans le cadre de la prestation de services de santé audit patient; des informations obtenues lors d'un contrôle ou de l'examen d'un organe ou d'une substance corporelle, y compris des échantillons biologiques; l'identification d'une personne en tant que prestataire de soins de santé au patient; ou toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, un dossier médical, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'une épreuve diagnostique in vitro*».

15. Le rapport explicatif de la convention 108 du Conseil de l'Europe[17] indique que la notion de «données à caractère personnel relatives à la santé» couvre «*les informations concernant la santé passée, actuelle et future, physique ou mentale d'un individu. Il peut s'agir d'informations sur un individu bien portant, malade ou décédé*». Il est intéressant de noter, à cet égard, que la notion peut également se rapporter à des individus bien portants (ce qui corroborerait l'idée que les informations concernant le mode de vie et le bien-être doivent aussi être prises en considération, dans la mesure où elles sont de nature à affecter la santé future d'un individu bien portant).

16. **En l'absence de définition claire, après évaluation des circonstances particulières, la notion de données de santé devrait recevoir une interprétation large**, comme recouvrant toute donnée relative à la santé physique et mentale d'une personne[18]. Il doit être dûment tenu compte du fait que ce n'est pas seulement la nature intrinsèque de l'information qui permet de l'identifier comme une donnée de santé: les circonstances entourant sa collecte et son traitement jouent aussi un rôle. Comme le souligne une autorité nationale de protection des données[19], la distinction entre les données de santé et les informations liées à la notion de bien-être n'est pas toujours claire. Il y a au contraire un continuum, allant des situations où les informations de bien-être ont peu ou n'ont pas de rapport avec la santé d'une personne, aux cas où – selon les circonstances de la collecte et du traitement des données, notamment l'ampleur de celle-ci et les finalités du traitement – elles constituent manifestement des données de santé et sont peut-être même utilisées dans un contexte médical.

17. Par conséquent, une interprétation trop étroite de la notion de données de santé priverait les intéressés d'une protection adéquate des données relatives à leur mode de vie et à leur bien-être, lesquelles sont susceptibles de révéler des informations très intimes les concernant et risqueraient de saper leur confiance, compromettant ainsi les gains économiques et sociaux apportés par la santé mobile[20].

18. En tout état de cause, les responsables du traitement de données à caractère personnel en répondent et doivent rendre compte de la manière dont ils définissent juridiquement les informations relatives au mode de vie qu'ils traitent. Dans la majorité des cas, ils disposent d'éléments décisifs pour attribuer à ces informations la qualification de données de santé. Dès lors, ainsi que le groupe de travail «Article 29» l'a déjà fait observer, **les données relatives au mode de vie peuvent, dans certains cas, «*fournir des informations sur la santé d'une personne, dans la mesure où les données sont enregistrées au fil du temps, ce qui permet de tirer des conclusions de leur variabilité sur une période donnée. Il convient que les responsables du traitement des données anticipent cet éventuel changement de qualification et prennent les mesures qui***

[17] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, 28 janvier 1981, nº 108.

[18] Les deux catégories de données (mode de vie et bien-être) peuvent impliquer le traitement de données à caractère personnel relatives à la santé, déclenchant ainsi la protection renforcée conférée par l'article 8 de la directive. Voir l'avis du CEPD du 27 mars 2013 sur la communication de la Commission relative au «Plan d'action pour la santé en ligne 2012-2020 – des soins de santé innovants pour le XXIe siècle», points 10 et 11.

[19] Commission nationale de l'informatique et des libertés (CNIL), *Le corps, nouvel objet connecté*, Cahiers IP, nº 2.

[20] Dans le cadre d'une initiative du Global Privacy Enforcement Network (GPEN), les autorités de contrôle de la protection des données ont concentré leur attention sur les applis de santé mobile. Voir également la lettre du groupe de travail «Article 29» à la Commission du 5 février 2015, disponible à l'adresse http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_en.pdf.

***s'imposent»*[21]. Cette règle est efficace en ce qu'elle fait peser l'appréciation de la nature des données traitées (et, en dernière analyse, le respect de la loi) sur le responsable du traitement, c'est-à-dire l'entité qui dispose des meilleures informations[22].

Conséquences du défaut d'identification et de protection appropriée des données personnelles et sensibles en santé mobile

19. Le livre vert de la Commission sur la santé mobile permet d'appréhender l'ampleur du risque associé à l'absence de protection des personnes. Selon des estimations récentes[23], le nombre d'applis de santé mobile actuellement disponibles sur diverses plateformes s'élève à 97 000, dont 70 % ont pour objet le bien-être et la forme physique du consommateur, tandis que les 30% restants ciblent les professionnels de santé[24]. On prévoit également que, d'ici 2017, 3,4 milliards de personnes dans le monde auront un téléphone intelligent et que la moitié d'entre elles utiliseront des applis de santé mobile[25].

20. En contraste avec ces chiffres, qui font entrevoir des perspectives florissantes, seuls 23 % des consommateurs, selon le livre vert, ont déjà utilisé une solution de santé mobile, quelle qu'elle soit. De plus, 67 % n'ont pas l'intention d'utiliser leur téléphone portable pour gérer leur santé et 77 % n'ont jamais utilisé leur téléphone pour des activités liées à la santé[26]. En outre, 45 % des consommateurs se disent préoccupés par l'utilisation abusive de leurs données lorsqu'ils se servent d'un dispositif mobile pour des activités liées à la santé[27]. Ces inquiétudes se voient confirmées par le constat que 9 des 20 applis de santé les plus utilisées transmettent des données à des sociétés recueillant des informations sur l'utilisation que les gens font des téléphones portables[28].

21. Au vu des chiffres rappelés ci-dessus, le manque de confiance constitue le principal danger causé par l'absence de protection suffisante des données émanant des utilisateurs de la santé mobile. **Si le législateur, les instances réglementaires et les responsables du traitement des données ne procèdent pas à une identification correcte des données personnelles et sensibles (par exemple, s'ils estiment que les informations relatives au mode de vie ne peuvent en aucun cas être considérées comme des données de santé sensibles), les utilisateurs se détourneront de la santé mobile.** Inversement, des mécanismes efficaces de protection des données permettront de renforcer la maîtrise des utilisateurs sur leurs données et, ainsi, de favoriser leur participation à la santé mobile[29].

---

[21] Groupe de travail «Article 29» sur la protection des données, *Opinion 8/2014 on Recent Developments on the Internet of Things*, p. 17.
[22] Le GT «Article 29» donne quelques indications concernant la définition des données de santé dans sa lettre du 5 février 2015, disponible à l'adresse http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_en.pdf.
[23] research2guidance (2013), *Mobile Health Global Market Report 2013-2017 – The commercialisation of mHealth applications (vol. 3)*.
[24] Étude du cabinet Deloitte, *mHealth in a mWorld*, 2012.
[25] research2guidance, op. cit.
[26] Boehm, E., *Mobile Healthcare´s Slow Adoption Curve*, 2011, Forrester Research Inc.
[27] Blue Chip Patient Recruitment, *Leveraging Mobile Health Technology for Patient Recruitment*, octobre 2012.
[28] «Health apps run into privacy snags», *Financial Times*, 1er septembre 2013.
[29] Avis du CEPD sur le plan d'action pour la santé en ligne 2012-2020, point 13.

II.3 Un marché aux acteurs multiples: assigner les responsabilités et donner aux utilisateurs les moyens d'exercer leur contrôle

22. **Les différents acteurs du secteur de la santé mobile – développeurs d'applis, développeurs de systèmes d'exploitation (OS), fabricants de dispositifs, magasins d'applis et tiers (p. ex. publicitaires) – s'appuient tous, quoiqu'à des degrés divers, sur des modèles économiques fondés sur la monétisation des données à caractère personnel générées par les utilisateurs (ou concernant ceux-ci)**.

23. À mesure que les modèles économiques s'orientent vers de nouvelles modalités de monétisation des données à caractère personnel (p. ex. les *plateformes* et la «*coopétition*»[30]), il devient de plus en plus difficile pour les utilisateurs de garder le contrôle non seulement sur l'*utilisation effective* qui est faite de leurs données, mais aussi sur la *réutilisation* des données par des partenaires commerciaux du responsable du traitement et sur *l'utilisation potentielle* qui pourrait en être faite dès que de nouvelles possibilités de monétisation se feront jour grâce à l'évolution de la technologie et de l'activité. Par exemple, des données à caractère personnel divulguées à l'origine à une association de patients, dans le but de partager des informations sur une maladie particulière, pourraient ultérieurement être communiquées par cette même association à une société pharmaceutique qui vend un médicament pour le traitement de cette maladie et qui utilisera ces informations à des fins commerciales. Comme l'a souligné le CEPD dans un précédent avis[31], les dynamiques de la monétisation sont multiples et soulèvent un certain nombre de questions importantes au regard de la protection des données.

24. **Tout d'abord, compte tenu de la multiplicité des acteurs de la santé mobile et du rôle différent que joue chacun d'eux, il peut s'avérer difficile d'identifier tous les responsables du traitement et tous les sous-traitants et d'assurer une répartition adéquate des responsabilités.** L'identification du ou des responsables du traitement réalisé via des dispositifs et des applis mobiles est cruciale pour la détermination des instances chargées de garantir le respect du droit en matière de protection des données[32]. **Chaque entité doit être transparente, visible, tenue de rendre des comptes, seule ou conjointement avec d'autres, pour le traitement qu'elle assure des données à caractère personnel.**

25. En second lieu, il est difficile pour les particuliers d'être pleinement informés et donc de contrôler l'utilisation effective de leurs données à caractère personnel, qui - notamment dans les entreprises basées sur des plateformes (p. ex. les réseaux sociaux) - sont transférées à différentes entités (fabricants de dispositifs, éditeurs d'applis, opérateurs de plateformes ou tout autre responsable du traitement ou sous-traitant) pour y faire l'objet d'un traitement. En raison du manque de transparence et du peu d'informations dont ils

[30] CNIL, op. cit., p. 31. La caractéristique principale de ce modèle réside dans la capacité de l'opérateur de plateforme à faire de ses concurrents réels ou potentiels des partenaires commerciaux, passant de la compétition économique à la «*coopétition*».

[31] Avis du CEPD de mars 2014, *Vie privée et compétitivité à l'ère de la collecte de données massives: l'interaction entre le droit à la protection des données, le droit de la concurrence et la protection des consommateurs dans l'économie numérique*.

[32] Voir l'avis 1/2010 du groupe de travail «Article 29» du 16 février 2010 sur les notions de «responsable du traitement» et de «sous-traitant» (WP 169).

disposent sur la manière dont sont traitées leurs données à caractère personnel, les particuliers ne sont pas en état de donner leur consentement explicite[33].

26. Le problème est donc celui de *l'asymétrie de l'information* entre les opérateurs et les utilisateurs. D'un côté, les opérateurs actifs dans un certain nombre de secteurs (soins de santé, technologie, publicité, assurance, etc.) vont s'appliquer à étudier toutes les possibilités d'exploitation des données dans le cadre de nouvelles initiatives commerciales et d'amélioration de leurs marges. De l'autre, les utilisateurs n'auront pratiquement aucune perception ni compréhension de la dynamique commerciale entraînant l'exploitation de leurs données à caractère personnel. **La quantité croissante de données rendues disponibles et traitées sous l'effet de la tendance à faire fond sur les mégadonnées ne pourra qu'amplifier cette *asymétrie de l'information* et creuser le fossé entre responsables du traitement et utilisateurs.**

II.4 Le rôle des mégadonnées dans le domaine de la santé mobile

27. À la faveur du développement de la santé mobile, les mégadonnées devraient, selon toutes les prévisions, avoir une incidence considérable sur le secteur de la santé. **Dans la mesure où elles permettent d'établir des connexions entre des ensembles de données jusque-là sans rapport – et de tirer de nouvelles conclusions de ces corrélations –, les mégadonnées ouvrent à la recherche médicale de nouvelles perspectives, inimaginables auparavant[34].** Il sera possible, par exemple, de relier des maladies – telles que l'obésité, les maladies cardiovasculaires, la dépression – à un comportement humain, un mode de vie ou d'autres causes qui sont caractéristiques d'une zone géographique ou d'une population donnée.

28. Les mégadonnées peuvent également faciliter, du côté de l'utilisateur, la prise de décision ou la collecte de renseignements pertinents[35]. Toutefois, c'est dans l'exploitation commerciale des connaissances obtenues par la combinaison des données que les mégadonnées risquent de porter le plus atteinte à la vie privée des individus (et de susciter des inquiétudes majeures).

29. La théorie économique montre qu'un fournisseur maximise son profit lorsqu'il est capable d'opérer une distinction entre ses différentes catégories de clients (et donc, le cas échéant, de pratiquer une discrimination par les prix). En principe, si tous les patients sont indifférenciés, le prix qu'une société pharmaceutique fixera pour un médicament sera le même pour tous. Toutefois, si cette même société est capable d'identifier, parmi ses clients, ceux qui ont davantage de moyens financiers ou ont davantage besoin du médicament, elle pourrait être en mesure de leur appliquer un prix plus élevé (en leur proposant, par exemple, une version «premium» censée être plus efficace). Les mégadonnées sont susceptibles de faciliter ces discriminations à l'égard de tel ou tel

[33] Avis du groupe de travail «Article 29» sur les applications destinées aux dispositifs intelligents, p. 7.

[34] Boyd, D., et Crowford, K., *Six Provocations for Big Data*, (2011), p. 3. «*Les mégadonnées se distinguent non pas par leur taille, mais par leur relationnalité à d'autres données. Grâce aux efforts d'exploration et d'agrégation des données, les mégadonnées sont fondamentalement réseautées. Leur valeur découle des structures que l'on peut mettre au jour en établissant des connexions entre des éléments d'information concernant une personne, des personnes en relation avec d'autres, des groupes de personnes ou simplement la structure de l'information elle-même*».

[35] Par exemple, un prestataire de soins de santé ayant directement accès aux informations concernant des lésions subies par un athlète amateur pourra transmettre à ce dernier une liste de médecins susceptibles de l'accompagner dans sa phase de réadaptation.

groupe. Il existe donc un rapport direct entre la disponibilité de grands ensembles de données de santé et le potentiel de profitabilité d'un certain nombre d'industries actives dans le secteur de la santé, dans la mesure où les entreprises seront capables de mieux cibler leurs propositions commerciales et donc d'accroître leurs bénéfices en exploitant les données à caractère personnel. **Selon un cercle qui s'auto-entretient, plus grandes seront les possibilités de profit, plus forte sera la demande de données et plus impérieuse la nécessité de mettre en place des garanties efficaces contre tout abus.**

30. L'une des garanties les plus efficaces, à cet égard, consiste à rendre les utilisateurs conscients des finalités poursuivies par le traitement de leurs données à caractère personnel (*limitation de la finalité*). Alors qu'il est obligatoire de spécifier les finalités pour lesquelles des données de santé sont traitées, les opérateurs qui déploient des solutions de santé mobile se montrent généralement réticents au suivi et à la limitation de ces finalités. Cela s'explique par la rapidité d'évolution de la dynamique de marché, qui conduit les entreprises à explorer des possibilités qu'elles n'avaient jamais envisagées jusque-là.

31. La grande disponibilité des données et la possibilité de les traiter de nombreuses façons différentes à des fins commerciales et scientifiques favoriseront leur duplication et leur maximisation, en violation du principe de minimisation des données énoncé à l'article 6 de la directive. De ce point de vue, la limitation de la finalité et la minimisation des données vont de pair. Plus on admet de flexibilité dans les finalités du traitement, plus il est difficile de limiter les données au minimum nécessaire (la prolifération des applis mobiles contribue également à la tendance à la maximisation des données)[36].

32. D'autre part, les interactions entre l'internet des objets[37] et les mégadonnées dans le domaine de la santé mobile peuvent présenter des risques importants pour la protection des données, eu égard à la forte pénétration des dispositifs intelligents et des applis de santé mobile. Les *dispositifs informatiques portables*, qui comportent de multiples capteurs interconnectés capables d'enregistrer des fonctions corporelles et des informations relatives au mode de vie, intéressent tout particulièrement la santé mobile. La qualité des données produites par ces dispositifs et capteurs est variable, allant de simples données brutes à des combinaisons et à des inférences de données plus sophistiquées relatives à la personne concernée, révélant des aspects particuliers de ses habitudes, de son comportement et de ses préférences[38], et confortant ainsi l'idée d'un *soi quantifié* (c'est-à-dire d'une projection numérique de la personne).

33. L'exemple qui suit illustre ce que l'on peut entendre par «minimisation des données»: lors de la conception d'une appli mobile destinée à aider à lutter contre l'obésité, les

[36] Il se peut que les données à caractère personnel collectées par le biais d'applis soient ultérieurement distribuées à des tiers dont l'identité n'est pas révélée, pour des finalités mal définies telles que «étude de marché». Des études récentes montrent que des quantités massives de données à caractère personnel sont collectées sur les téléphones intelligents sans que cela ait le moindre lien sérieux avec la fonctionnalité manifeste de l'appli. Voir *Wall Street Journal*, «Your Apps Are Watching You», http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html.

[37] Avis du groupe de travail «Article 29» sur l'internet des objets (*Opinion 8/2014 on Recent Developments on the Internet of Things*): *«La notion d'internet des objets (IdO) désigne une infrastructure dans laquelle des milliards de capteurs intégrés à des dispositifs courants de la vie quotidienne – des «choses» en tant que telles ou des choses reliées à d'autres objets ou à des personnes – sont destinés à enregistrer, à traiter, à stocker et à transférer des données et, dans la mesure où des identificateurs uniques leur sont attribués, à interagir avec d'autres dispositifs ou systèmes utilisant des fonctionnalités de réseau»*.

[38] Avis du GT «Article 29» sur l'internet des objets, p. 8.

développeurs devraient s'assurer qu'elle ne collecte que les données à caractère personnel strictement nécessaires pour cette finalité. De ce point de vue, bien que l'appli puisse parfois faciliter le suivi calorique (en permettant par exemple aux utilisateurs de lire le code-barres des produits alimentaires qu'ils achètent), toute exploitation ultérieure par l'opérateur des informations sur les préférences des utilisateurs en matière de marques de produits va au-delà de la finalité première de l'appli et serait donc excessive.

34. **En outre, la collecte généralisée de données de santé sensibles ouvre la porte au profilage et à de possibles phénomènes de sélection adverse, par exemple dans le cadre d'un recrutement ou d'un contrat d'assurance.**

35. S'agissant du profilage, depuis quelques années déjà, les prestataires de soins de santé utilisent les mégadonnées (y compris la collecte de données génétiques) et des algorithmes pour développer la «médecine prédictive», discipline visant à prévenir les risques de santé futurs découlant des modes de vie actuels (tels que rapportés par les données). Les compagnies d'assurance pourraient également s'inscrire dans cette tendance en parrainant des programmes destinés à promouvoir le recours à des dispositifs mobiles de surveillance et au dépistage génétique[39].

36. Quant à la sélection adverse, le risque est que, si tous les assureurs et tous les prestataires de soins de santé privés adoptent, en tant que pratique normale, l'examen approfondi des données de santé à caractère personnel en vue d'adapter leur offre commerciale à chaque client, ils pourront automatiquement refuser de couvrir ceux qui s'opposent à cette divulgation ou à ce partage, indépendamment de leur état de santé ou de leurs facteurs de risque. Dans ces conditions, la pratique du partage des données entraînera automatiquement une discrimination à l'égard de ceux qui préfèrent ne pas divulguer ou partager leurs données de santé.

37. Les éventuelles distorsions – en particulier la maximisation des données et le profilage – causées par les mégadonnées peuvent être contrebalancées, du moins en partie, par l'application correcte du droit d'opposition de l'utilisateur[40], ainsi qu'il sera expliqué plus en détail à la section III.

II.5 Ingénierie d'une appli de santé mobile: principes essentiels

Obligations en matière de sécurité des données

38. Ainsi qu'il est souligné plus haut, le manque de confiance détournera les utilisateurs de solutions innovantes et empêchera la société de récolter les bénéfices de la santé mobile. **Il est par conséquent de la plus haute importance que tous les opérateurs garantissent la confidentialité, l'intégrité et la disponibilité des données à caractère**

[39] Pour le profilage, voir aussi la recommandation CM/Rec(2010)13 du Conseil de l'Europe sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage (adoptée le 23 novembre 2010), disponible à l'adresse https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec%282010%2913&Language=lanFrench&Ver=original&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383.

[40] L'article 14 de la directive est consacré à ce droit, qui est particulièrement important à l'ère de l'internet et dans le domaine de la santé mobile. La directive impose également une obligation de mise à jour des données (article 6) et permet à la personne concernée de s'opposer au traitement des données ou d'obtenir leur verrouillage lorsqu'elle estime qu'elles sont inexactes (article 12). L'état de santé d'une personne évolue en effet avec le temps et nul ne devrait être associé à des informations obsolètes.

personnel traitées dans le respect des règles de protection des données[41], des normes internationales et des bonnes pratiques[42]. Parmi toutes les options possibles en matière de sécurité de l'information, la gestion continue des risques est la pierre angulaire de toute activité de sécurité.

39. Bien que la confidentialité des données soit l'exigence la plus souvent mentionnée, d'autres aspects de la sécurité – l'intégrité et la disponibilité – sont tout aussi importants pour les données de santé.

40. Le manque d'outils et de pratiques appropriés (*respectueux de la vie privée*) est un problème pour tous les acteurs techniques concernés par le développement de dispositifs et d'applications de santé mobile (p. ex. développeurs d'applis et fabricants de dispositifs). Dans un environnement technologique en évolution rapide, les développeurs doivent livrer leurs produits rapidement, sous peine d'être devancés par leurs concurrents. Il arrive donc souvent qu'ils réutilisent des composants existants, malgré les failles que ceux-ci peuvent présenter en matière de respect de la vie privée. Cela laisse malheureusement peu de place à la conception de briques applicatives pour des applis et des services respectueux de la vie privée, avec souvent pour conséquence un faible niveau de sécurité. **Dans ces conditions, la mise en œuvre des principes du *respect de la vie privée par défaut* et du *respect de la vie privée dès la conception*, conjuguée à un effort systématique d'ingénierie de la vie privée, est indispensable pour remédier au problème. Le réseau IPEN[43] constitue un cadre pour la coopération entre ingénieurs et experts juridiques et réglementaires sur ces questions.**

Transfert de données vers les pays tiers

41. **Les dispositifs et les applis étant distribués à l'échelle mondiale par des sociétés informatiques et de soins de santé établies en dehors de l'Union européenne, il est fréquent que le traitement des données ait lieu à l'extérieur des frontières de l'Union.** En particulier, le scénario le plus pertinent (et le plus typique) en santé mobile comporte la réalisation du traitement des données dans un environnement en nuage mondial, les données étant transférées vers des pays tiers à l'insu ou sans le contrôle de l'utilisateur, souvent sous l'autorité d'un responsable du traitement établi en dehors de l'Union ou en dehors des pays couverts par une décision de la Commission constatant le caractère adéquat de la protection des données.

42. Une compagnie d'assurance allemande collectant des données sur les profils de risques de ses clients dans l'Union pourra, par exemple, en vertu de l'article 25 de la directive, les

[41] Notamment l'article 17 de la directive, qui impose au traitement des données l'application d'une gestion des risques liés au traitement d'informations.

[42] Groupe de travail «Article 29», op. cit., p. 14. Pour les mesures à prendre, les développeurs d'applis peuvent se reporter à des lignes directrices publiques en matière de sécurité telles que les «Smartphone Secure Development Guidelines» publiées par l'ENISA et disponibles à l'adresse http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/smartphone-secure-development-guidelines/at_download/fullReport.

[43] L'initiative IPEN (Internet Privacy Engineering Network – réseau d'ingénierie de la vie privée sur Internet) réunit des développeurs et des experts de la protection des données issus des instances réglementaires, du monde de l'entreprise, de la société civile et du milieu universitaire pour leur permettre de travailler ensemble à l'élaboration de solutions respectueuses de la vie privée dans le cadre de problèmes pratiques (https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/IPEN). À cet égard, nous encouragerons l'IPEN à effectuer des tests sur la santé mobile et à vérifier quelles sont les bonnes pratiques susceptibles d'être lancées/évaluées/recommandées par sa communauté d'ingénieurs et d'experts.

partager ultérieurement avec une autre compagnie d'assurance au Canada, ce pays ayant été reconnu, par décision de la Commission[44] [45], comme assurant un niveau de protection adéquat. Dans d'autres circonstances, en revanche, les transferts de données ne peuvent avoir lieu que si les critères et les garanties prévus aux articles 25 et 26 de la directive sont respectés[46].

III. PISTES POUR L'INTÉGRATION DES EXIGENCES EN MATIÈRE DE PROTECTION DES DONNÉES DANS LA CONCEPTION DES APPLIS DE SANTÉ MOBILE

III.1 Cadre législatif

43. Ainsi qu'il est exposé plus haut, dans le contexte de la santé mobile, nombre de types de données disponibles sur les dispositifs mobiles intelligents constituent des données à caractère personnel, de sorte que leur traitement doit s'effectuer dans le respect des règles de protection des données.

44. En outre, les données de santé révèlent des aspects intimes de la personne et peuvent aussi représenter une intrusion significative dans sa vie privée. Il y a lieu, à cet égard, de garantir le droit à la vie privée en remplaçant les mesures excessivement intrusives par d'autres options qui servent la même finalité tout en étant moins intrusives.

Mise en œuvre des règles en vigueur applicables au domaine de la santé mobile

45. Les responsables du traitement effectué à l'aide d'applis mobiles aussi bien que les concepteurs d'applis doivent tenir compte des règles existantes en matière de protection des données et, notamment, du caractère sensible des données de santé lorsqu'ils conçoivent leurs applis de santé mobile.

46. **En particulier, il est impératif que les responsables du traitement et les sous-traitants de données fassent un effort pour améliorer la transparence de leurs modalités de traitement, de partage et de réutilisation des données à caractère personnel, ainsi que des objectifs qu'ils poursuivent.** Le fait que le traitement de données à caractère personnel relatives à la santé puisse être motivé par des finalités commerciales aussi multiples que diverses n'exempte pas le responsable du traitement de son obligation d'informer correctement les utilisateurs, au contraire: il y a lieu de leur communiquer des informations suffisantes pour leur permettre de donner spécifiquement

[44] Décision 2002/2/CE de la Commission du 20 décembre 2001 constatant, conformément à la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par la loi canadienne sur la protection des renseignements personnels et les documents électroniques [notifiée sous le numéro C(2001) 4539].

[45] Dans de tels cas, le terme «transfert» couvrirait donc à la fois les «transferts délibérés» et l'«accès autorisé» aux données par le ou les destinataires. L'accès illégal et le piratage seraient exclus.

[46] Voir l'avis 3/2009 du groupe de travail «Article 29» (WP 161) concernant le projet de décision de la Commission relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants de données établis dans des pays tiers en vertu de la directive 95/46/CE (responsable du traitement de données vers sous-traitant de données) et la liste des questions les plus fréquentes soulevées par l'entrée en vigueur de la décision 2010/87/UE de la Commission du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE (WP 176), de même que les avis du GT sur les règles d'entreprise contraignantes et le document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995 (WP 114), tous disponibles à l'adresse http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

leur accord au traitement de leurs données de santé. La liberté de l'utilisateur de choisir et de décider ou non du traitement de ses données de santé ne doit pas se trouver limitée du fait de la conception de l'appli.

47. **De ce point de vue, l'une des garanties importantes que les applis et les dispositifs de santé mobile devraient mettre en œuvre serait d'accorder aux personnes concernées le choix de limiter le traitement des données de santé au seul niveau local, c'est-à-dire sur leurs dispositifs intelligents et non pas sur un serveur distant. De même, donner aux personnes concernées le libre choix d'autoriser ou non le responsable du traitement à partager leurs données à caractère personnel avec un tiers ou à les transférer à celui-ci constitue une fonctionnalité importante qui devrait être intégrée dans toutes les applications et tous les dispositifs de santé mobile. Toutes ces options devraient être intelligentes et faciles à mettre en œuvre, même par des utilisateurs non experts, sur la base d'un avis clair et simple à lire.**

48. **Il conviendrait que les concepteurs et les fabricants déploient, pour fournir aux utilisateurs des avis et des options de paramétrage concernant le respect de la vie privée efficaces et conviviaux, le même niveau de créativité et de dynamisme dont ils font ordinairement preuve lorsqu'ils mettent sur le marché des applis et des dispositifs attractifs. Les utilisateurs seraient ainsi en mesure de définir des options en matière de respect de la vie privée et de protection des données en ayant pleinement conscience qu'il s'agit d'un élément important de l'utilisation des dispositifs et des applis, et qu'il y va de leur intérêt personnel, au lieu que cela leur apparaisse comme une formalité ennuyeuse ou une tâche inutile.**

49. Afin de faciliter la maîtrise de l'utilisateur sur ses propres données – et à l'image de ce que font certains logiciels tournant sur ordinateur personnel –, au moment d'activer un dispositif ou une application de santé mobile, l'utilisateur devrait pouvoir décider aisément s'il souhaite définir manuellement ses paramètres de protection des données ou bien accepter/modifier les paramètres par défaut, qui doivent correspondre à des normes particulièrement élevées de respect de la vie privée et de protection des données (application du principe du *respect de la vie privée par défaut*). Il conviendrait également que les développeurs d'applis modèlent leurs options de protection des données sur des lignes directrices bénéficiant d'une large reconnaissance en la matière (p. ex. celles adoptées par l'ENISA[47]).

50. Il y a lieu de noter que le traitement de données à caractère personnel à l'aide d'applis mobiles est aussi, dans certains cas, le fait d'utilisateurs privés, ce qui peut entraîner leur responsabilité conjointe, en tant que responsables du traitement, pour les données qu'ils traitent. Un tel traitement ne saurait relever de l'«*exception prévue pour les activités domestiques*»[48] lorsque, par exemple, l'utilisateur de l'appli a l'intention de diffuser des données à caractère personnel sur Internet (via un réseau social ou une liste de diffusion). L'exception domestique doit aussi être appliquée de manière stricte[49] en ce sens que, indépendamment de la question de savoir si l'utilisateur satisfait à ses critères, les organisations participant à la conception, à la fourniture et au fonctionnement de l'appli

[47] Voir supra note 42.
[48] Article 3, paragraphe 2, de la directive.
[49] Arrêt de la Cour du 11 décembre 2014 dans l'affaire C-212/13, František Ryneš/Úřad pro ochranu osobních údajů (points 29 et suivants).

(concepteurs d'applis, magasins d'applis et tiers) conservent la responsabilité du traitement qu'ils effectuent à leurs propres fins.

51. Dans la mesure où la santé mobile implique le traitement de données par l'intermédiaire de dispositifs intelligents, il y a lieu de noter que le consentement informé et valable de la personne concernée est une condition préalable au stockage ou à l'accès à des informations sur l'équipement terminal d'un abonné ou d'un utilisateur[50].

Le RGPD: la «modernisation» du cadre régissant la protection des données

52. Le RGPD, qui n'est encore, pour l'heure, qu'une proposition, mais dont l'examen est déjà bien avancé, apportera des modifications substantielles concernant la protection des données en ligne, y compris dans le domaine des soins de santé.

53. **De manière générale, le RGPD vise à renforcer les droits de la personne concernée, notamment dans les situations où l'atteinte à son droit à la vie privée risque de se trouver amplifiée par l'interaction en ligne[51]. Le RGPD introduit également de nouveaux principes directeurs et de nouvelles règles applicables à la santé mobile[52].** Par exemple, le respect de la vie privée dès la conception et le respect de la vie privée par défaut deviennent des obligations légales (et non plus de simples «bonnes pratiques») dans le cadre du RGPD[53], et devront donc être pleinement pris en considération lors de la conception de nouveaux dispositifs ou applis de santé.

54. Quant à l'interaction entre le droit de l'Union européenne et le droit national, le RGPD semble laisser une marge de manœuvre substantielle au législateur national[54]. À cet égard, dans la mesure où le secteur de la santé est concerné par l'exercice d'un tel pouvoir discrétionnaire, nous pensons qu'**il ne faudrait pas que l'adoption d'une législation nationale porte préjudice à l'application cohérente du droit de l'Union en matière de protection des données en créant plus de divergences qu'il n'en résout.**

III.2 Mesures complémentaires visant à renforcer les garanties en matière de protection des données dans le domaine de la santé mobile

Renforcer la responsabilisation

55. Une approche systématique des enjeux de la santé mobile exige que le ou les responsables du traitement des données soi(en)t correctement identifié(s) et que les responsabilités

[50] Article 5, paragraphe 3, de la directive «vie privée et communications électroniques» (2002/58/CE), applicable à toute entité, quelle que soit sa nature (publique ou privée, personne physique ou personne morale, responsable du traitement, sous-traitant ou tiers), qui place ou lit des informations sur des dispositifs intelligents. Voir aussi groupe de travail «Article 29», op. cit., p. 7.
[51] Voir, par exemple, les articles 11, 12 et 14.
[52] En particulier, l'article 4, point 12), qui définit les «données concernant la santé», l'article 20 relatif au profilage (y compris le profilage en matière de santé et le profilage «prédictif»), l'article 33 sur l'analyse d'impact relative à la protection des données (y compris les traitements présentant des «risques particuliers», comme celui des données de santé) et l'article 81 relatif aux garanties encadrant le traitement des données de santé.
[53] Article 23 sur la «Protection des données dès la conception et protection des données par défaut».
[54] Avis du CEPD sur le paquet de mesures pour une réforme de la protection des données, points 50 et suivants.

soient organisées efficacement, dans l'hypothèse où plusieurs acteurs du marché participeraient au traitement des données[55] [56].

56. De ce point de vue, nous avons expliqué plus haut que la dynamique du marché ne cesse d'évoluer en créant de nouveaux modèles économiques, qui font éventuellement intervenir de nouvelles entités ou de nouveaux opérateurs. Afin d'éviter que la croissance rapide d'un environnement de marché articulé ne dégénère en chaos, il est indispensable que la responsabilité de chaque traitement de données soit attribuée de manière cohérente et systématique. Quiconque a un intérêt, ou poursuit un objectif, lié à des données à caractère personnel et qui, à ce titre, procède à leur traitement, est responsable devant les utilisateurs dont il traite les données.

Garantir l'application correcte des règles de protection des données

57. Bien que la santé mobile soit pour une large part un phénomène nouveau, tant la directive «protection des données» que la directive «vie privée et communications électroniques» comportent des dispositions capables de protéger les droits des utilisateurs. Il appartient donc aux décideurs politiques, aux responsables du traitement et aux autorités de contrôle de la protection des données de s'assurer que les règles en la matière sont correctement mises en œuvre, de façon responsable et proactive.

58. Comme le souligne le groupe de travail «Article 29», le principe de la limitation de la finalité et celui de la minimisation des données vont de pair[57]. Ils contribuent tous deux à prévenir la réutilisation illicite des informations à caractère personnel. Dans la mesure où le contexte économique actuel tend vers la réutilisation et l'exploitation intensive de données à de multiples fins (y compris, parfois, des fins imprévues), il est impératif que la finalité du traitement soit clairement identifiable pour les utilisateurs, que les mesures de protection soient correctement appliquées par les responsables du traitement et que la divulgation et le traitement des données soient limités au minimum nécessaire.

59. Il est clair, de ce point de vue, que les autorités compétentes en matière de protection des données, au niveau de l'Union comme à l'échelon national, ont un rôle essentiel à jouer en surveillant l'application de ces règles et en intervenant si nécessaire. D'autre part, la dimension mondiale du traitement appelle de manière impérieuse une coopération renforcée entre les autorités de contrôle de la protection des données du monde entier, dans le cadre d'une stratégie cohérente.

Promouvoir une application cohérente des règles de protection des données dans le domaine de la santé mobile

60. Il importe également que le législateur de l'Union et les acteurs de la santé mobile tiennent dûment compte des lignes directrices établissant des normes pour le traitement des données de santé, telles que le document de travail du groupe «Article 29» sur le traitement des données à caractère personnel relatives à la santé contenues dans les

[55] Voir avis 1/2010 du GT «Article 29» du 16 février 2010 sur les notions de «responsable du traitement» et de «sous-traitant» (WP 169), disponible à l'adresse http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_fr.pdf.

[56] Avis du CEPD sur le plan d'action pour la santé en ligne 2012-2020, point 19. Nous observons à cet égard que le RGPD comporte des règles plus spécifiques en matière de responsabilisation, dans le souci d'une répartition efficace des responsabilités et de la détermination correcte de la ou des entités responsables.

[57] Avis du groupe de travail «Article 29» sur les applications destinées aux dispositifs intelligents, p. 20.

dossiers médicaux électroniques (DME)[58] et la recommandation du Conseil de l'Europe sur la protection des données médicales[59]. Un code de conduite élaboré par les acteurs de la santé mobile avec la contribution des autorités de contrôle de la protection des données pourrait également faciliter l'application cohérente des règles existantes en matière de protection des données dans le domaine de la santé mobile.

Donner aux utilisateurs les moyens d'exercer leur contrôle

61. L'un des objectifs liés au développement de la santé mobile est de renforcer l'*autonomisation* des patients, en leur donnant les moyens d'exercer un plus grand contrôle sur leur santé et leurs soins de santé.

62. Nous considérons qu'il est nécessaire, parallèlement, d'accroître le niveau d'autonomisation dans le domaine de la protection des données, en renforçant le contrôle des utilisateurs sur leurs propres données à caractère personnel. Les concepteurs et les magasins d'applis devraient s'attacher à améliorer la transparence dans l'intérêt des utilisateurs. Il conviendrait que les utilisateurs soient mieux informés au sujet du traitement de leurs données et que leur soit offerte, en temps utile et de manière effective, la possibilité de donner/retirer leur consentement au traitement ou de s'y opposer, le cas échéant. Un moyen particulièrement efficace de renforcer le contrôle de l'utilisateur consiste à lui accorder la possibilité de traiter ses données à caractère personnel au niveau strictement local, sans aucun transfert à un prestataire ou fournisseur quel qu'il soit.

63. De ce point de vue, dans un contexte de complexité croissante, nous préconisons également la portabilité des données (ainsi que l'interopérabilité des formats et des technologies), dans la mesure où cette solution favorise la simplification, la transparence et le contrôle par les utilisateurs et fait obstacle à la duplication des données.

Sécuriser les données à caractère personnel et renforcer les exigences en matière d'ingénierie

64. Le législateur devrait imposer à tous les acteurs l'obligation de garantir la confidentialité, l'intégrité et la disponibilité des données à caractère personnel traitées dans le respect des règles de protection des données, des normes internationales et des bonnes pratiques. Parmi toutes les options possibles en matière de sécurité de l'information, la gestion continue des risques doit être la pierre angulaire de toute activité de sécurité.

65. Il est indispensable que les principes de *respect de la vie privée par défaut* et de *respect de la vie privée dès la conception*, combinés avec un effort systématique d'ingénierie de la vie privée, soient appliqués dans l'ensemble de l'écosystème de la santé mobile. Le législateur devrait encourager l'adoption d'outils destinés à la conception innovante d'applications et de services respectueux de la vie privée (bibliothèques, modèles de conception, snippets, algorithmes, méthodes et pratiques).

Garanties concernant l'utilisation des mégadonnées en santé mobile

66. Les mégadonnées sont porteuses d'améliorations dans le secteur public et privé de la santé, mais elles risquent aussi de remettre en cause le droit à la protection des données, notamment par la pratique à grande échelle de l'exploration des données et du profilage. Il

[58] Document de travail du GT «Article 29» du 15 février 2007 (00323/07/FR).
[59] Recommandation n° R (97) 5 du 13 février 1997.

est donc nécessaire que le législateur adopte des dispositions en vertu desquelles l'exploration de données en santé mobile n'est acceptable que dans des circonstances spécifiques et sous réserve que les règles de protection des données soient pleinement respectées.

67. Eu égard au fait qu'il est très difficile de parvenir à une véritable anonymisation des données et que les données pseudonymes demeurent des données à caractère personnel, tout traitement de gros volumes de données à des fins d'analyse doit être soumis à des garanties strictes de protection des données. Il conviendrait en outre que les personnes autorisées à accéder à ces données, ainsi que les modalités de cet accès, soient clairement définies.

68. Le rapprochement de données en vue de l'établissement de profils peut, dans certains cas, et s'il est appliqué correctement (p. ex. médecine personnalisée), s'avérer extrêmement bénéfique pour l'individu, mais il soulève aussi de sérieuses inquiétudes en matière de protection des données, en particulier s'il conduit à prendre d'autres types de décisions susceptibles d'affecter des personnes (une compagnie d'assurances pourrait, par exemple, décider de ne pas assurer quelqu'un si elle a accès au profil médical d'une personne indiquant que celle-ci a une forte probabilité de développer un cancer)[60]. Par conséquent, a fortiori lorsqu'il ne répond pas simplement à des finalités de recherche, dans le cadre d'une séparation stricte des fonctions, mais vise également à l'individualisation et au traitement différencié des personnes concernées, le profilage ne devrait être possible que dans des circonstances bien précises, sur une base juridique ad hoc et/ou avec le consentement exprès de la personne concernée, et à condition de se conformer à des exigences de protection des données strictes (comme celles prévues, notamment, à l'article 15 de la directive et à l'article 20 de la proposition de RGPD). En outre, la faculté dont dispose la personne concernée d'exercer à tout moment son droit d'opposition au traitement des données constituera une garantie supplémentaire.

IV. CONCLUSIONS

69. La santé mobile ouvre un monde de possibilités nouvelles, en termes d'amélioration de la qualité et de la réactivité des services de santé, de progrès dans la prévention des maladies, de diminution des coûts de santé pour les systèmes de protection sociale et d'élargissement des perspectives pour les entreprises. Toutefois, si l'on veut que les domaines que nous venons de citer puissent tous profiter pleinement de ces développements, il faut que chacun assume les responsabilités qui découlent de ces nouvelles opportunités.

70. Nous attirons l'attention, en particulier, sur la responsabilité à l'égard des individus et sur la nécessité de préserver leur dignité et leurs droits au respect de la vie privée et à l'autodétermination. Dans un contexte de mutations économiques rapides et d'interactions dynamiques entre différents opérateurs publics et privés, il importe que ces principes fondamentaux ne soient pas oubliés et que des profits privés ne se traduisent pas par un coût pour la société.

---

[60] Voir avis du groupe de travail «Article 29» du 2 avril 2013 sur la limitation de la finalité (*Opinion 03/2013 on purpose limitation*), disponible à l'adresse http://idpc.gov.mt/dbfile.aspx/Opinion3_2013.pdf: *«En particulier, un algorithme peut détecter une corrélation et en tirer une inférence statistique qui, utilisée pour motiver une décision de commercialisation ou autre, est déloyale et discriminatoire. Cela risque de perpétuer les préjugés et les stéréotypes existants et d'aggraver les problèmes d'exclusion et de stratification sociales»* .

71. À cet égard, les principes et les règles de protection des données fournissent des orientations dans un secteur qui échappe encore dans une large mesure à la réglementation. S'ils sont dûment appliqués, ils renforceront la sécurité juridique et la confiance dans la santé mobile, contribuant ainsi à son plein développement.

Fait à Bruxelles, le 21 mai 2015.

(signature)

Giovanni BUTTARELLI
Contrôleur européen de la protection des données