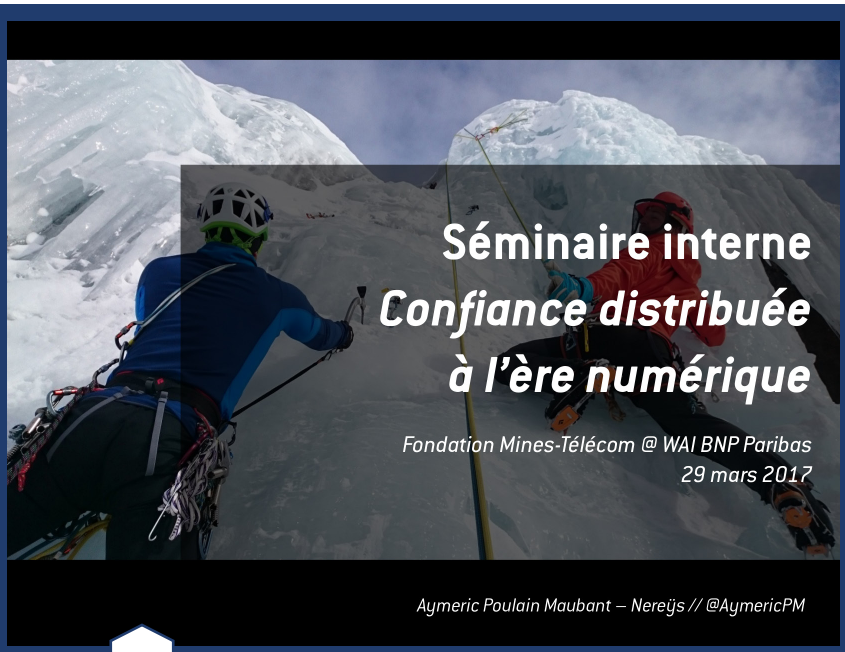
Confiance distribuée

[Compte-rendu du séminaire du 29 mars 2017]

Un séminaire interne de la Fondation Mines-Télécom

La **Fondation Mines-Télécom** est la fondation de l'**Institut Mines-Télécom** pour la formation, la recherche, l'innovation et la prospective. Dans le cadre de son programme innovation, elle publie chaque année un Cahier de veille qui est la synthèse d'études menées conjointement par des enseignants-chercheurs de l'Institut Mines-Télécom et des experts industriels. Tout à la fois complet et concis, le cahier de veille propose un état de l'art technologique, et une analyse tant du marché que des aspects économiques, sociologiques, juridiques et éthiques, en mettant l'accent sur les points les plus cruciaux. Il se conclut sur des perspectives qui sont autant de pistes possibles de travail en commun entre les partenaires de la Fondation Mines-Télécom et les équipes de l'Institut Mines-Télécom.

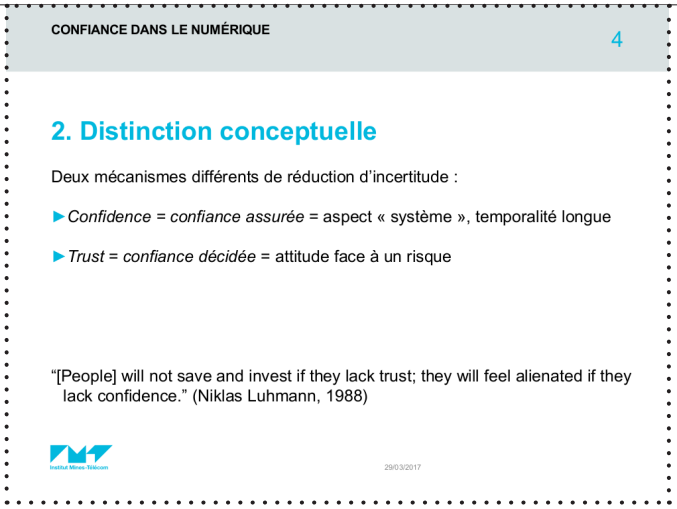
Un **séminaire interne** a lieu en mars pendant la rédaction du cahier. D'une durée d'une demi-journée, il réunit autour de deux tables-rondes des enseignants-chercheurs des écoles de l'Institut et des experts des partenaires. Le séminaire permet de creuser certains axes du *position paper* initial pour intégrer dans le cahier des contributions coproduites, récentes et nouvelles. Le présent document en propose un compte-rendu à partir des textes de préparation et du verbatim du séminaire.



Après quelques mots d'accueil de la Fondation Télécom et de BNP Paribas (ci-dessous, **Xavier Terrasse**, trésorier de la Fondation Mines-Télécom et responsable du schéma directeur IT Groupe 2020 à BNP Paribas) qui nous reçoit dans ses locaux du WAI, **Aymeric Poulain Maubant** coordinateur et rédacteur du cahier de veille sur la Confiance, à paraître en juin 2017, présente l'organisation de la matinée en deux tables-rondes.

La première table-ronde permet de préciser la notion de confiance, à la fois du point de vue des chercheurs, et du point de vue des institutionnels et des entreprises qui la mettent en œuvre. La seconde table-ronde développe le sujet de la Confiance dans le domaine de la santé, un des cas qui sera discuté dans le cahier de veille. Ce compte-rendu suppose une connaissance minimale de la blockchain dont il sera amplement question dans le cahier.

Les présentations des intervenant.e.s sont publiées sur le site web de la Fondation Mines-Télécom. Ce compte-rendu fait référence à certains des transparents.



La confiance dans le numérique, de quoi parlons-nous?

Armen Khatchatourov ouvre le séminaire en posant d'emblée la question du sens des mots : *« On nous dit qu'il faut rétablir la confiance. Qu'est-ce que cela signifie au fond ? Y aurait-il un mécanisme, un indicateur, qui aurait été perdu avec le numérique ? »*. Pas tant que cela, finalement, estime-t-il. Quand on étudie le concept de la confiance, il y a toute son histoire à prendre en compte. Il y a des époques dans le développement de ce concept, et un des aspects fondamentaux à bien avoir en tête, c'est que *la confiance n'est pas une chose homogène*.

Il faut pour commencer faire la distinction entre ce que les anglophones savent séparer par deux mots différents, et pas les francophones. Il y a d'un côté *confidence*, et de l'autre *trust*. Nous dirons en français, «confiance assurée» (CA) pour la notion de *confidence*, et «confiance décidée» (CD) pour celle de *trust*. Cette distinction conceptuelle est proposée par [Niklas Luhmann, 1988]. Elle met en lumière l'existence de deux mécanismes simultanés, qui sont des mécanismes de réduction de l'incertitude.

Prenons un exemple. Je me lève chaque matin en faisant confiance à la monnaie. J'ai confiance dans le système monétaire qui ne va pas s'écrouler du jour au lendemain. C'est une confiance de temporalité longue, relative au système social dans lequel nous vivons. C'est la confiance-*confidence*-assurée. Or ce matin, j'ai décidé de faire un investissement, je vais acheter une voiture. Je suis chez le vendeur et j'écoute ses arguments. J'ai déjà été sensible à la publicité sur le véhicule qui m'intéresse, et plusieurs avis d'amis m'ont poussé à envisager l'achat. J'ai examiné les risques, et je suis décidé, je vais acheter. Le mécanisme en jeu, qui s'est déroulé à une échelle individuelle, est la confiance-*trust*-décidée.

La confiance assurée est très liée au contrat social, nous dit Luhmann. Pour être dans l'actualité, la confiance dans le système politique relève de cette confiance *confidence*. En revanche, accorder sa confiance à tel ou telle candidat.e, c'est de la confiance décidée, du *trust*.

Les deux confiances servent à diminuer l'incertitude, mais de manière différente (slide ❹). Dans le premier, *confidence*, c'est l'aspect système qui prévaut. *« Comment cela s'agence-t-il ? Il y a un équilibre, une conjonction pendant laquelle les deux marchent ensemble. Que se passe-t-il si on perd d'un côté ou de l'autre ? Si la* confidence *diminue, c'est le desarroi social. Il faut tenir les deux ensemble. »*

De *confidence* vers *trust* ?

Un changement s'opère à notre échelle contemporaine. Il y a un déplacement vers plus de *trust*, vers l'individu. À l'extrémité, ce *trust* devient du pur calcul de risque. On peut raisonnablement faire l'hypothèse que le numérique prolonge et accentue cette tendance. SI l'on examine les règlements européens sur les données des personnes, et ceux sur les identités numériques, on voit dans les versions anglophones que le terme *confidence* n'apparaît pas, et il ne s'agit pas là d'un problème de traduction, et bien d'une mise en visibilité de la tendance actuelle.

Position of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC
https://goo.gl/LW64xU

Nous nous retrouvons dans une articulation paradoxale, entre d'une part un individualisme de plus en plus poussé dans nos sociétés, et d'autre part une demande de régulation croissante, qui impose un certain nombre de signes de confiance. Sur quoi la régulation doit-elle alors porter ? Si l'on souhaite «*redonner de la confiance*», de quel aspect, *trust* ou *confidence*, doit-on prendre soin ? Et quel nouvel équilibre va s'établir ? À ces questions encore ouvertes, Armen Khatchatourov ajoute, pour la suite des échanges, qu'il ne faut pas limiter la confiance à deux notions qui lui sont souvent liées : la transparence et la sécurité.

Parmi les scientifiques de l'Institut Mines-Télécom invités au séminaire de la Fondation Mines-Télécom, **Claire Levallois-Barth et Armen Khatchatourov** sont membres de la Chaire Valeurs et politiques des informations personnelles.

Coordonnée par Claire Levallois-Barth, cette chaire réunit une équipe pluridisciplinaire de chercheurs de Télécom ParisTech, Télécom SudParis et Télécom École de Management, et traite des aspects juridiques, techniques, économiques et philosophiques qui concernent la collecte, l'utilisation et le partage des informations personnelles ainsi que leurs conséquenes sociétales. Elle bénéficie du mécénat de l'Imprimerie Nationale, de BNP Paribas, d'Orange, de LVMH, de Dassault Systèmes et d'un partenariat conclu avec la CNIL et la DINSIC. Son deuxième Cahier de chercheurs, à paraître en juin 2017, s'intéresse aux marques et labels de confiance.

Confiance et familiarité – Problèmes et alternatives, Niklas Luhmann 1988 (traduction dans le n°108 de la revue Réseaux : https://goo.gl/lqTuHz)

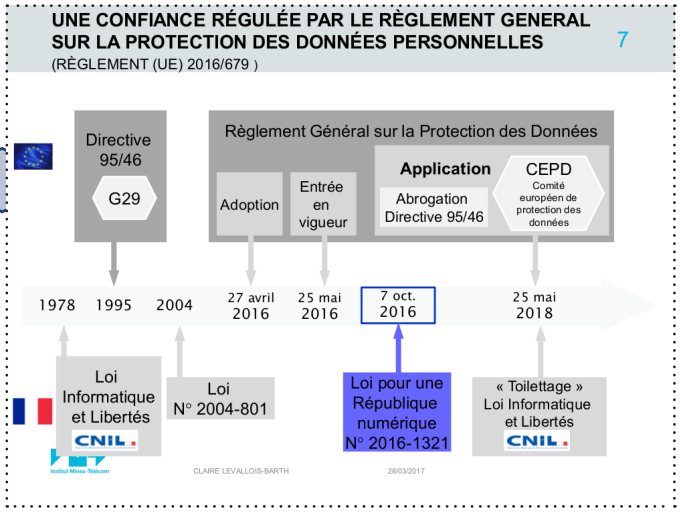
La confiance régulée : l'exemple des labels en matière de protection des données personnelles

Claire Levallois-Barth enchaîne en rappelant qu'à l'origine «*le droit intervenait pour protéger la partie faible. Il intervient aujourd'hui pour établir la confiance du consommateur, et non plus celle de la partie faible. On va donc envoyer des signes de confiance à des acteurs particuliers.*» Ces signes et marques de confiance prennent en particulier la forme de labels. Ces signes de confiance labellisent des caractéristiques très diverses, et s'adressent à des groupes tout aussi divers : mineurs, commerce en ligne, commerce à distance… principalement pour des processus et des produits, et également pour des services, de la formation, de l'audit…

On observe qu'il y a une multitude de labels qui naissent (plus de 90 labels répertoriés par la Chaire Valeurs et politiques des informations personnelles, voir encadré page 2, dont 70 en Europe). Une sorte de «marché de la confiance» se construit. Cette multitude de labels dessert sans doute leurs finalités. Qui connaît bien les labels europrice, les labels CNIL ? Un rapide sondage dans la salle montre qu'il y a des progrès à faire.

Labels délivrés par des entités de différente nature

63% par des entreprises privées
26% par des associations
11% par des entités publiques



La confiance est régulée par le règlement général sur la protection des données personnelles (*General data protection regulation, GDPR*, 2016/679) adopté le 27 avril 2016 par l'Union européenne, règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Ce texte est entré en vigueur le 25 mai 2016 et s'appliquera dès le 25 mai 2018.

Un nouveau principe issu du droit anglo-saxon y est introduit, l'***accountability***, qui a été très mal traduit en *principe de responsabilité* : il s'agit plus précisément d'un *principe d'obligation de rendre des comptes*. C'est là un renversement total de la doctrine antérieure, qui était celle de la déclaration préalable. Celle-ci disparaît, et il faut en revanche être capable à tout moment de démontrer sa *conformité* aux nouvelles obligations. Ce processus activable en permanence «*permet au responsable de traitement de s'assurer et d'être en mesure de démontrer qu'il gère les risques d'atteinte aux données personnelles*» (slide ❽). Ces «*éléments de démonstration*» acquièrent un statut d'éléments constitutifs de la confiance. Ils peuvent par exemple prendre la forme d'une politique de protection des données, d'un code de conduite approuvé (avec des adhérents qui adhèrent effectivement à ce cade) ou encore des mécanismes de certification approuvés. Pour piloter la gouvernance des données personnelles, il est recommandé et parfois obligatoire de désigner une personne ayant une mission d'information, de conseil et de contrôle en interne : le *délégué à la protection des données*. En France ce rôle prendra la suite de celui du correspondant informatique et libertés bien connu. C'est une première étape essentielle pour se préparer à l'arrivée du GDPR.

Une autre nouveauté introduite par le GDPR est la possibilité de passer par des *certifications*, *labels* ou *marques* relatives à la protection des données personnelles. Ces certifications peuvent être délivrées par une autorité de contrôle, comme la CNIL en France, ou par un organisme de certification bénéficiant d'un agrément. Le renforcement de la confiance et de la transparence s'opère à la fois sur la personne concernée (en mode B2C pourrait-on dire) et vis-à-vis des autres responsables de traitements (en mode B2B), de la collecte à la transmission de la donnée, en passant par son utilisation.

«*Quel va être le rôle de l'État dans ce contexte ? Le règlement laisse beaucoup d'options aux CNIL et à la Commission*» note Claire Levallois-Barth qui ajoute que l'on attend encore en mars 2017 les lignes directrices des CNIL qui devaient être publiées fin 2016. Du côté des acteurs privés, les choses sont clairement en train de bouger. Attention cependant : il y a des risques que certains labels ne valent rien du tout.

L'évolution des tiers de confiance et la gouvernance des blockchains

Intervention de Nadia Filali, responsable du Développement des Mandats et des Offres, Caisse des Dépôts

Nadia Filali rappelle que la Caisse des Dépôts est tiers de confiance depuis déjà 201 ans. Certains de ses clients sont également tiers de confiance. Alors qu'on compte aujourd'hui plus de 700 crypto-monnaies différentes dans le monde, construites selon plusieurs protocoles, la Caisse des Dépôts s'est très tôt intéressée à ces mécanismes, et a proposé à plusieurs acteurs d'explorer ensemble ce nouveau monde. Lancé en décembre 2015, Labchain est un laboratoire d'innovation dédié aux architectures de consensus décentralisé, qui est à la fois un *think tank* et un *do tank*. Un des défis de ce groupe est que les acteurs qui s'y réunissent se font confiance et sont concurrents en même temps. Nadia Filali souligne également que la Caisse des Dépôts travaille avec des startups et des développeurs *en France*.

La blockchain a été inventée pour des gens qui ne se faisaient pas nécessairement confiance, et en conséquence tout est transparent. De plus, les blockchains publiques sont fondées sur l'anonymat des participants et aucun régulateur n'est dans la boucle. Cela pose un problème pour les acteurs commerciaux comme les banques, qui sont sujets à des réglementations strictes, qui interviennent dans des contextes régulés et ont l'obligation par la conformité de connaître l'identité des acteurs qui utilisent leurs services. C'est donc sans surprise qu'un des premiers cas étudiés au sein du do tank a été celui de l'identité numérique : cette personne en face de moi est-elle bien celle qu'elle prétend être ?

Désintermédiation et blockchain

Blockchain/bitcoin a trois composantes : un réseau peer-to-peer c'est-à-dire sans intermédiaire, un mécanisme de cryptographie qui apporte confiance et sécurité, un registre distribué. C'est ici l'algorithme qui remplace le tiers de confiance et apporte la confiance aux acteurs. Nadia Filali pose la question de la désintermédiation des tiers de confiance. Il faut travailler sur des garants, qui vont alimenter les données. Cela pose la question de l'évolution de ces tiers de confiance.

La blockchain trouve en effet tout son intérêt en étant appliquée à d'autres projets que les crypto-monnaies, et en particulier en intégrant des données provenant du monde

analogique. On peut parler d'hybridation avec le monde réel. Et celle-ci n'est pas du tout immédiate, car l'immuabilité (le principe exprimant qu'une fois une chose écrite dans une blockchain, elle y est inscrite pour toujours) supposée de la blockchain (nota: ceci sera expliqué / discuté dans le cahier de veille) serait remise en cause si une donnée placée dans la blockchain était ultérieurement changée, ce qui est un des aspects de la vie des données (leur variabilité dans le temps). Un mécanisme dit d'Oracles a cependant été construit pour rendre la blockchain perméable au monde extérieur, malgré les risques encourus pour les capacités d'immuabilité. Ces oracles qui sont des services pouvant entrer des données extérieures dans la blockchain font que la désintermédiation n'est pas complète. Comment leur faire confiance ? Qui plus est, les tiers de confiance sont repositionnés vers des acteurs qui n'avaient pas été considérés comme tels avant.

Gouvernance des blockchains

Le sujet de la gouvernance des blockchains reste donc entier. Dans le cas de blockchain/bitcoin par exemple, il y a l'inventeur initial, les *core developpers* (on peut les identifier, mais s'ils font évoluer le projet dans un autre sens, on ne contrôle plus), les mineurs (qui utilisent divers mécanismes de la théorie des jeux pour s'organiser entre eux). Les protocoles blockchain sont un protocole social, et si on veut vraiment chercher de la confiance, il faut différencier les types d'acteurs en train de se faire confiance. Ce n'est pas la même chose entre institutions d'une part, et entre gouvernants / gouvernés d'autre part (selon les pays ; cf. notamment des cas d'usage pour les cadastres ou les systèmes administratifs). Entre institutions existe un degré de confiance plus élevé a priori, on met alors en place des blockchains de consortium, des blockchains de permission. Il y a les distinctions à établir entre blockchains privées et blockchains publiques, les mécanismes de *proof of work* et ceux de *proof of take*… Se posent les questions de comment répartir les coûts, les autorisations. Comment faire évoluer les rôles et équilibres des uns par rapport aux autres ?

Les individus semblent ne plus avoir confiance dans les systèmes sociaux qui existent. Alors ils envisagent deux solutions : échanger entre eux, ou ne rien faire et «voter» contre. C'est un vrai sujet sur le risque social et sociétal. Comment avoir confiance dans des systèmes où il n'y a personne au milieu (qui pourraient pourtant apporter des solutions sur des enjeux comme la gestion des déchets, la consommation énergétique) ?

Rendre lisible la confiance

Intervention de Didier Louvet, Directeur de la Confiance Numérique chez Le Groupe La Poste

Didier Louvet précise d'emblée, rebondissant sur les échanges précédents à propos du GDPR, qu'il parlera de la confiance numérique vue du particulier plutôt que celle vue du consommateur. Pour lui, la confiance c'est aussi et surtout celle du citoyen, la personne dans le quotidien de son travail, la personne et ses préoccupations de santé.

Un premier exemple est celui du bureau numérique du particulier. Il s'agit de le ré-équiper d'un endroit sécurisé, *bienveillant*, qui n'apporte pas de biais, qui n'a pas de finalité cachée, c'est-à-dire que le gestionnaire de cet espace ne profite pas d'une connaissance de ce qui y est entreposé pour vendre des services en plus. C'est ce que propose Digiposte : un coffre-fort numérique dédié au particulier, conçu pour rassembler, sécuriser, maîtriser son patrimoine numérique. C'est la mise à disposition d'un « *espace de confiance sécurisé, personnel, bienveillant* ». Les personnes y déposent leurs documents d'un simple glisser-déposer de leur ordinateur. Elles peuvent confier leurs logins et mots de passe pour que leur coffre aille récupérer à leur place et en leur nom des informations telles que leurs documents fiscaux ou des données d'e-commerce. Il y a du reste un effet spectaculaire d'utilisation de cet espace pour le bulletin de salaire numérique, en raison de la récente loi El Khomri (effet de l'aspect opt-out des bulletins de paie dématérialisés). Digiposte est par ailleurs en train de s'équiper d'un module hébergement des données de santé.

L'idée pour les particuliers est d'avoir sa donnée personnelle dans son coffre, de la récupérer et aussi / surtout de la réutiliser. C'est ce dernier point qui est intéressant. Réutiliser la donnée pour la comprendre, pour l'analyser, pour agir et réagir. Dans un monde transactionnel et relationnel, la renvoyer à d'autres personnes, réalimenter son écosystème… La question se pose de comment fluidifier cette (ré)utilisation de la donnée, et est-ce que pouvoir fluidifier l'utilisation contrôlée de ses données personnelles contribue à augmenter la confiance.

Le groupe La Poste s'appuie sur son ADN de confiance, construit sur deux actifs pour lesquels il est reconnu : la bienveillance et la transparence sur la finalité des choses. Dès que la personne a un doute sur la finalité des choses, elle perd en confiance. Or, moins il y a de confiance, moins il y a d'usages.

Digiposte rend donc des services aux particuliers et exclusivement pour eux.

Transitivité de la confiance

La question de la transitivité de la confiance se pose ensuite. La Poste est un acteur de confiance, qui n'apporte pas de biais, qui est agnostique. Elle apporte en revanche la possibilité de confirmer, en ne présentant que le minimum d'informations requises (par ex. « *Oui, untel est en CDI* » et non pas « *Oui, voici le contrat de travail de untel dans lequel vous pouvez voir vous-même quel est le type de son contrat* » ou pire « *Oui, voici le bulletin de salaire de untel dans lequel vous pouvez voir qu'il s'agit bien d'un CDI* »), des informations souhaitées par des tiers.

Le rôle de la Poste est de se positionner dans la transitivité de la confiance. Plusieurs cas d'usage sont déclinés par Didier Louvet (et d'autres l'ont été plus tôt, comme les informations demandées à l'accueil de l'hôtel juste pour prouver qui vous êtes, ou que vous serez solvable demain matin), comme le bulletin de salaire qui contient trop d'informations alors qu'il s'agit juste de prouver à son propriétaire qu'on pourra le payer. Connaissant par exemple la bonne réputation de la personne sur un service comme Amazon, croisée avec la connaissance que vous êtes un bon conducteur grâce aux documents d'assurance et celle que vous possédez bien votre permis, le système pourrait apporter à un loueur de voitures les éléments de satisfaction nécessaires sans être détaillés (pas de nom, pas de provenance par exemple) pour qu'il accepte de vous louer un véhicule. On établit là une sorte de confiance pré-créée, construite dans un domaine X qui peut s'appliquer, se transférer dans un domaine Y. Techniquement, ceci passe par une analyse des documents écrits, et l'obligation de pouvoir expliquer ce qui a été analysé et compris.

Management des permissions

Le travail de la donnée personnelle nécessite un consentement éclairé. La question de l'ingénierie du management des permissions et du consentement des particuliers est un chantier important : guider le particulier pour savoir comment accepter les requêtes des tiers sur ses informations, comment vérifier qui demande, comment transmettre ces informations. Une IA pourrait gérer cela en partie.

Comment s'assurer que le particulier a bien compris ce qu'il autorise… Il y a là une normalisation à travailler. L'enjeu est essentiel : c'est celui de rendre la confiance lisible et compréhensible.

Échanges

De nombreux échanges ont suivi cette première table-ronde, et nous en listons ici les principales questions, certaines toujours ouvertes. Une première remarque concernait l'enregistrement initial au service Digiposte qui n'est pour l'instant pas certifié, il n'est pas en face à face. La réponse est que tout le processus est repris actuellement depuis zéro. La convergence numérique se fera courant 2017. L'idée est de mettre un niveau de sécurité au moment où les gens en ont besoin, et pas nécessairement dès le début de la connexion. Le niveau de confiance est adapté à la sensibilité des données. Il y a un équilibre à établir entre sécurité et niveau d'usages. Noter que ces curseurs vont devoir évoluer avec le temps. Dans le cahier de veille nous pourrions mettre des points de vigilance sur les sujets de ce type qui pourraient bien devoir évoluer avec le temps et les habitudes sociales. Nous en avions parlé au sujet des IA dans le cahier de veille précédent.

Il faut reconnaître que le fait de devoir se présenter physiquement pour s'identifier une première fois est paradoxal dans un monde numérique. Le risque zéro n'existe pas pour autant. Ceci dit, les personnes malveillantes seront détectées quand un faisceau d'informations ne sera plus crédible.

Suit un court échange sur les projets aux USA autour de la gestion des permissions de santé (UMA, *User Managed Access*, à développer dans le cahier).

La discussion se poursuit sur les équilibres entre sécurité et liberté, avec des anecdotes sur des cas de fausse usurpation d'identité lors de passages de frontières. On rappelle à ce propos la norme de sécurité européenne eIDAS, avec plusieurs niveaux de sécurité, chaque niveau de garantie correspondant à un niveau d'authentification qui permet d'effectuer certains types de procédures : *faible* qui permet de réduire le risque d'usurpation, *substantiel* qui le réduit beaucoup plus, et *élevé* qui doit l'empêcher.

La question de l'unicité de la personne est posée. On a le droit d'avoir plusieurs passeports, tout en sachant qu'il y a d'autres unicités à prendre en compte, nous rappelle Bruno Salgues. S'ensuivent des échanges sur *les questions relatives à l'identité numérique*, à partir de travaux antérieurs des chercheurs de la première table-ronde, que nous pourrons reprendre dans le cahier. À différentes identités possibles doit correspondre la possibilité de faire de la divulgation sélective de ses informations personnelles.

Les participants enchaînent sur la question des jeunes qui n'auraient pas conscience des traces qu'ils laissent : comment les former ? Nous parlons ici de la relation à ce qu'on est, ce que l'on montre, ce que l'on démontre. Il est possible de répondre par «l'éducation par l'exemple». De manière générale, mettre pédagogiquement les personnes devant leurs responsabilités. Nous ferons le lien dans le cahier entre la confiance et la e-réputation, qui n'est pas la même en fonction de l'expérience et de l'âge. Pour Armen Khatchatourov, un des auteurs du cahier Identités numériques de la chaire Valeurs et politiques des informations personnelles, il faut garder en tête que différentes générations co-existent (*«l'être humain n'a pas peur avant ses 7 ans»*), et différents pays. Tout le monde ne ressent pas les choses de la même manière. On peut comparer à cet effet utilement deux systèmes de sécurité d'identification totalement différents : l'Allemagne et l'Estonie. Comparables en niveau de *trust*, ils ne le sont pas du point de vue de la construction sociale.

Ces premiers échanges se terminent sur une discussion sur l'opposition entre local et global : il y a peut-être trop de régulateurs locaux, alors que nous sommes dans une économie globale. Comment équilibrer les règlements nationaux versus les règlements internationaux ? Claire Levallois-Barth rappelle qu'on parle le plus souvent de rapprochement et non pas d'harmonisation totale. Sur ces questions d'équilibres internationaux, il faut étudier les mécanismes des pays qui exportent leurs normes vers les autres, ainsi que les normes ISO. Le livre blanc de Bureau Veritas sur la protection des données personnelles, paru en novembre 2016, est cité.

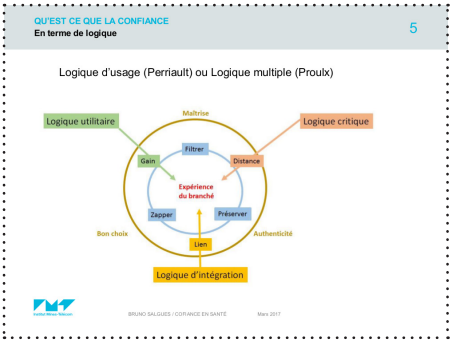
Santé & Confiance

Qu'est-ce que la confiance dans le domaine de la santé ?

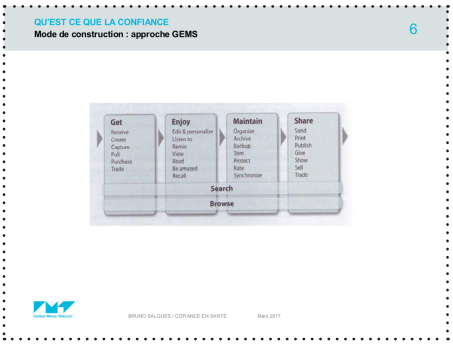
Bruno Salgues, enseignant-chercheur à Mines Saint-Étienne, et auteur de *Industrialisation de la santé : Identité, biopouvoir et confiance* https://goo.gl/s4RUot

« Qui est le tiers de confiance ? Car quand vous mourrez, vous devez savoir. » C'est en ces termes que **Bruno Salgues** ouvre la deuxième table-ronde, consacrée à un focus sur la Confiance dans le domaine de la santé . *« Il y a des fois où on va dans des lieux de santé où on n'a pas confiance, mais on n'a pas le choix car on n'a pas le temps de choisir. »*

Un des problèmes fondamentaux, traité dans l'ouvrage récent de Bruno Salgues, est l'industrialisation de la santé : comment faire la même chose en faisant beaucoup moins cher. En quelques transparents, le chercheur fait le parallèle entre les mécanismes de diffusion de l'innovation selon Everett Rogers, et l'établissement de la confiance (envers les thérapies, les médecins, les médicaments, les dispositifs médicaux, les lieux). Comment expérimenter l'opération que vous aurez dans quelques temps ? Par la réalité virtuelle, par l'accès à des patients experts qui ont subi la dite opération dans le passé ?



La confiance se construit autour d'une certaine logique (slide ❺). *«Derrière, il y a une logique de création de la confiance»*. Cela passe par les institutions. *« En France par exemple, nous avons confiance dans la CPAM. »*



Un autre paradigme proposé en 2007, l'approche GEMS, qui se fonde sur la dynamique des états de fébrilité des communautés, peut servir à expliquer la construction de la confiance en santé. *« Par exemple pour enjoy, c'est le point où on va acquérir la confiance. »* *Get*, c'est le moment où l'on récupère les paramètres (x,y,z,t) en sortie d'IRM, les logiciels de construction d'image n'étant pas toujours les mêmes pour autant. *Maintain*, c'est comment je stocke tout cela et où je le retrouve, sachant que les dates de conservation sont bien trop faibles, la durée de la vie augmente et cela n'a pas été pris en compte. *Share* : je partage avec qui et comment.

Bruno Salgues poursuit avec d'autres cadres conceptuels qui apportent tous de nouveaux éléments pour comprendre comment se

constitue la Confiance, y compris dans le cas général (pas seulement dans le domaine de la santé). Le slide ❾ signale notamment les travaux d'Anne-Marie Gagné (*La confiance et le soupçon – Faire des relations publiques à l'ère de l'entreprise « responsable »*, 2011). S'y trouvent déclinées quatre formes de confiance. La confiance attitudinale, une ouverture d'esprit ; la confiance rationnelle, qui est celle de la communication ; la confiance organisationnelle, celle de la structure de l'organisation, ses normes et ses valeurs ; et enfin une composante stratégique, celle des respects des engagements et des promesses, la cohérence des discours et des actes.

L'utilisation de la blockchain en milieu hospitalier

Chloe Giraut, Research Analyst chez Stratumn

La blockchain repose avant tout sur un rapport de confiance entre ses utilisateurs. Or, la confiance est la base de la relation médicale : secret médical, accès aux soins, consentement, partage des données, suivi du traitement… **Chloe Giraut** présente plusieurs prototypes et projets d'utilisation de la blockchain dans un milieu hospitalier. Ils seront étudiés en détail dans le cahier de veille.

Stratumn a ainsi développé à l'hôpital Hôtel-Dieu (labo épidémiologie) DocChain, un projet pilote de consentement numérique aux protocoles d'essais cliniques avec horodatage. Le recueil du consentement des patients dans le cadre d'un essai clinique est une procédure encadrée et réglementée. Le patient exerce son consentement au protocole proposé en y apposant sa signature. Les amendements aux protocoles sont fréquents et chaque nouvelle itération nécessite un nouveau consentement du patient. Utiliser une blockchain augmente la transparence et la reproductibilité des essais cliniques : *audit trail* de l'essai, du protocole initial (qui ne pourra donc être modifié en chemin), des consentements des patients (plus d'inventions de faux patients ou de retraits des patients gênants).

Les autres cas présentés concernent l'échange de données médicales électroniques, la traçabilité et le suivi du matériel hospitalier et des factures, la garantie de l'intégrité des données et médicaments contre la contrefaçon, l'accès au dossier médical partagé, l'amélioration de la confidentialité des données patients…

Tous ces prototypes et projets doivent prendre en compte les réglementations établies par de nombreux organismes : l'Agence européenne des médicaments, l'Agence Nationale de Sécurité des Médicaments (ancienne Afsaaps), la Food and Drug Administration, la CNIL et le GDPR. 30% de startups dans le domaine de la santé numérique, où la législation est extrêmement lourde et handicapante. Concernant le GDPR, le fait de devoir justifier a posteriori va changer beaucoup de choses, car on quitte le régime de l'autorisation stricte.

Un opérateur télécom dans la santé

Emmanuelle Pierga, directrice de la communication chez Orange Healthcare

Orange Healthcare a été créée en 2007 pour trouver des relais de croissance. L'entreprise revêt de nombreuses activités : développement du parcours de soins (transformation digitale de l'hôpital) slide ❽ ; transformation digitale de l'industrie pharmaceutique, qui ne se développe pas encore assez, d'un point de vue digital (tout ce qui accompagne le médicament, là où l'industrie va aller au-delà de la boîte de médicament) ; dispositifs médicaux qui communiquent (suivi constant par le médecin) slide ❾; mutuelles et assurances (maintien à domicile) ; institutions de santé publique (ARS…) qui sont à l'origine du développement de la transformation digitale de la santé ; et tout ce qui est lié aux startups (clients et partenaires)…

Emmanuelle Pierga rappelle qu'une donnée de santé n'est pas n'importe quelle donnée. On parle ici de donnée de santé dans le cadre de l'hôpital, dans le cadre d'un protocole médical, et pas de données provenant par exemple des bracelets de suivi de bien-être. «*Une donnée de santé est une donnée médicale et/ou relative aux déterminants généraux de la santé se rapportant à l'état de santé d'une personne concernée qui comporte des informations sur sa santé physique ou mentale passée, présente ou future, y compris des informations relatives à son enregistrement pour la prestation de services de santé.*»

La première confiance numérique qu'on établit c'est une réponse technique, concernant la sécurité des données. Le pôle cyberdéfense d'Orange est ici essentiel pour la garantir. Les cyberattaques sont un risque important pour les hôpitaux.

Orange Healthcare va être conforme à la certification GDPR 2018, évolution de leur agrément actuel d'hébergeurs de donnés à caractère personnel. En 2010, Orange était devenu le 1er opérateur de télécommunications à obtenir l'agrément d'hébergeur de données de santé à caractère personnel. Il y a également des travaux en cours pour l'extension aux réglementations Nord Américaines (HIPAA/HiTrust…)

Échanges libres

L'ambulatoire peut être tout à fait sécurisé grâce à sa numérisation. Le numérique est nécessaire ou inévitable. La médecine moderne ne peut pas encore se déployer, s'industrialiser, mais de toute manière les pratiques vont se digitaliser. Le secteur bancaire est beaucoup plus agile que le secteur de la santé, placé dans sa législation contrainte qui l'empêche de se développer.

Les jeunes médecins ne vont plus se poser de questions, ne vont pas pouvoir vérifier si les données de leur téléphone mobile sont cryptées avant d'envoyer une demande de diagnostic en urgence. Le projet «mes infos santé» de la FING est cité. Il fait notamment référence à une pratique danoise où les personnes ont toutes leurs informations de santé dans leur téléphone.

La réglementation ne permettra pas à des tiers de confiance de stocker des données de santé sur une durée longue. Donc il faudra le faire «chez soi». Ce qui pose de nouveaux problèmes : le réseau vers chez moi est-il accessible à tout instant (lien télécom, réseau énergétique…)

Il faut arrêter d'avoir peur. Ce qu'on stocke sur la blockchain, c'est un historique de preuves de données, ce ne sont pas les données médicales elles-même. Ce qui ouvre la voie au carnet de santé digital.

La bienveillance est centrale dans le domaine de la santé. Comment la digitaliser : c'est la question. «*On confie ce que l'on possède de plus précieux au monde, sa vie*». Des données vitales liées à l'intimité de l'individu, c'est pour cela que cela coince tant.

Avec le Brexit, que va devenir l'Agence européenne des médicament, localisée à Londres ? Que vont devenir les directives européennes de la santé rédigées en anglais, qui perd son statut de langue officielle ?

Comment certifier / garantir des objets physiques (médicaments, instruments…) une fois sortis de leur packaging ?

Le mot de la fin : l'idée de la blockchain n'est pas de faire disparaître les tiers de confiance, mais de redonner une valeur, une force, à ces tiers de confiance grâce à la technologie.