Le contrôle systémique des identités numériques

José REMY[1]

[1]openOSI – Sté civile d'études et de recherches

jose.remy@openosi.org

Résumé – Cet article propose un modèle pour la protection de la vie privé dans la gestion des identités numériques. Il propose une synthèse des perspectives concurrentes de l'individu et de l'Etat. Il s'inspire de la technologie des Métasystèmes d'identité et des lois sur l'identité. Le modèle proposé est confronté à des études de cas et à la théorie du contrôle social. Cette confrontation enrichi le cadre théorique du contrôle en définissant la notion de contrôle systémique et les pré-requis de sa réalisation. Il est montré qu'un contrôle social numérique centré sur le citoyen est possible et acceptable dans les sociétés démocratiques. Il est même possible de restituer sa souveraineté au sujet numérique. Elle inclut le plein contrôle de ses identités numériques tout en permettant les fonctions régaliennes de l'Etat. L'innovation technologique réside dans l'extension à la sphère civile du modèle marchand qui sous-tend les technologies de l'information actuelles. Il s'agit de formaliser les procédures publiques au dessus des procédures marchandes.

Abstract – This article is a proposal of a framework enhancing privacy within digital identity management. This is a mediated approach between public policies enforcing efficiency, error control and individual sovereignty. It expands from the concept of identity metasystem and the laws of identity. Use cases and social control theory are brought face to face. This allows enriching control framework with concept of systemic control. Providing few prerequisite it is shown that digital social control is possible and acceptable in democratic countries. The condition is to empower the citizen; giving him backs his sovereignty, as digital subject; allowing full control over own digital identities; allowing enforcement of law by public authorities. The enabling technology is an enhancement of the business model underlying information technologies to meet privacy regulation. That is developing "public services" over "business services".

1. Position du problème

Le citoyen est à la fois un émetteur de données privées et un sujet de connaissance (renseignement). La révolution numérique modifie profondément la notion d'identité. Elle définit une dimension additionnelle qui est celle de l'identité virtuelle. Sa forme est l'identité numérique. Plus précisément c'est une multiplicité d'identités numériques. Elles correspondent à la singularité du corps et aux différents rôles sociaux de la personne. Le corps et chacun de ces rôles fait l'objet d'un contrôle social. Pour le corps c'est celui de la médecine. Pour les rôles sociaux il s'agit de celui de l'Etat, notamment pour le maintient de l'ordre; mais il s'agit aussi de multiples acteurs privés comme les employeurs, les assureurs ou les banques. Michel Foucault a évoqué la notion de contrôle biopolitique sur les corps[1]. Deleuze a évoqué celle de société de contrôle pour l'identité codée[2]. Ces approches expriment une inquiétude sur les libertés individuelles et publiques. A l'opposé, les instances du contrôle social procèdent par une démarche empirique. Pour améliorer leur efficacité, elles utilisent les nouvelles technologies de l'information. Mais cet usage produit des erreurs. Elles sont parfois dans une telle proportion que l'efficacité est remise en cause. Le problème qui se pose aux sociétés démocratiques et laïques est de maitriser l'usage de ces technologies qui ont le potentiel d'améliorer l'efficacité du contrôle social. Mais elles ont été principalement développées par le secteur marchand ; qui plus est dans des pays où par tradition le rôle de l'Etat est minimisé. Par exemple, il n'existe pas en anglais informatique de terme pour décrire un processus administratif. C'est le terme générique de « business process » (processus marchand) qui est employé. Aux Etats-Unis la notion de protection de la vie privée s'applique essentiellement à la protection des informations financières[3], et plus récemment aux données médicales[4]. En conséquence, il n'existe tout simplement pas de cadre théorique informatique pour penser le rôle de l'Etat et sa relation aux citoyens. Il existe encore moins un cadre méthodologique correspondant, et aucune technologie spécifique. Les pays de tradition romano-germanique en sont réduits à penser leurs systèmes de traitement de l'information en termes de processus marchands. Cette situation ne permet pas la maîtrise nécessaire des technologies considérées. Elle entrave la prise de conscience indispensable.

2. Le contrôle systémique

2.1 Les prémisses

Le contrôle systémique propose un cadre théorique pour concevoir des systèmes de contrôle social qui soient conformes aux règles de droit d'un Etat démocratique de type européen. Il s'agit principalement d'une théorie formelle. Mais ses hypothèses sont confrontées à l'évaluation de trois cas. Le dossier médical partagé en France, le fichier de police français des infractions constatées (STIC), et la vidéosurveillance au Royaume-Uni. Dans chacun de ces cas des dysfonctionnements majeurs révèlent des problèmes de conception. L'évolution des outils informatiques a dépassée l'évolution des méthodes de contrôle. Comme dans le domaine de l'environnement nous sommes dans des dynamiques, dites systémiques, qui ne sont plus maitrisées. Alors, les modalités du contrôle passent à la dimension sensorielle. C'est la peur au niveau individuel, et c'est la communication au niveau politique. Il est notable que le traitement de l'information financière reste globalement sous contrôle, du moins en ce qui concerne la monnaie. C'est en partie lié aux moyens des banques. Mais c'est aussi lié à une priorité, qui s'est imposée, de l'économique sur le politique. Il s'est développé une régulation à deux vitesses.

C'est le développement d'Internet qui change la donne, avec l'avènement des réseaux sociaux. Le besoin de partage des identités numériques se développe, tout en exigeant une certaine étanchéité entre les rôles (persona) représentés. Ces nouveaux systèmes d'identification, les Métasystèmes d'identité, sont les prémisses du contrôle systémique. Néanmoins ils restent basés sur les spécificités de la tradition anglo-saxonne, c'est à dire l'approche contractuelle et le communautarisme. La notion de contrôle systémique réintroduit des déterminations liées à l'approche romano-germanique de l'état de droit. L'ajout d'un niveau conceptuel doit permettre le lien avec la théorie politique. La nécessité du rôle de l'Etat est réintroduite, accompagnée d'une contrainte de formalisme à exprimer avec les logiques de description[5] et les langages de politiques[6] de confiance. Ce formalisme deviendra probablement la forme dominante du droit positif.

Là où le livre blanc français sur la défense[7] voit les risques associés au développement d'Internet, cet "écosystème" social et technique fait aussi émerger des capacités d'autocontrôle.

2.2 Les principes

Le contrôle systémique est un concept qui fait partie des sciences systémiques et cybernétiques. Il repose sur plusieurs principes. **Le premier est la nécessité de contrôler les systèmes de contrôle**. Il s'agit de l'application de l'idée de Kant selon laquelle «*chacun, parmi eux (une société de plusieurs personnes), abusera toujours de sa liberté si personne n'exerce sur lui un contrôle d'après les lois* »[8]. **Le second est le principe de subsidiarité**. Il est notamment issu du droit canon de l'église dont cette partie a été initialement formulée par Saint Thomas d'Aquin (*subsidium affere*). L'échelon le plus bas n'abandonne à l'échelon supérieur que ce qui est strictement nécessaire. C'est devenu le principe fondateur de l'Union Européenne depuis le traité de Maastricht[9]. La portée de la subsidiarité a été progressivement élargie. Il s'est d'abord agit de considérer que la personne devient la "substance première" face au corps politique parfait qu'était la cité. Puis ces "centres autonomes" deviennent un modèle politique qui étend cette structure à une perspective de nature fédéraliste ou d'Etat décentralisé. Les fonctions publiques ne sont pas nécessairement réalisées par l'Etat. Plus généralement il y a une acceptation de la loi du marché et du rôle de l'individu. Il est plus ou moins rationnel, mais «l'individualisme méthodologique» s'affirme face aux logiques collectives. **Le troisième principe est celui de la reconnaissance d'une structure systémique**. Elle implique une conception et une technologie du contrôle qui se développent sur l'ensemble des échelles sociales issues de la subsidiarité. C'est à dire que la régulation s'étend du contrôle de l'Etat régalien jusqu'à l'individu. **Le quatrième principe est celui d'évaluation**. Il permet la mesure de l'efficacité du contrôle. C'est à dire qu'il permet la correction des erreurs et l'arrêt, au service du pilotage. Or il y a toujours des erreurs dans un système complexe ; et il y a toujours une difficulté, voir une impossibilité de l'arrêt d'un système autonome.

L'application de ces principes permet au contrôle social d'être plus efficace. Mais en contre partie la visibilité accrue sur les erreurs transforme la perception de la réalité. Elle apparaît comme la juxtaposition de systèmes complexes. Leur régulation implique la tolérance à l'erreur. C'est dans le double sens du maintient du contrôle et de l'acceptation d'erreurs non corrigées. En d'autres termes c'est une gestion d'équilibres. Il s'agit d'une vision systémique de l'Etat. Elle considère les politiques publiques comme des procédures dont l'efficacité est à améliorer[10]. La transparence sur les comportements des individus révèle un désordre apparent qui fonde l'ordre à l'échelle supérieure. Cette perspective des systèmes complexes remplace les approches réductionnistes actuelles.

2.3 La technologie

C'est dans le domaine de l'informatique et d'Internet que se développent les premiers contrôles systémiques. Ils n'ont pas été théorisés en tant que tels. Mais ils sont générés par leur environnement technique spécifique. C'est à dire celui de la cybernétique. C'est un modèle qui implique des conventions pour permettre l'existence de «cérémonies» entre humains et systèmes techniques[11]. Le cœur de ces cérémonies est la négociation des termes d'un échange. Ils concernent notamment la place de marché qu'est devenue Internet. La notion de cérémonie est intimement liée à celle de confiance. Elle repose pratiquement sur des «protocoles de sécurité des réseaux». Il a été constaté que les mieux conçus pouvaient échouer dans leurs fonctions de sécurité lorsque l'interaction avec les «composantes» humaines n'était pas prise en compte. Ce n'est que récemment que les méthodes de conception informatique disposent des premiers standards de travail permettant d'intégrer cette notion de cérémonie. Il s'agit de «BPEL4People[12]» et de «WS-HumanTask[13]». Leur fondement est de considérer l'humain comme «un citoyen de première classe» face aux systèmes techniques. Cette notion d'intégration humaine est une des sept lois d'identités définies par Kim Cameron[14].

Ces lois vont définir la notion de MétaSystème d'identité. Ce sont : la loi du contrôle par l'usager et de son assentiment ; la loi de divulgation minimale pour un usage défini ; la loi des parties prenantes nécessaires et justifiées ; la loi des identités dédiées (personas, identifiant exclusif) ; la loi du pluralisme des opérateurs et des technologies ; la loi de l'intégration humaine (sus citée) ; la loi de la cohérence de présentation selon les contextes. Ces lois vont s'appliquer à l'ensemble des relations d'identification entre différentes entités : Une partie confiante (relying party), c'est à dire celle qui a besoin de confiance à propos d'informations reçues ; un fournisseur d'identité numérique ; un entrepôt d'identités ; le sujet numérique, c'est à dire la personne concernée par l'échange ; les requêtes d'identité (claims), c'est à dire des assertions à évaluer concernant le sujet numérique. Ces assertions sont échangées entre une partie confiante et le sujet numérique. L'évaluation concerne le lancement de la réalisation de l'échange, la véracité des informations, leur adéquation aux besoins du destinataire. Dans ce contexte l'identité numérique est constituée d'un ensemble de requêtes d'identité.

Des technologies ont été développées pour répondre à des scénarios-type d'échanges conformes aux lois sur l'identité. Il s'agit principalement de ceux qui sont rencontrés sur Internet. Ils permettent la fourniture d'informations ou de biens avec paiement. Microsoft est le premier à avoir développé une architecture de MétaIdentité dénommée Infocard. Elle est centrée sur la personne. La technologie correspondante s'appelle Cardspace pour suivre la métaphore d'une distribution de cartes (de visites ou d'identité). D'autres entreprises et acteurs développent des technologies compatibles dans la même architecture[15]. Un projet de recherche européen[16] participe à cet effort. Il développe par exemple une formalisation des processus d'assurance et d'évaluation, ainsi qu'un système de gestion formelle des obligations[17]. Les domaines principalement concernés sont les places de marché, les réseaux sociaux et les espaces collaboratifs. Plus généralement il est proposé un cadre d'analyse pour améliorer la protection de la vie privée. Ces travaux s'insèrent dans une politique de développement de technologies de protection de la vie privé[18] (Privacy Enhancement technologies) soutenue par la commission européenne. C'est une contribution à l'établissement et la gestion de la confiance avec les technologies numériques.

3. Etudes de cas

L'évaluation de trois cas en Europe montre des dysfonctionnements majeurs dans les systèmes de contrôle et de pilotage. Les technologies disponibles pour le traitement de l'identité numérique ont été utilisées sans être insérées dans une vision systémique adaptée. C'est une démarche réductionniste qui a été utilisée. Elle est propre au développement scientifique des 19èm et 20èm siècles. Aussi bien en France qu'au Royaume-Uni les législations appropriées existent. Mais pour la gestion des données médicales, de police ou de vidéosurveillance publique ni l'application de la loi, ni l'efficacité n'ont été satisfaisantes. Il s'en suit une tentation de résoudre les problèmes par des postures politiques plutôt que par des solutions techniques.

3.1 Le dossier médical partagé en France

Le dossier médical partagé en France était prévu pour 2007. Il repose sur l'idée que les données médicales sont la propriété du patient[19]. Mais elles sont créées et hébergées par des tiers. Les personnels soignants et administratifs de santé les consultent. Il s'agit d'un MétaSystèmes d'identités numériques. Après de multiples expérimentations régionalisées, un premier déploiement national est prévu en 2010. Il reposera sur un hébergeur unique. En d'autres termes, pour des raisons de faisabilité, la technologie retenue n'est pas celle des MétaSystèmes d'identités numériques. Il est à noter qu'un grand projet britannique a connu des difficultés similaires. Elles sont mêmes plus importantes compte tenu des budgets en jeu. Par contraste un projet Israélien plus petit, plus décentralisé semble fonctionner efficacement.

La création du dossier médical partagé a été décrétée par le pouvoir politique. Pourtant dès 1979 Michel Crozier avait écrit "*On ne change pas la société par décret*"[20]. Les difficultés techniques du projet et ses implications sociales ont été sous-estimés. La plupart des travaux existant

s'orientaient vers une gestion régionale, où la technologie utilisée est relativement homogène. De plus la question critique d'un identifiant unique des personnes faisait l'objet de procédures spécifiques. En effet depuis 1966 la commission de l'informatique et des libertés déconseille l'utilisation du numéro de sécurité sociale[21] (NIRPP), qui d'ailleurs n'est pas toujours unique. Il existe par contre depuis plusieurs années un cadre unique d'identification des personnels de santé au travers d'une "carte de professionnel de santé" (CPS). Mais ce moyen n'est pas communément utilisé dans les systèmes régionaux, ni dans les structures de soins, ni chez les praticiens libéraux. Il nécessite une infrastructure généralisée de lecture de carte à microprocesseur. Les usages et la loi reposent sur une structure décentralisée, que l'on peut même qualifier d'atomisée si on prend en compte les praticiens libéraux. L'évolution naturelle de l'existant va vers des systèmes coopératifs. Mais la technologie et surtout les standards ne sont pas encore matures. La solution retenue d'un hébergeur unique pour un portail unique est sans doute celle de la raison compte tenu des contraintes. Mais ce choix crée aussi une identité numérique unique, simplifiée, qui peut être contradictoire avec la dynamique propre des systèmes existants et de la société.

3.2 Le fichier de police français STIC

Le fichier de police français STIC (Système de Traitement des Infractions Constatées)[22] a fait l'objet d'évaluations par les autorités de contrôle[23]. Ces évaluations sont fortement conflictuelles. Ainsi le rapport d'information de l'assemblée nationale note que « *c'est bien un dialogue de sourds qui semble s'être instauré entre les services de police et ceux de la CNIL, les premiers exigeant une plus grande reconnaissance de leurs préoccupations de la part de la CNIL et les seconds rappelant la nécessité d'une bonne tenue des fichiers de police* ». Effectivement le rapport de la CNIL note que seules 17% des fiches qui concernent environ 35 millions de personnes sont exactes, certaines parties comportant jusqu'à 32% d'erreurs. Cet outil majeur de la police nationale ne fonctionne pas correctement. Compte tenu de l'état de l'art technique, il ne paraît pas possible de le corriger. Ce qui conduira probablement à des pertes d'information importantes comme en 2004 où déjà 1,2 millions de fiches ont été effacées volontairement. L'analyse fait apparaître qu'un autre acteur, le Ministère de la Justice ne remplit pas ses obligations. Il ne met pas les informations à jour[24], ce qui détermine la dégradation du fichier. Mais en termes de moyens il faut observer que la France dépense deux fois moins par habitant pour sa justice que l'Allemagne. Il est toutefois curieux qu'un fichier appartenant à une administration dépende d'une autre administration pour sa mise à jour. Il n'y a pas d'homogénéité entre les procédures de fonctionnement et celles de gestion. C'est une erreur de conception en ce sens qu'elle substitue une approche intégrée à une coopération entre systèmes. Celle-ci étant, il est vrai, plus difficile à mettre en œuvre.

En outre il apparaît que ce fichier est occasionnellement exploité par des personnes non autorisées. Elles revendent les informations à des employeurs, des banques ou des assurances. Indépendamment, il arrive que des informations soient gracieusement fournies à des relations privées. En d'autres termes la valeur des informations a été sous-estimée et les mesures pour leur protection ne sont pas adéquates. Il faut néanmoins observer que l'état de l'art ne fournit pas encore de réponses matures, et standardisées.

Ce fichier de police correspond aussi à un MétaSystème d'identité numérique. Mais il a été mis en place avant que les concepts ne soient développés. La connaissance nécessaire à la conception n'est pas suffisante, les politiques formelles de contrôles sont insuffisantes et il ne peut y avoir de formation adaptée.

Les données concernées doivent être prochainement fusionnées avec celles correspondantes de la gendarmerie (JUDEX) pour créer ARIANE. La taille du "fichier" va encore augmenter, et la question de sa qualité sera encore plus critique.

3.3 La vidéosurveillance au Royaume-Uni

La vidéosurveillance au Royaume-Uni, est devenue un phénomène de masse. Il existe actuellement environ 4 millions de caméras. Par ailleurs le fichier d'ADN comporterait plus de 100.000 personnes innocentes[25] ; et à partir de 2009 toutes les personnes en relation professionnelle avec des enfants doivent se faire enregistrer, soit environ 11 millions de personnes[26].

Une évaluation globale de la commission des affaires constitutionnelles[27] conclue à la transformation de la société britannique en société de contrôle, et que cela doit changer. Il est notamment recommandé de changer la loi[28]. Une des principales recommandations est que la protection de la vie privée doit devenir partie intégrante des technologies de surveillance elles-mêmes. Il est aussi conseiller de limiter l'usage des moyens d'investigation aux infractions punies d'au moins deux ans d'emprisonnement. Toutes les nouvelles mesures devraient s'accompagner d'une évaluation constante de type post-législative. Les technologies des MétaSystèmes d'identité numérique sont explicitement citées. Le nouveau système de cartes d'identités nationales devrait d'abord être bâti autour des préoccupations du citoyen. Le cryptage des données personnelles doit être envisagé dans certains cas. L'emploi des technologies de protection de la vie privé est

demandé au gouvernement. Les notions de nécessité et de proportionnalité sont rappelées.

La réaction du secrétaire d'Etat à l'intérieur, Jacqui Smith, a été de rejeter l'appréciation selon laquelle le Royaume-Uni serait devenu une société de surveillance[29]. Mais depuis plusieurs années le comité britannique de la recherche en informatique a énoncé des mises en garde et des règles à suivre[30]. Le volume de données personnelles collectées, archivées et échangées doit être minimisé. Il faut également minimiser les durées d'archivage et mettre en place des techniques de destructions, y compris sur les sauvegardes. Il faut minimiser le nombre de personnes ayant des droits d'accès et contrôler le type d'accès. Il faut encrypter les données archivées. Enfin il faut développer des systèmes plus performants que ceux disponibles.

Le comité constitutionnel du point de vue de la loi, et le comité de la recherche informatique du point de vue technique ne font qu'exprimer la perte de contrôle sur les systèmes mis en place. La généralisation de la vidéosurveillance, par exemple, crée un nouveau type de système pour lequel se pose, notamment, la question de la copie de l'information, de l'identification par corrélation et de l'expérimentation d'un nouveau mode de contrôle social. Dans chacun de ces domaines il y a une élaboration insuffisante des concepts d'emploi et des outils de "contrôle du contrôle". Les sciences humaines n'ont pas été mises suffisamment à contribution et les technologies du contrôle et de la limitation d'accès ont été sous-employées. Il se crée par ailleurs des espaces d'expérimentation sociale laissés à l'initiative privée. C'est le cas lorsqu'une société propose de rémunérer toute personne qui via Internet remarquerait un incident, une infraction potentielle ou une conduite suspecte.

Le constat général est que la capacité de contrôle doit croitre avec les déploiements.

4. Le pilotage systémique

La mise en œuvre du contrôle systémique des identités numériques est une innovation sociale. Elle est de nature à restaurer le contrôle des systèmes complexes évoqués dans les études de cas. Une "*culture de la protection des données comme élément de bonne gouvernance*[31]" peut être rendue effective. Il est par ailleurs admis que l'interférence de l'Etat dans ces droits individuels peut être nécessaire pour le bien public[32].

4.1 La mise en œuvre

La mise en œuvre des principes et des technologies du contrôle systémique exige des compléments aux Métasystèmes d'identités numériques. Ceux-ci sont principalement issus des travaux d'entreprises commerciales. Presque toutes sont américaines, deux sont allemandes (SAP, Software AG). Aucun gouvernement ne s'est impliqué dans les processus de standardisation. Comme pour le dossier médical partagé la perspective est que le citoyen soit propriétaire de ses données. Les lois de l'identité ont une valeur universelle dans les démocraties. Mais des entités formelles supplémentaires par rapport à celles qui ont été déterminées sont nécessaires. Il faut prendre en compte l'existence du sujet réel à côté du sujet numérique. C'est lui dont les comportements sont formalisés par les nouvelles méthodologies comme BPEL4PEOPLE, WS-Human-Tasks, et P3P (Platform for Privacy Preferences).

C'est la relation entre le sujet réel et le sujet numérique (la cérémonie) qui fonde toutes les techniques de biométrie. Elles succèdent à l'anthropométrie de police. La singularité du sujet réel est définie par son corps, alors que la multiplicité des rôles sociaux est représentée par le sujet numérique. C'est la traduction du débat philosophique sur le corps et l'esprit, et du débat politique sur la souveraineté attachée au corps[33]. Les données sur le corps et sur l'esprit en tant que système neurologique appartiennent bien à l'individu selon la loi. Mais les données sur les rôles sociaux ont une dimension collective. Certaines sont liées à des relations bilatérales comme une relation bancaire. Mais d'autres sont liées à des relations multilatérales comme la dangerosité d'un comportement. Dans ce cas l'entité sociale qui est responsable du "bien public" doit être formalisée c'est l'Etat. Il s'agit d'une entité virtuelle qui se réalise dans de multiples fonctionnaires. Chacun ayant un rôle social particulier. Le fonctionnaire est bien une entité particulière du Métasystèmes d'identité numérique. Il dispose, dans son domaine, d'un droit d'accès privilégié aux informations privées. Dans certains cas ce droit peut être délégué à des tiers qu'il s'agisse d'organisations privées ou d'Etats étrangers. Pour des raisons culturelles ce rôle n'est pas formalisé dans les standards actuels issus des acteurs économiques, principalement liés à la tradition anglo-saxonne du "moins d'Etat". Le fonctionnaire n'est pas seulement une partie confiante, il est aussi un fournisseur d'identité, comme l'est le personnel soignant. Face à ces fournisseurs d'identité le sujet réel devient un fournisseur de sujets numériques. Seul le sujet réel dispose de la souveraineté sur sa personne. Seul il a la légitimité pour relier à lui les sujets numériques. Le droit français s'est déjà trouvé confronté à une situation similaire lorsque la législation sur le cryptage a évoluée. Le passage de l'interdiction à la tolérance s'est traduit par la création des tiers de confiance[34]. Ils étaient chargés de conserver la partie secrète d'une clé de chiffrement publique. Ils devaient la fournir à l'autorité administrative ou judiciaire en cas de besoin.

D'une manière générale dans les standards formels actuels, la société en tant qu'acteur n'est pas présente. Cela se traduit par l'absence de l'Etat, mais aussi par une formalisation insuffisante des procédures de protection du

"bien collectif" dont l'expression n'est pas marchande. De plus en Europe par exemple, le droit d'intrusion des entités marchandes dans la vie privée est limité. Or cette pratique d'inspiration Nord américaine correspond à une forme d'expression du "bien public". La compatibilité entre les différentes approches internationales implique de distinguer formellement ce domaine, qu'il soit pris en charge par des Etats, des organisations marchandes ou la société civile.

.

4.2 L'innovation technico-sociale

Le contrôle systémique implique une architecture qui supporte un MétaSystèmes d'identité numérique. Les données appartiennent au sujet réel. Mais une partie de ces données sont la copropriété de tiers, un de ces tiers particulier est l'Etat. Dans cette architecture, l'Etat est vis à vis du sujet réel dans une position de partie confiante (relying party) et de fournisseur d'identité. Il n'est pas nécessaire qu'il soit entrepôt de données ou tiers de confiance. Ces rôles peuvent être délégués. Conformément aux lois de l'identité le sujet réel devrait connaître les requêtes sur son identité numérique. Il devrait donner son assentiment ; même si la loi pourrait le punir de ne pas le donner dans certaines circonstances d'intérêt public. L'usage des technologies de cryptographie permet d'utiliser des entrepôts de données décentralisés, confiés au secteur privé ou à l'individu. In fine il serait reconnu que seul l'individu est en mesure de procéder à des corrections d'erreurs efficaces. Celui-ci pouvant éventuellement se faire assister de professionnels. Toutes les autres lois de l'identité s'appliquent au cas du contrôle social. La détermination de la frontière entre identités dédiées et identité partagée est un choix important. Elle conditionne la capacité de l'individu à garder le contrôle de sa sphère privée. En principe une identité dédiée correspond à un rôle social particulier. Elle est anonyme, lorsqu'il est difficile de la lier à une identité partagée ou à l'identité biométrique.

Selon les pays et les domaines d'activité il y a des regroupements d'entités « parties confiantes », par exemple dans le secteur bancaire (mauvais payeurs), le secteur des assurances (fraudes) ou celui de la location immobilière (impayés). L'Union Européenne et son espace de droit, de sécurité et de liberté est un autre exemple, à l'échelle des parties confiantes que sont les Etats. L'ensemble des règles d'échange au sein de ces communautés devrait se traduire en politiques de sécurité formelles. Elles devraient être strictement conformes au droit positif. Des mécanismes de négociation doivent pouvoir arbitrer des situations hybrides. L'application des politiques et les systèmes de négociation doivent s'appuyer sur des ontologies. C'est à dire sur une classification rigoureuse des informations constitutives de l'identité numérique dans un contexte donné. Il s'agit soit du contexte d'une relation bilatérale, d'une relation multilatérale ou d'une relation étrangère. Dans ce dernier cas il doit y avoir connaissance des espaces de noms qui se confrontent.

La formalisation n'est pas seulement une garantie de conformité à la loi. C'est aussi la possibilité de déployer des agents de contrôle automatiques. En d'autres termes l'Etat doit prévoir son extension au sein des processus et services autonomes qui formeront l'Internet Futur (sémantique et dynamique). Ce sont ces mêmes processus qui commencent à former les architectures orientées services en informatique patrimoniale.

Confier ses données à l'individu serait une révolution des pratiques. Mais ce ne serait qu'une mise en cohérence avec les révolutions numériques. Ceux qui sont exclus de cet "écosystème" pourraient faire appel à des tiers de confiance. Les technologies qui garantissent l'intégrité des données sont disponibles. En contre partie de ce renforcement des droits et pouvoirs des individus, la loi peut adapter son système de sanctions. C'est d'ailleurs la première étape de la mise en place du contrôle systémique a ses différents niveaux, du collectif à l'individuel. Cette étape implique la prise en compte et la formalisation des obligations des différentes parties, du fonctionnaire, aux organisations marchandes, à l'individu. L'autocontrôle de l'Etat étant renvoyé au domaine judiciaire comme il est d'usage dans les démocraties.

Références

[1] 1986: Gilles Deleuze (1925-1995 FR) dans « Foucault », Editeur : Editions de Minuit (mai 2004), ISBN-13: 978-2707318831

[2] 1990: Gilles Deleuze (1925 - 1995 FR) dans "Post-scriptum sur les sociétés de contrôle", Editeur : L'autre journal, n°1, (mai 1990)

[3] 1999: The Gramm-Leach Bliley Act ou «Financial Modernization Act » , Financial Privacy Rule, Safeguards Rule and pretexting provisions (usage de faux prétextes) et « Right to Financial Privacy Act » titre 12 du code des Etats-Unis, paragraphe 3401.

[4] 1996 : Health Insurance Portability and Accountability Act (HIPAA). Certains aspects ne sont entrés en vigueur qu'en 2007 et 2008.

[5] 2003 : F. Baader, D. Calvanese, D. L. McGuiness, D. Nardi, P. F. Patel-Schneider: The Description Logic Handbook: Theory, Implementation, Applications. Cambridge University Press, Cambridge (UK 2003). En français voir : A. Napoli "Une introduction aux logiques de description" Rapport de recherche INRIA n° 3314 Décembre 1997.

[6] Rule Markup Language (RuleML) exprimé en XML (Extensible Markup Language) du W3C, défini par des enterprises et des universités (ruleml.org); et SWRL

(Semantic Web Rule Language) décrit dans « SWRL: A Semantic Web Rule Language Combining OWL and RuleML », W3C Member Submission 21 May 2004 (Ian Horrocks, Network Inference; Peter F. Patel-Schneider, Bell Labs Research, Lucent Technologies; Harold Boley, National Research Council of Canada; Said Tabet, Macgregor, Inc. ; Benjamin Grosof, Sloan School of Management, MIT; Mike Dean, BBN Technologies)

[7] 2008: Livre blanc sur la défense, Odile Jacob / La documentation Française (juin 2008), ISBN 978-2-7381-2185-1.

[8] 1784: Emmanuel Kant dans « idée d'une histoire universelle au point de vue cosmopolitique », 6èm proposition, traduction faite à partir de l'édition des œuvres complètes de Kant de l'Académie de Berlin (Tome VIII), Traduction (2002) : Philippe Folliot.

[9] 1992 (7 Fev.), article 5.

[10] 1921: Thornstein Veblen (1875-1929 US) dans "The engineers and the price system (les ingénieurs et le système des prix)", Soviet of engineers; ce sont les prémisses d'une théorie de la gestion publique efficace avec l'école institutionnelle américaine et le mouvement des technocrates.

[11] 2003: Carl Ellison dans « UPnp Security Ceremonies Version 1.0», Intel (3 oct. 2003); et en 2005 dans « Ceremony Design and Analysis »

[12] 2007: WS-BPEL Extension for People (BPEL4People) Version 1.0, an approach for integrating human interactions using Web Services Business Process Execution Language (WS-BPEL) 2.0; Active Endpoints Inc., Adobe Systems Inc., BEA Systems Inc., International Business Machines Corporation, Oracle Inc., and SAP AG.

[13] 2007: Web Services Human Task, (WS-HumanTask), Version 1.0; (Adobe, BEA, Oracle, Active Endpoints, IBM, SAP)

[14] 2005 : Kim Cameron dans « The laws of identity », Microsoft Corporation (mai 2005).

[15] Un grand nombre d'entreprises dont IBM et SAPdans le projet Higgins, Novell dans le projet Bandit qui contient aussi le projet Higgins; SUN dans le projet openSSO ; OSIS ou Intelink-U, un projet dérivé du projet Intelink qui fédère les acteurs publics (DEA, CIA, FBI, NSA…) et privés du renseignement au Etats-Unis.

[16] 2004-2008: Privacy and Identity Management for Europe (PRIME) coordonné par IBM Suisse; et la seconde phase 2008-2012: PrimeLife - Bringing sustainable privacy and identity management to future networks and services.

[17] Obligation Management System (OMS); cycle de vie des capacités des systèmes gérant des données relatives à la vie privée (livrables du projet PRIME – FP7 Union Européenne).

[18] 2007 : Mémo de la commission européenne « Technologies renforçant la protection de la vie privée », MEMO/07/159 (2 mai 2007) ; Privacy Enhancing Technologies (PET) basées sur les directives 95/46/EC, 2002/58/EC et leur rapport d'application COM (2003) 265(01), 15.5.2003. Rapport de la conférence « Fine Balance 2007 - Privacy Enhancing Technologies» organisée par la commission européenne (21 novembre 2007).

[19] 2002: Loi relative aux droits des malades et à la qualité du système de santé (4 mars 2002) dite « loi Kouchner ».

[20] 1979: Michel Crozier dans "On ne change pas la société par décret", Edition Le livre de poche, (1982), ISBN 978-2253028864.

[21] 1966: Avis de la CNIL du 9 juillet 1966.

[22] Décret n° 2001-583 du 5 juillet 2001 ; et article 21 de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure

[23] 2009: Commission Nationale de l'Informatique et des Libertés : Les propositions de la CNIL pour une utilisation du fichier plus respectueuse du droit des personnes (20 janvier 2009) ; et Assemblée Nationale, rapport d'information n°1548 sur les fichiers de police (24 mars 2009).

[24] Selon le rapport de la CNIL le Ministère de la Justice ne renseigne les classements sans suites que dans 21,5% des cas, les relaxes dans 6,8% des cas et les non lieu dans 0,5% des cas.

[25] 2009: Forensic Science Service (FSS), environ 4,3 millions de fiches, concerne toute personne arrêtées ou suspectée (Angleterre et Pays de Galle)

[26] 2009: Independant Safeguarding Authority (ISA), selon une loi de 2006 qui concerne l'Angleterre, le Pays de Galle et l'Irlande du nord. L'estimation de l'ampleur du fichage est du journal "Daily Telegraph" cité par le journal "Le Monde" du 18 septembre 2009 (Virginie Malingre)

[27] 2009: « Les citoyens et l'Etat », rapport de la commission des affaires constitutionnelles de la chambre haute du 6 février 2009 (Chambre des lords).

[28] Data Protection Act de 1998.

[29] BBC news, 6 février 2009

[30] 2007: UK Computing Research Committee (UKCRC, juin 2007)

[31] 2006: European Data Protection report.

[32] Article 13 de la directive sur la protection des données privées and l'article 15 de la directive sur la vie privée électronique (ePrivacy).

[33] 1995: Giorgio Agamben (1942 - vivant en 2009 IT) dans "Homo sacer: le pouvoir souverain et la vie nue", Introduction, Editeur : Seuil (21 mars 1998), ISBN-13: 978-2020256452

[34] Loi n°90-1170 du 29 décembre 1990 sur la réglementation des télécommunications, Paragraphe II de l'article 28