Sécurité numérique : de l'acceptabilité de la contrainte au renforcement de la valorisation d'une organisation

Ingrid DUMONT
Coordinatrice scientifique
Projet DRIFT-FH

Marina PISANO
Chercheuse Ph.D
Université Technologique de Compiègne

Notre retour d'expérience s'inscrit dans le cadre du programme de recherche DRIFT-FH (Digitalisation, Risques, Incertitudes et Fragilités des Technologies associées aux Facteurs Humains), qui vise à réduire les vulnérabilités associées aux facteurs humains en sécurité du numérique dans les secteurs de la santé et de la défense. Ce projet transdisciplinaire allie les sciences humaines et sociales et les sciences de l'ingénieur pour atteindre ses objectifs. Lancé en janvier 2022 et financé par l'Agence Nationale de la Recherche (ANR), il entre dans la catégorie sécurité globale et cybersécurité. L'étude que nous vous présentons dans cet article fera l'objet d'une publication scientifique que nous partagerons au CyberCercle et qui vous rendra compte de l'intégralité des résultats. Notre témoignage porte sur l'acceptabilité de la contrainte dans la sécurisation des données au sein des organisations du secteur de la santé et la manière de parvenir à cette dernière.

Le secteur de la santé subit des vagues de cyberattaques mettant à rude épreuve ses diverses organisations, leurs personnels tout comme l'ensemble de leurs parties prenantes. La santé étant un secteur particulièrement prisé par les cyberattaquants, les données de santé sont parmi les plus recherchées sur le marché noir et comptent parmi les plus coûteuses. La question de la protection des données est donc un sujet particulièrement sensible. L'atteinte à ces données peut constituer dans un même temps une violation du secret médical mais également porter préjudice à la vie privée des personnes concernées. Visé par l'article 9 du Code civil, le respect de la vie privée représente un enjeu important pour les personnes concernées dans les atteintes aux données de santé. De plus, il convient de considérer que la santé n'est pas le secteur le plus aisé en matière de sécurité numérique car le secret médical est un secret partagé et la gestion des accès à ce dernier n'est pas la même selon les acteurs considérés.

De manière générale, lorsque nous parlons de la sécurité des données, il convient de prendre en compte trois critères pour en saisir ses particularités : l'intégrité, la disponibilité et la confidentialité. Selon les acteurs, le degré d'urgence et la gravité de la situation, la priorisation n'est pas la même. En effet, si les médecins privilégient la disponibilité et l'intégrité des données, les patients quant à eux accordent une attention particulière à la confidentialité de l'information (d'autant plus quand une fuite de cette dernière leur fait perdre l'accès à certains droits). Il est donc fondamental de considérer que les acteurs des organisations de santé évoluent dans un environnement empreint du secret médical, et que leur dynamique culturelle les prédispose à la protection du secret. Cela fonde

l'expectative d'une acceptation plus importante des mesures de sécurité (techniques et organisationnelles) de l'information par rapport à d'autres secteurs d'activité.

Outre les cybermenaces extérieures, ce secteur doit aussi faire face aux conséquences des vulnérabilités internes qui relèvent des individus et/ou des organisations et de leur environnement et qui peuvent involontairement porter atteinte aux informations (données personnelles et sensibles) des personnes concernées (patients et leur famille -pour les antécédents familiaux-, personnel de l'établissement, partenaires, etc.). Les vulnérabilités internes sont diverses et sont autant des sujets techniques qu'organisationnels et humains.

C'est pourquoi une analyse de risques techno-centrée ne permet pas suffisamment de prendre en compte les mesures organisationnelles de sécurisation. Le Règlement Général de la Protection des Données (RGPD) permet dans le cadre des analyses d'impact sur la vie privée d'allier les fiabilités techniques et humaines dans l'analyse de risques relatifs aux données et d'intégrer de la sûreté à la sécurité de l'information.

C'est dans ce contexte que nous avons conduit une étude [1] qui porte sur la question de savoir si *la manière dont un acteur de santé publique peut, sous couvert d'une mise en conformité à une réglementation visant à renforcer la protection des données, accroître sa fiabilité en s'appuyant sur ses facteurs organisationnels et humains en complément des aspects techniques de la sécurisation de ses systèmes d'information. Sous les aspects d'un contexte de contrainte, l'organisation peut-elle ainsi se créer une opportunité en fédérant l'ensemble de ses parties prenantes autour des enjeux de sécurité de l'information ?*

L'étude que nous avons conduite a pour but de favoriser la construction d'une dynamique de changement individuel, collectif et organisationnel au sein d'un organisme de prévention en santé publique via l'intégration de l'ensemble de ses parties prenantes.

Elle présente un double objectif. Le premier objectif relève de la mise en conformité juridique de l'ensemble des pratiques des parties prenantes de l'organisation en considérant le Règlement Général de la Protection des Données Personnelles (RGPD). Le deuxième objectif porte sur la levée de certaines résistances de la part du personnel et du public cible.

L'organisme de prévention en santé publique

L'organisme au sein duquel nous avons conduit cette étude se constitue d'un centre régional et d'antennes locales (par départements) et comporte un effectif compris entre 20 à 49 personnes. Une des principales actions de l'organisme repose sur une mission de service public dans le cadre de la prévention en santé publique, et notamment d'une prise en charge du dépistage de pathologies. Il met ainsi en œuvre la politique de prévention en santé publique tout en coordonnant les divers acteurs intervenant dans le cadre de sa mission (laboratoires, médecins, infirmières, etc.). De plus, il contribue à la formation initiale des médecins et à la recherche médicale dans son domaine d'activité.

Si nous avons choisi cette structure, c'est parce qu'elle a dû faire face dans le même temps à différentes contraintes organisationnelles, humaines et réglementaires qui ont eu des effets difficiles à gérer et pouvant porter atteinte à son bon fonctionnement. Elle venait notamment d'opérer une refonte de ses systèmes d'information (SI) quand la pandémie de COVID-19 est apparue,

[1] Ce RETEX a été repris dans le cadre du projet DRIFT-FH (Projet-ANR-21-CE39-0015) sélectionné par l'ANR dans le cadre des AAPG2021. Il est coordonné par la Fondation Saint-Cyr et réunit plusieurs partenaires (IRBA, AMSCC, Psycle, COSTECH, HEUDIASYC et IBISC). https://f-sc.org/financement-dun-projet-de-recherche-par-lanr/

aggravant l'instabilité et l'incertitude du contexte (obligation de mettre en place le télétravail, ralentissement des examens de dépistage et des prises en charge), exposé d'autre part à l'attrait des cyberattaquants pour les organisations du secteur de la santé. A cela s'ajoutait le fait que cette structure, qui a des interactions avec des individus multiples pour la réalisation de ses missions, a ainsi une surface d'attaque importante, son système d'information nécessitant de multiples interconnexions augmentant le risque d'une cyberattaque directe ou indirecte contre l'organisme. Ce dernier est aussi un acteur d'un système interdépendant pour la sécurité et la qualité des données de sa population éligible (ou public cible).

Une démarche sur-mesure et co-construite en trois temps pour permettre la conformité au RGPD de l'organisation

Pour conduire cette étude et ainsi favoriser la construction d'une dynamique sur-mesure à la fois individuelle, collective mais aussi organisationnelle, nous avons déployé notre démarche en trois temps, par des étapes à la fois distinctes et complémentaires : 1. Diagnostic ; 2. Ateliers de réflexion et de sensibilisation ; 3. Formalisation des outils adéquats au bon déploiement de la démarche et de son acceptation.

1. Le diagnostic : une première étape d'identification des pratiques et de la libération de la parole des parties prenantes

Le diagnostic est une première étape incontournable de la démarche qui consiste à observer l'organisation et évaluer sa conformité au RGPD selon notre compréhension de son contexte, de son histoire, ses pratiques, son environnement (conditions de travail, réseaux de partenaires, public cible, etc.). Il permet de saisir quelle perception ses parties prenantes (internes et externes) ont de l'autorité et de la protection des données. D'autre part, il est un véritable outil qui permet de libérer la parole et de mettre en lumière les flux de communication formels et informels au sein de l'organisation. L'analyse des pratiques et des comportements des acteurs est aussi une opportunité d'expliciter l'enjeu de notre étude. Le diagnostic favorise ainsi les échanges, et finalement la transparence et la compréhension de la démarche, indispensables pour dissiper les peurs et lever les freins au changement qui accompagnent tout projet de mise en conformité réglementaire. Grâce au diagnostic, le facteur humain est intégré ; ce dernier étant un élément de succès dans les changements organisationnels (Bareil, 2004)[2].

Si cette phase de diagnostic permet de mettre certes en lumière les points de l'organisation à améliorer, elle favorise aussi et surtout l'identification d'atouts à faire fructifier pour atteindre plus aisément les objectifs fixés (la mise en conformité juridique). Le diagnostic permet l'identification des leviers et des piliers sur lesquels il est possible de nous appuyer dans notre démarche.

Enfin, la restitution du diagnostic représente elle aussi une étape fondamentale pour susciter l'engagement du personnel dans la construction et le développement de la démarche à co-construire. En effet, plus la marche est grande pour atteindre les objectifs fixés, plus il est primordial de donner confiance tant à la direction qu'aux opérationnels. Cette confiance ne peut se faire pleinement si l'organisation est accablée par une mise en avant de ses points faibles. Autrement dit, les stratégies s'appuyant sur la peur ou sur la psychologie inversée, etc. demeurent contre productives.

[2] Bareil C. (2004), Gérer le volet humain du changement, Collection Entreprendre, Montréal, Les Editions Transcontinental Inc.

2. Réflexion et mise en place d'ateliers : une deuxième étape fondamentale pour favoriser la gouvernance, l'implication et la sensibilisation des opérationnels

La réflexion et la mise en place d'ateliers représentent la deuxième étape de notre démarche. Les ateliers sont construits en tenant compte des différentes pratiques quant aux traitements des données (une approche par les métiers - ce qui est prescrit - et les usages - le réel). Ils permettent ainsi de donner du sens à la règle de droit, de transmettre les savoirs essentiels appliqués au groupe concerné et de libérer la parole sur les usages. Ainsi, l'animation de l'atelier amène à une prise de conscience par les acteurs concernés et de leurs pratiques. Cette prise de conscience, lors de la sensibilisation, facilite l'appropriation des concepts clés de la protection des données par les acteurs de l'organisation et le sens donné à la règle les libère de la contrainte par une compréhension des principes qui sont proches de leurs pratiques ; inconsciemment, ils sont en partie conformes à la norme juridique (par le respect des règles relatives au secret médical) et le passage vers la mise en conformité devient beaucoup moins contraignant.

Une démarche co-construite peut faciliter l'acceptation, l'adaptation des comportements individuels, collectifs et organisationnels, l'implication, la responsabilisation et la satisfaction au travail.

Pour pallier la difficulté de prévenir le risque cyber et pour favoriser une telle dynamique du changement individuel, collectif et organisationnel, il convient de ne pas omettre d'intégrer la hiérarchie non pas pour les comptes rendus d'avancement mais bien comme un acteur à part entière. En effet, l'efficacité personnelle d'une personne peut être liée à sa perception de sa hiérarchie tout comme du degré d'implication de cette dernière (Ayache et Laroche, 2010)[3].

De plus, une hiérarchie qui suit de loin la mise en conformité perd des éléments de compréhension de la situation pour donner les moyens à ses équipes de respecter toutes les règles sans élaborer de stratégies de contournement. Si l'erreur est humaine, il ne faut pas oublier que la faute est souvent organisationnelle même dans le domaine de la sécurité numérique.

Par rapport à des enjeux sociétaux et de santé, la prévention des risques cyber peut pleinement contribuer à la satisfaction des parties prenantes des organisations notamment par le développement d'un leadership singulier enclin aux enjeux individuels, collectifs et organisationnels de son époque mais aussi futurs.

C'est ainsi que la deuxième étape de la démarche favorise au fur et à mesure de son avancée l'apparition d'une autonomisation sur le sujet du RGPD et de la sécurité des données mais aussi la création d'une responsabilisation de la part de l'ensemble des parties prenantes. C'est d'ailleurs dans ce contexte que nous observons le développement d'un véritable leadership responsable partagé au sein de la structure mais aussi, en dehors.

3. La formalisation de la documentation RGPD : une troisième étape qui rassure et verrouille la démarche sur-mesure et co-construite

Il est humain de percevoir la formalisation de procédures, du fait de leur caractère obligatoire, comme une contrainte. Cette perception est d'autant plus forte dans les organisations

[3] Ayache M, Laroche H. (2010), « La construction de la relation managériale. Le manager face à son supérieur », Revue française de gestion, Vol.4, n°203, pp. 133-147.

autoritaires. En effet, la formalisation permet la justification de la sanction. C'est pourquoi, il appartient à la gouvernance d'établir la confiance en favorisant les organisations apprenantes et en utilisant la formalisation comme un outil d'aide à l'autonomisation des opérationnels. Le cadre, lorsqu'il est connu et compris, a le mérite d'être rassurant et de servir de pilier pour l'autonomisation et la responsabilisation du personnel. Il est essentiel que l'encadrement contribue au partage de la vision de la direction et du sens (le pourquoi de l'action) auprès de tous les acteurs internes pour que ces derniers soient en mesure d'œuvrer dans le même sens et perçoivent leurs rôles et leur utilité pour l'atteinte de l'objectif final.

Dans la conduite d'un changement tel que celui que nous avons opéré, il est important de parvenir à aider et à encourager l'ensemble des parties prenantes à dépasser leurs craintes mais aussi leurs peurs. Cela passe par exemple par le fait de valoriser leurs bonnes pratiques existantes tout comme le fait de les relier au sens de leur mission et de leur travail. Dans le monde de la santé le rapport au secret médical est un appui pour faciliter l'acceptabilité des mesures de sécurité qu'elles soient techniques ou organisationnelles. Le secret médical est un secret partagé sur lequel nous avons capitalisé. La bonne compréhension et gestion du secret médical facilitent l'appropriation des mesures de sécurité préconisées par la réglementation et participent ainsi au développement d'un sentiment de responsabilisation ; car si la sécurité des systèmes d'information est l'affaire de tous, c'est encore plus bénéfique quand chacun en devient le maillon fort !

C'est ainsi que dès lors que la réglementation et les pratiques deviennent limpides pour les parties prenantes, la demande de déploiement d'outils devient naturelle. Leur appropriation en devient ainsi plus rapide et acceptée.

Le renforcement de la fiabilité de l'organisation et la valorisation de son capital social : un résultat au-delà de l'objectif initial de mise en conformité juridique

La valorisation, par cette approche, des pratiques professionnelles génère un levier de motivation, d'implication, de satisfaction, d'engagement et de fidélisation des parties prenantes. La prise en compte de l'humain, à titre individuel et collectif, permet de donner du sens aux procédures et de retenir l'attention de ceux qui devront accepter les « contraintes ».

Au-delà de la co-construction de la démarche proposée avec la gouvernance et les opérationnels, l'enjeu, dans ce type de démarche, est de permettre le développement d'un capital humain nécessaire à l'organisation, et finalement, de le reconstruire puis de le renforcer autour d'une culture partagée de la cybersécurité. Pour le reconstruire et le renforcer, il s'agit donc de considérer que le collectif, et ainsi l'appartenance des acteurs à une même structure, doit favoriser le développement d'une certaine confiance, la circulation de l'information, tout comme le renforcement d'une vision commune. L'ensemble est entretenu à la fois par les interactions sociales mais aussi par le partage de valeurs et d'une culture organisationnelle singulière.

Dans ce prolongement, il s'agit de capitaliser sur ce que l'on nomme « le capital social » (Coleman, 1988[4]; Nahapi et Ghosal, 1998 [5] ; Putnam, 2000 [6]) de l'organisation.

A partir de la confiance partagée entre les acteurs, qui est la base du concept du capital social, leur

[4] Coleman J.S. (1988), Social capital in the creation of human capital, American Journal of Sociology, vol.94, n°supplement, p.95-210.
[5] Nahapiet J., Ghoshal S. (1998), Social capital, intellectual capital, and the organizational advantage, The Academy of Management Review, vol.23, n°2, p.242-266.
[6] Putnam R.D. (2000), Bowling alone-The collapse and revival of American community, New York, Simon and Schuster.

coopération, engagement réciproque et la cohésion sociale se solidifient. Le capital social devient ainsi un levier fondamental pour permettre, à terme, l'amélioration de la performance organisationnelle et l'accélération de la diffusion des savoir entre les personnes (OCDE, 2001[7]). Dans la mise en place d'une démarche visant à la mise en conformité juridique d'une organisation, nous appuyons donc l'argument selon lequel la capitalisation portant sur l'association complémentaire du capital humain et du capital social favorise une adaptation et une adaptabilité efficace et rapide face aux enjeux liés à la cybersécurité tout en tenant compte de leur évolution rapide (et une facilitation de la résilience de l'organisation par un renforcement du collectif).

C'est ainsi que l'autonomisation des bonnes pratiques par les opérationnels en matière de sécurisation amplifie la sûreté des informations, et leur communication tout comme de leur verrouillage peuvent être renforcés tant en interne que vis-à-vis des partenaires externes. Les enjeux sont ainsi connus et reconnus par l'ensemble des parties prenantes internes et externes de l'organisation, ce qui peut même donner naissance au développement d'une marque employeur. Cette dernière aide à renforcer le sentiment d'appartenance, de satisfaction et de fierté de la part des équipes internes tout comme la confiance et la bonne réputation de l'organisme auprès des publics cibles.

La mise en conformité et la valorisation des pratiques pour la protection des personnes favorisent donc le développement de la confiance des publics cibles qui peuvent aussi avoir des freins quant au dépistage dans le cadre des politiques de prévention en santé publique, du fait de la peur des conséquences d'une atteinte aux données les concernant. En effet, la hausse des cyberattaques en santé amplifie une forme de déni et de peur de la divulgation, ce qui entraîne des freins au dépistage des pathologies. Or, ces peurs sont des obstacles à la prise en charge précoce et sont à l'origine de « perte de chance » de guérison pour les personnes dépistées tardivement. Toute action, dans ce secteur, en faveur de la protection des données permet une protection du secret médical et de la vie privée. Ainsi la prise de conscience des conséquences des pratiques professionnelles donne du sens aux procédures, et facilite l'adaptation des comportements des différents acteurs concernés et leur responsabilisation. La sécurité des systèmes d'information n'est donc plus seulement l'affaire de tous mais bien de la responsabilité de chacun.

Le Projet DRIFT-FH (Projet-ANR-21-CE39-0015) est financé par l'ANR. Il est porté par la Fondation Saint-Cyr et soutenu par la Banque Française Mutualiste.
Pour en savoir plus sur le programme de recherche DRIFT-FH : drift-fh@f-sc.org

[7] Organisation de Coopération et de Développement Economiques (OCDE). (2001), Du bien-être des nations : le rôle du capital humain et social, Editions de l'OCDE, p. 1-7.