

Éditorial : La protection de l'information en sciences humaines et sociales : de la prise de conscience à la vigilance
par Patrice Bourdelais _ 1

La sensibilité de l'information en SHS
par Joseph Illand _ 1

Approches juridiques de la protection de la vie privée et de la sécurité informatique
par Isabelle de Lamberterie _ 2

Sécuriser l'information dans une MSH
par Denis Duperray _ 4

C'est aussi arrivé ... en SHS
par Joseph Illand _ 6

Éditorial

La protection de l'information en sciences humaines et sociales : de la prise de conscience à la vigilance

PATRICE BOURDELAIS

Directeur de l'Institut des Sciences Humaines et Sociales (INSHS)

Que seraient les sciences humaines sans l'information, depuis celle livrée par les traces des civilisations lointaines jusqu'à l'analyse des faits sociologiques des sociétés contemporaines. Tous les éléments d'information sont récupérés, traités et archivés. Ils prennent déjà et prendront tous un jour une forme électronique. La reconstitution des monuments en 3D n'est que l'un des aspects les plus spectaculaires de l'usage de la numérisation et de l'informatique.

Mais l'information numérique a ses fragilités. Elle peut être perdue, volée ou devenir illisible du fait du vieillissement des supports ou de l'évolution des logiciels. Parfois de façon insidieuse, elle peut être faussée ou dénaturée, ou encore récupérée par des mains non souhaitées, alors que s'y attache une confidentialité momentanée ou définitive.

Le bulletin « Sécurité de l'information », dont la vocation est précisément d'alerter sur les risques d'atteintes à l'information, choisit dans ce numéro de traiter des sciences humaines et sociales.

C'est ici le fruit d'un partenariat entre la recherche elle-même et les services d'accompagnement à la recherche. En cela il convient de remercier la directrice de recherche émérite Isabelle de Lamberterie, d'avoir apporté à la réalisation de ce numéro tout l'acquis de ses travaux sur la société de l'information et de la sécurité. Elle y signe elle-même un article qui éclaire fort utilement des concepts liés à la nécessaire protection de la vie privée.

Pourtant, traiter de la « sécurité » en SHS surprendra plus d'un collègue, convaincu que la sécurité est l'affaire d'autres disciplines plus sensibles, mais non du monde ouvert et universel des sciences humaines. Joseph Illand, Fonctionnaire de Sécurité de Défense du CNRS, s'attache ici à démontrer cette idée simpliste et à montrer que les atteintes graves n'arrivent pas qu'aux autres...

Le diable se cache dans les détails ... de l'organisation et de la gestion informatiques, même dans des laboratoires de sciences humaines. Denis Duperray, responsable informatique de la Maison de l'Orient de la Méditerranée à Lyon, nous livre son témoignage sur le difficile métier de gardien de l'information.

« Sécurité de l'information » aura, je l'espère, l'occasion de revenir prochainement sur d'autres aspects de la problématique des risques. Je pense en particulier à la sécurisation des missions en pays à risques, certes non spécifiques au monde SHS mais où la part des chercheurs de ce domaine est prépondérante.

Il me reste à formuler le vœu que ce bulletin saura maintenir une saine vigilance dans nos initiatives quotidiennes, sans paranoïa ni naïveté excessives.

patrice.bourdelais[at]cnrs-dir.fr

La sensibilité de l'information en SHS

Joseph Illand

Fonctionnaire de Sécurité de Défense du CNRS

Dans le domaine des sciences dures et plus particulièrement lorsqu'il s'agit de recherches appliquées touchant des activités susceptibles d'application militaire ou tout simplement de compromissions à des fins d'espionnage scientifique ou industriel, la notion de données ou de secteurs « sensibles » ne suscite guère d'objection.

Dans les secteurs correspondants, les chercheurs ont, dans leur grande majorité, intégré les notions de menaces et de nécessaire protection.

Le monde des sciences humaines et sociales, à l'instar de la recherche fondamentale, pourrait sembler à l'abri du concept. Sans encourir l'accusation de paranoïa aiguë, peut-on reconnaître aussi en SHS l'existence de recherches « sensibles » ?

Dans l'affirmative, on sera enclin à identifier cette sensibilité aux questions de défense et de sécurité nationales.

► Travaux portant sur les questions de défense

Ainsi, loin d'être étanches, les domaines des sciences humaines et sociales et de la défense ont des rapports étroits.

Le monde de la « défense » (dans une acception large incluant la sécurité du territoire et des populations) ne peut ignorer l'apport des réflexions et travaux scientifiques relevant des sciences humaines : géopolitique internationale, étude des conflits territoriaux, étude des comportements de combattants ou populations lors de conflits armés, théorie et histoire des conflits, terrorisme, délinquance financière, etc.

Ces recherches peuvent être commanditées par des instances du ministère de la défense ou du ministère de l'intérieur ; elles peuvent aussi relever d'initiatives individuelles ou collectives du monde de la recherche.

Cet apport de scientifiques du monde des sciences humaines et sociales peut aussi s'exercer au profit d'organisations privées, d'entreprises industrielles, de groupes d'influence, voire d'États étrangers.

Il faut y ajouter, notamment à l'occasion de missions à l'étranger, des « consultances » occasionnelles ou régulières de chercheurs sollicités sur des questions de géopolitique et pour leur connaissance du « terrain ».

>>> suite page 8

Approches juridiques de la protection de la vie privée et de la sécurité informatique

Isabelle de Lamberterie

directrice de recherche émérite (CECOJI)

► Invitation à une « culture » de la sécurité informationnelle

La dualité « protection » versus « prévention » est au cœur de toute recherche de sécurité. Les cadres juridiques de la sécurité informatique accordent une place importante à chacun de ces objectifs : réprimer les atteintes mais aussi prévenir les risques. Nous ne nous étendrons pas sur la question de la répression des atteintes qui a déjà fait l'objet de nombreux développements dans le cadre de ce bulletin et nous insisterons ici sur l'autre volet, préventif qui invite à mettre en place une « culture de la sécurité ».

Cette culture de la sécurité passe par une sensibilisation à l'évaluation des risques par les intéressés eux-mêmes (détenteurs de fichiers, responsables de traitement mais aussi chacun de nous quand nous communiquons des données personnelles nous concernant). En SHS beaucoup d'entre nous – tant pour les besoins de leurs recherches que dans le cadre des autres missions des chercheurs (évaluation, expertise) – traitent des données personnelles ou recueillent des informations qui peuvent être confidentielles. Qu'est-ce qu'une donnée personnelle ? Qu'est-ce qu'un traitement ? Une information confidentielle ? Que signifie droit au respect de sa vie privée ? Ces différentes notions ne recouvrent pas les mêmes champs du droit même si elles se recoupent quant il s'agit de sécurité informationnelle versus liberté d'expression. Si le sens commun est évident, le sens juridique et le cadre auquel il renvoie n'est pas toujours évident.

Notre propos ici se limitera à ouvrir quelques pistes concernant les questions de sécurité liées au droit de l'information auxquelles peuvent être confrontés les chercheurs en sciences humaines. Pour aller plus avant, nous vous invitons à aller voir les sites des affaires juridiques du CNRS (notamment ce qui concerne « internet et régulation ») et de la CNIL (rubrique « nos libertés, droits et responsabilités »).

► Vie privée, confidentialité

Bien que la notion de vie privée ne soit pas définie par le législateur, ce principe a servi de fondement pour construire toute la jurisprudence sur le droit à l'image des personnes et même des biens. Ainsi, le consentement de la personne concernée (ou du propriétaire du bien) est requis avant publication ou diffusion d'une photo de ces personnes ou de ce bien.

Quant aux notions de confidentialité ou de secret, elles se rapportent, le plus souvent à des obligations statutaires ou contractuelles : secrets professionnels ou encore engagements de confidentialité (ex. souscrits par les membres d'une commission d'évaluation).

Le non-respect de ces différentes obligations classiques ne manquera pas d'entraîner des problèmes de sécurité comme cela a pu être évoqué dans certains des témoignages de ce bulletin.

► La loi « Informatique, fichiers, libertés »

Plus difficiles à appréhender, les notions se rapportant à la protection de la vie privée au regard du traitement de données à caractère personnel – sur lesquelles nous nous étendrons plus longuement – concernent de plus en plus de chercheurs. Souvent comprise uniquement comme imposant des contraintes administratives (déclaration, demande d'autorisation...), la loi « Informatique, fichiers, libertés », pose, dès son article 1, les grands principes sur lesquels est fondée la protection de la vie privée (dans une société où la circulation de l'information sur les réseaux est devenue le lot quotidien de chacun) : « L'informatique doit être au service de chaque citoyen. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ».

Aujourd'hui, où l'utilisation de l'informatique n'est plus réservée à quelques chercheurs qui traitent des grandes masses de don-

nées, chacun des membres de la communauté SHS est concerné quotidiennement par les principes énoncés ci-dessus dans le cadre des usages qu'il fait des différents réseaux (courrier électronique, site internet, réseaux sociaux, etc.) quand ces usages peuvent être appréhendés comme un traitement de données à caractère personnel. Ainsi, les définitions légales de ce que recouvrent les notions de protection de la vie privée au regard du traitement¹ de « données à caractère personnel » méritent attention. Nous les remettrons dans leurs contextes historique et sémantique.

► Mise en contexte historique : des initiatives qui remontent au début des années 70

Juillet 1970 : le législateur introduit, explicitement, dans la loi française un droit au respect de la vie privée : « Chacun a droit au respect de sa vie privée »². Dans le même temps, les risques liés au développement de l'informatique dans l'administration préoccupent les pouvoirs publics. Des cris d'alarme sont lancés contre le projet SAFARI. Le rapport Tricot (1974) relève les risques du moment : « Seule ou combinée

1. La notion de traitement aurait mérité elle aussi des développements. On rappellera ici le caractère très large de cette notion qui couvre tout le cycle de vie des données : « Constitue un **traitement de données à caractère personnel** toute opération ou tout ensemble d'opérations portant sur de telles données, **quel que soit le procédé utilisé**, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction » (Art 2 al 3).

2. Article 9 du code civil (Loi 70-589 du 9 juillet 1970)

avec d'autres techniques modernes, l'informatique permet de conserver les données et les résultats des traitements plus sûrement et d'une façon plus massive qu'autrefois... » tendant « à figer les situations en attachant aux individus des étiquettes » dont il était, avant, plus facile de se débarrasser.

Suivant les recommandations du rapport (*protéger le citoyen contre les menaces ou dérives d'une exploitation systématique et centralisée des données personnelles*), la France se dote, en janvier 1978, d'une « loi relative à l'informatique, aux fichiers et aux libertés »³.

Vingt ans plus tard, l'informatique s'est banalisée et comme le relève Guy Braibant dans son rapport au Premier Ministre en 1997, « le citoyen passif, mis en fiche par les grandes organisations est devenu un utilisateur actif de l'informatique et des réseaux... Les moteurs de recherche permettent d'opérer des croisements et des synthèses »⁴. Prenant en compte ce nouveau contexte ainsi que la nécessité de transposer la directive européenne de 1995⁵, le Parlement adopte en 2004⁶ la révision de la loi du 6 janvier 1978.

► Des « informations nominatives » aux « données personnelles »

Dans le nouveau texte, la notion de « données personnelles » est substituée à celle de « informations nominatives ».

Il convient de s'arrêter sur ce glissement sémantique et de voir sa portée. Nous partirons de l'arrêt du 22 décembre 1981 relatif à l'enrichissement du vocabulaire de l'informatique pour comprendre ce que recouvrent ces différentes notions. « *Information* » est définie comme un « élément de connaissance susceptible d'être représenté à l'aide de conventions pour être conservé, traité ou communiqué ». Alors qu'une « *Donnée* » est la « représentation d'une information sous une forme conventionnelle destinée à faciliter son traitement ».

L'approche sémantique, montre que ces deux notions très proches ne se recoupent pas complètement. Une donnée se distingue

d'une information par la transformation que cette dernière subit quant celle-ci est utilisée dans un traitement informatique. Selon cette acception, la donnée apparaît comme une information valorisée. La distinction entre les deux notions a le mérite de mettre en évidence la valeur ajoutée d'ordre technologique que supporte l'information brute pour devenir une donnée traitable informatiquement.

► Qu'en est-il du passage du nominatif au personnel ?

Comme on peut le constater, le terme « *personnel* » est aujourd'hui considéré comme mieux adapté, plus conforme à la réalité que « *nominatif* ». Il lève l'ambiguïté du sens étroit de « *nominatif* ». En utilisant « *personnel* » on cherche à mieux intégrer tous les éléments d'identification, tous les renseignements qui concernent une personne physique et permettent de l'identifier et non pas uniquement son nom. Toutefois, dès 1978, le législateur a posé clairement les limites de la distinction en donnant un sens large au terme nominatif : « Sont réputées nominatives au sens de la présente loi les informations qui permettent, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou par une personne morale »⁷. Le changement de vocabulaire, en 2004, ne marque pas une distinction significative. Il s'explique plus pour des raisons d'harmonisation européenne et internationale que pour des questions de fond.

Il n'en est pas de même de la portée de la définition de « donnée à caractère personnel » qu'introduit la loi de 2004 : est ainsi qualifiée « toute information relative à une personne physique identifiée ou qui peut être identifiée directement ou indirectement ou par référence à un numéro d'identification ou à plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne »⁸. On notera que le législateur français a voulu – par ce travail de définition mettre l'accent, explicitement, sur les traitements qui ne comportent pas de noms de personnes en insistant sur les *moyens* d'identification directs ou

indirects. Toutefois, il n'a pas jugé utile de reprendre – *in extenso* – la définition de la directive en particulier les détails relatifs aux « éléments propres de la personne » : identité physique, physiologique, économique, culturelle ou sociale.

Sans entrer de façon détaillée dans le régime de protection des données personnelles, il faut, néanmoins, mentionner la distinction qu'opère la loi suivant la nature des données. Pour certaines données dites sensibles, « il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les opinions raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci ». Par dérogation à cette interdiction, certains traitements de données sensibles restent possibles dans la mesure où la finalité du traitement l'exige et moyennant le respect de certaines conditions. Parmi ces dérogations (qui sont au nombre de dix), on relèvera « les traitements mis en œuvre par une association ou tout autre organisme à but non lucratif et à caractère religieux, philosophique, politique ou syndical » pour les données correspondant à l'objet de l'association, « sous réserve qu'ils ne concernent que les membres ... et le cas échéant, les personnes entretenant avec l'organisme des contacts réguliers ... ».

Pour comprendre ce qu'est une « donnée personnelle » il faut, aussi, analyser quand cette donnée n'est plus personnelle.

► Qu'est-ce qu'une donnée anonyme ?

« *Anonyme* »⁹ peut être considéré comme l'antonyme d'« *identifié* ». Un ouvrage anonyme est sans nom d'auteur, une société anonyme est une société dont les propriétaires restent inconnus du public.

Une donnée anonyme est une donnée qui ne peut être rattachée à une personne physique. Le processus d'anonymisation, auquel sont tenus ceux qui souhaiteraient utiliser des données nominatives, consiste, donc, en la destruction (effacement) des identifiants. Une fois le fichier anonymisé, son traitement ne relève plus des contraintes des lois sur la protection de la vie privée au regard du traitement de l'information et l'on mesure

3. Loi n°78-17 du 6 janvier 1978 (JO 7 janvier 1978 et rectificatif au JO du 25 janvier 1978)

4. G. Braibant *Données personnelles et Société de l'Information* La documentation Française 1998

5. Directive 95/46/CE du 24 octobre 1995

6. Loi 2004-801 du 6 août 2004 (JO du 7 août 2004) relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel

7. Article 4 ancienne loi de 1978.

8. Article 2 3° alinea

9. Dans le Vocabulaire Juridique (G. Cornu), 8^e édition, PUF, 2000 : Anonyme (1) Qui n'a pas de nom patronymique.... (2) Qui ne porte pas de nom de personne.

l'importance à accorder aux frontières entre *nominatif* et *anonyme*¹⁰.

► **Où commence l'anonymat ?**

Où s'arrête l'indirectement nominatif ?

Pour apporter quelques éléments de réponse à cette question, il convient de cerner la notion d'identifiant direct ou indirect. Une donnée qui, apparemment, peut être considérée comme anonyme peut, en fait, être indirectement nominative. L'identification n'est pas définie en tant que telle par les textes, si ce n'est que ceux-ci, nous venons de le voir, prennent plus ou moins la peine

10. La question de l'anonymisation s'est posée à propos de la mise à disposition des décisions de jurisprudence à un large public. Certains pensent qu'il y a un risque d'atteinte à la vie privée des parties si on laisse le nom de celles-ci dans les bases de données de jurisprudence. D'autres défendent le point de vue inverse en rappelant que les jugements sont des données publiques et que l'anonymisation va à l'encontre de la publicité des jugements. On renverra à la recommandation de la CNIL qui invite à retirer le nom des parties en s'appuyant sur l'efficacité et les dangers pour la vie privée des moteurs de recherche sur internet (Délibération n° 01-057 du 29 novembre 2001 portant recommandation sur la diffusion de données personnelles sur internet par les banques de données de jurisprudence).

de préciser les éléments qui permettent de procéder à l'identification d'une personne. On peut admettre que l'identité d'une personne en droit (notamment en droit civil à travers la distinction des personnes physiques) repose sur la différenciation, c'est-à-dire le marquage d'un individu par un certain nombre de caractéristiques, qu'il partage, pour chacune d'entre elles, avec d'autres individus, mais qui, prises ensemble, permettent de le singulariser, de l'individualiser. Seul un identifiant unique – on songe évidemment au numéro dit de sécurité sociale ou éventuellement à une identité génétique complète – permet à lui seul d'individualiser une personne déterminée de façon univoque (*unicité*) avec certitude, et c'est à juste titre qu'il fait peur. Hors des cas où l'on se trouve en possession d'un identifiant unique, l'identification suppose non pas une donnée mais un ensemble de données permettant de renvoyer à une personne précise et à elle seule.

La qualité d'identifiant dépend, aussi, de l'aptitude du destinataire à identifier la personne à travers les données la concernant. Autrement dit, un identifiant identifie une personne *pour* quelqu'un. On mesure à travers cette analyse la relativité d'un identifiant qui n'est lisible que par certains. On mesure aussi qu'une donnée qui apparemment peut sembler être anonyme ne l'est pas pour celui qui a le pouvoir d'identifier une personne, à travers cette donnée.

L'identification est, alors, ou non possible, non pas tant selon les caractéristiques du fichier ou des données en elles-mêmes, mais plutôt en fonction de l'information dont dispose le destinataire et de sa capacité à la lire.

Ce constat permet de mesurer les limites d'une protection de la vie privée fondée sur une opposition – *in abstracto* – entre anonyme et nominatif. Pour apprécier les risques effectifs d'une possible atteinte ne doit-on pas tenir compte de plusieurs facteurs : tout d'abord les éléments du contexte, mais aussi, la volonté du destinataire de l'information de procéder à une identification – que les données soient ou non anonymes ; enfin, les informations dont celui-ci dispose pour effectuer la recherche d'identification.

Quels pourraient être alors les critères pour caractériser le vraiment *non identifiable* ? Rien n'est dit dans la loi sur ce point si ce n'est que l'on dispose des critères d'appréciation pour dire si une personne est identifiable : l'article 2 de la loi de 2004 renvoie « à l'ensemble des moyens ... dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne ». Néanmoins, force est de constater le caractère relatif de ces notions qui sont laissées à l'appréciation de la CNIL ou du juge. ■

delamberterie[at]ivry.cnrs.fr

Sécuriser l'information dans une MSH

Denis Duperray

Responsable informatique de la MOM

Expert auprès de la Coordination Régionale SSI de la Délégation Rhône-Auvergne du CNRS

► **La Maison de l'Orient et de la Méditerranée (MOM) en quelques mots**

La MOM, située à Lyon, est l'une des vingt Maisons des Sciences de l'Homme (MSH) en France. Elle a été créée en 1975 et est composée à ce jour d'une Fédération de Recherche (FR) et de 5 Unités Mixtes de Recherche (UMR), l'ensemble regroupant 180 personnels statutaires et

160 doctorants, soit un total de 340 personnes. L'activité de recherche concerne l'étude de la Méditerranée, du Proche et du Moyen-Orient sous ses aspects passés et présents. Le pilotage et le bon fonctionnement de la MSH sont assurés par la Fédération qui, composée de services opérationnels mutualisés, offre ses prestations de services aux UMR et collabore à leurs activités de recherche.

► **La prise de conscience des problèmes de Sécurité du Système d'Information (SSI)**

En 1998 le rapport scientifique de la MOM fait état d'un parc de seulement 69 machines connectées au réseau internet et d'un site web « expérimental » tout juste mis en service en début d'année. La MOM vit en cette période les prémices d'une métamorphose de son système

informatique qui l'amènera vers l'accès « banalisé » aux nouvelles technologies de l'information et de la communication qu'elle connaît aujourd'hui avec un parc qui a plus que triplé ! Comme dans de nombreux autres laboratoires à l'époque, ce développement va s'opérer à la MOM dans l'enthousiasme de la nouveauté **sans précaution particulière en matière de sécurisation de l'information**. Il convient de préciser qu'alors les problèmes de sécurité du réseau internet étaient moins répandus qu'aujourd'hui et ne préoccupaient que les spécialistes. Les premières recommandations du CNRS pour sensibiliser les directeurs à la sécurité des systèmes d'information ne sont apparues que quelques mois plus tard.

Courant 2000, alors que la MOM observe une augmentation de ses déploiements et de ses besoins liés aux technologies de l'information, le poste d'administrateur des systèmes et réseaux devient vacant et la gestion correspondante n'est plus assurée. Rapidement la MOM se retrouve victime d'attaques répétées depuis le réseau internet. Celles-ci finissent par neutraliser complètement son serveur de diffusion web et de messagerie. Cible d'un pirate dont l'ambition ne semblait pas être de voler des données mais plutôt de nuire à l'institution, la MOM connaît là ses premiers problèmes sérieux de sécurité informatique et prend conscience, à ses dépens, de l'insécurité grandissante sur le réseau internet et de l'impact désastreux que celle-ci peut avoir sur le fonctionnement de l'organisme.

Le directeur démuni face à ces piratages récurrents, commande une mission auprès de l'Unité Réseau du CNRS (UREC) pour dresser un état des lieux et préconiser des recommandations. Le rapport suggère la mise en place urgente de règles de filtrage (alors inexistantes) des accès internet, une réorganisation complète de l'architecture réseau, une restructuration des services internet et surtout le recrutement d'un Administrateur Systèmes et Réseaux (ASR) pour la mise en œuvre opérationnelle.

En septembre 2001, le poste est enfin pourvu. C'est dans ce contexte que j'ai pris mes fonctions d'ASR à la MOM avec pour mission principale de restructurer le réseau et pour axe stratégique : **la sécurité du système d'information**. Implicitement, le rôle effectif de « Responsable de la Sécurité du Système d'Information » (RSSI) venait d'être créé à la MOM.

► Des mesures rapides et efficaces

Avec un axe stratégique aussi clairement soutenu et des moyens en adéquation, les changements se sont rapidement opérés. Des mesures organisationnelles ont tout d'abord été prises. Le service en charge des déploiements a été créé et nommé « Réseau, Système ET Sécurité ». La composante sécurité des systèmes d'information inexistante auparavant complétait donc officiellement ma mission d'ASR. J'avais ainsi toute légitimité pour communiquer et faire prendre conscience aux différents acteurs des problèmes posés par la SSI et des mutations qu'ils imposeraient désormais dans l'usage de l'outil informatique.

Un schéma directeur technique, prévoyant au rythme du contrat quadriennal les directives et les moyens appropriés, a été discuté et validé avec la direction. Une politique informatique intégrant explicitement la sécurité prenait ainsi forme et m'assurait les moyens de sa mise en œuvre.

Les techniques, aujourd'hui incontournables et connues de tous les ASR mais pas très répandues à l'époque, ont alors été déployées à la MOM. Un pare-feu a été installé pour gérer les règles de filtrage plus facilement que sur le routeur d'entrée de site. Les hubs, complètement obsolètes, ont été remplacés par des commutateurs permettant la segmentation du réseau et le cloisonnement dans une zone dite délimitarisée des machines les plus sensibles, tels que les serveurs web et messagerie qui avaient subi les piratages et continuaient à en être la cible. Les services internet ont été redéployés sur des serveurs renouvelés et les logiciels et systèmes d'exploitation entièrement mis à jour. Une salle machine climatisée et ondulée a été construite. Enfin un système de sauvegarde centralisée et un système d'accès à distance par réseau privé virtuel ont été implémentés. Dans le même temps, un périmètre d'intervention et un catalogue de services ont été définis donnant naissance à une nouvelle procédure et à **un formulaire de « demande d'accès aux ressources informatiques »**. Ce formulaire accompagné de la charte officielle du CNRS a été instauré dès 2003. Celle-ci devait obligatoirement être signée à chaque nouvelle demande d'accès afin de sensibiliser les utilisateurs des ressources informatiques et de les responsabiliser quant à leurs devoirs. Enfin, une politique d'achat et de gestion de parc a été conduite afin de renouveler des machines vieillissantes inaptées aux mises à jour et à la mise en place de nouveaux logiciels.

Bien que relativement isolé en tant qu'ASR d'une MSH, j'apprécie tout particulièrement et ce depuis le début, ma collaboration avec le RSSI de notre tutelle : l'Université Lumière Lyon2. J'ai par ailleurs toujours été accompagné par le CNRS tout au long de la démarche et j'ai bénéficié de réseaux et de contacts d'une extraordinaire compétence. J'ai tout d'abord participé dès 2001 aux formations SIARS¹, puis VCARS² en 2002, pour rapidement occuper un rôle régional actif de coordinateur sécurité de la Délégation Régionale Rhône-Auvergne (DR7) et dispenser moi-même au sein de ce réseau des formations relevant de l'expérience acquise. A la suite de l'évolution de l'organisation de la SSI au CNRS en 2007, j'ai été nommé expert auprès de la Coordination Régionale SSI (CRSSI) de la DR7.

► De nouvelles menaces et plus de vigilance de la part des utilisateurs

Ainsi la MOM a atteint maintenant un niveau de sécurité de son système d'information plutôt satisfaisant. Les techniques de piratage dont elle était jadis victime se sont rapidement heurtées aux règles de filtrage implémentées sur le pare-feu. La sensibilisation des utilisateurs sur l'usage systématique d'un anti-virus sur leurs postes, ainsi que le déploiement de passerelles réseau ont porté leurs fruits pour lutter contre les virus, spam et autres espionnages.

Mais il ne faudrait surtout pas « se reposer sur ses lauriers ». L'ingénierie sociale prend de plus en plus la relève comme en témoigne **ce récent cas de piratage** dont a été victime un utilisateur de la MOM. Celui-ci me signale dans un premier temps ne plus recevoir de messages électroniques. Je vérifie son compte et je découvre qu'il a paramétré une simple redirection de ses mails vers une adresse personnelle, probablement, me dis-je, pour gérer une période d'absence. Je lui signifie avec diplomatie qu'il a certainement oublié de désactiver cette redirection. Très surpris, il me précise n'avoir jamais procédé lui-même à ce paramétrage. Un nouveau contrôle de son profil montre que son

1. **SIARS** (Sécurité Informatique pour les Administrateurs Réseaux et Systèmes) était une formation d'une semaine destinée aux administrateurs système et réseau des laboratoires du CNRS qui était donnée dans les régions dans les années 2001 et 2002.

2. **VCARS** (vers des Communications et des Applications Réseaux plus Sécurisées) est une école thématique organisée par le CNRS et l'INRIA en 2002 et 2003 sur le thème de la sécurité informatique des communications

compte est très actif la nuit pour envoyer des messages « publicitaires ». Plus de doute, il s'agit bien là d'un usage frauduleux de sa messagerie dans le but d'envois massifs de « spams », le pirate ayant pris soin de rediriger automatiquement les messages entrants afin de ne pas éveiller les soupçons.

Mais comment celui-ci a-t-il pu prendre possession du compte ? Rien de plus simple ; l'utilisateur m'a avoué plus tard avoir répondu quelques jours auparavant à un mail semblé venir de l'administrateur système de la MOM. Ce message le mettait en demeure de communiquer en retour son identifiant et son mot de passe pour raisons techniques ; très discipliné il s'était exécuté sans délais. Bien évidemment ce mail usurpait l'adresse de l'administrateur système et les réponses faites (avec identifiant et mots de passe) partaient directement dans la boîte du pirate qui a pu par la suite en faire l'usage que l'on sait. Cette anecdote d'hameçonnage (phishing) dont nous avons ainsi fait les frais n'est pas exceptionnelle mais illustre bien l'un des nouveaux procédés d'ingénierie sociale, très largement utilisé, et qui ne requiert aucune technicité de la part du malfaiteur pour voler des données ou des ressources. Les messages d'information pourtant envoyés régulièrement au sein de la MOM pour rappeler qu'aucun identifiant, mot de passe, code de carte ne doit JAMAIS être communiqué par mail n'ont pas suffi, confirmant qu'il fallait sans relâche informer et sensibiliser pour lutter contre ce type d'attaques dont seul l'utilisateur par sa vigilance personnelle pourra dorénavant se prémunir.

► La PSSI de la MOM : un projet à part entière et des mutations à venir

Dans le cadre de la réorganisation de la SSI au CNRS, toutes les unités de recherche doivent nommer, depuis 2008, leur Chargé de Sécurité du Système d'Information (CSSI).

La MOM, qui est constituée de la fédération et de cinq UMR partageant la même infrastructure pour son système d'information, a fait le choix de ne nommer qu'un seul CSSI mutualisé comme l'y autorise la Politique de Sécurité du Système d'Information (PSSI) du CNRS. Mon implication dans la SSI au sein de la MOM et au niveau régional m'ont conduit naturellement à être nommé CSSI mutualisé pour l'ensemble des unités constitutives de la MOM.

Depuis cette année, reprenant la méthodologie préconisée par la CRSSI, j'ai adopté une véritable méthode projet pour mener à bien la mise en place du Système de Management de la Sécurité de l'Information (SMSI) et la rédaction de la PSSI locale. A ce jour, les directeurs des unités constitutives ont tous reçu l'information de sensibilisation à la SSI et ont nommé **le comité de pilotage du « projet PSSI »**. Ce groupe de travail (8 personnes plus moi en tant que chef de projet) se veut représentatif des processus métiers que nous avons distingués à la MOM : la recherche, l'enseignement et la gestion.

Le comité de pilotage a commencé ses travaux d'identification et de valorisation des actifs primordiaux relevant de ces processus métiers. Il devra ensuite distinguer un certain nombre d'actifs de soutien, les vulnérabilités intrinsèques et les menaces ; la finalité étant de calculer le niveau de risque sur chacun des actifs à protéger et de présenter à la direction une analyse de risque objective et formalisée du système d'information. Cette analyse devra conclure pour chaque menace, comme l'indique la norme ISO 27001, à un traitement du risque : *accepter, diminuer, transférer* ou *éviter* le risque. La déclaration d'applicabilité et enfin la PSSI de la MOM seront rédigées par la suite.

A quel type de décision cette analyse va nous conduire ? Considérons par

exemple notre salle machine dont l'une des vulnérabilités est de ne pas posséder d'accès identifié. L'analyse de risque conclura que le niveau de risque de la menace d'intrusion physique dans cette salle machine est relativement élevé. *Accepter* le risque consisterait à ne prévoir aucune action corrective, ce qui n'est pas responsable. *Éviter* le risque le serait encore moins puisque cela reviendrait à prendre la décision de supprimer la salle pour que le risque disparaisse. *Diminuer* le risque nous amènerait à définir des actions voire des projets destinés à réduire le niveau de risque : par exemple faire poser un lecteur de badge contrôlant l'ouverture de la porte ! Enfin, *transférer* le risque reviendrait à déplacer la responsabilité de celui-ci sur un tiers, en externalisant par exemple l'hébergement de nos machines. Dans cet exemple pris isolément, le choix le plus simple serait de *diminuer* le risque par la pose du lecteur de badge. Mais considérant bien d'autres menaces (les pannes de climatiseur, d'alimentation électrique, d'onduleur, l'incendie, etc.) pour lesquelles *diminuer* le risque par diverses actions plus ou moins coûteuses ne serait pas forcément le meilleur choix stratégique et économique, la MOM réfléchit objectivement à *transférer* les risques en externalisant l'hébergement de ses serveurs auprès de l'université. Cet exemple nous montre que par le biais de son projet de PSSI et par sa démarche d'analyse de risque, la MOM va certainement vivre dans les mois à venir de nombreuses mutations de son système d'information. Elle devra relever ce défi en tenant compte toujours plus des réels besoins de l'institution et des attentes des utilisateurs en gardant comme priorité : la sécurité de son système d'information. ■

denis.duperray[à]mom.fr

C'est aussi arrivé ... en SHS

Joseph Illand

Fonctionnaire de Sécurité de Défense du CNRS

► Atteinte à des intérêts nationaux

En avril 2007, un mail « coup de gueule » est expédié par un agent d'un centre du CNRS à l'étranger, dans un pays où les intérêts de la France peuvent être sujets à remise en cause.

Ce libelle incendiaire pourfendant la « dictature » du régime en question, et transmis en toute naïveté à une soixantaine de destinataires, s'est retrouvé en quelques minutes sur la Toile. Un impair qui a failli provoquer

la rupture des relations culturelles entre le régime incriminé et la France. Cet incident s'est accompagné de maladresses comme un démenti hâtif des responsabilités de l'agent et une mise en ligne

sur un site américain par un enseignant-chercheur sans vérification... mettant ainsi l'accent sur les limites de l'information et de la désinformation sur le Net.

Cet incident a montré les risques politiques d'une absence de « réserve » de la part d'agents en poste à l'étranger vis-à-vis du pays d'accueil. Il a montré également le potentiel d'impact de l'utilisation non maîtrisée de l'outil informatique. Ces divers textes (courriel diffamatoire et vrais-faux démentis, toujours en ligne sur le net) montrent qu'en matière de communication via Internet, le droit à l'oubli n'existe pas.

► Atteinte à des chercheurs impliqués dans des recherches sensibles

Certaines recherches dans des contextes à forte composante conflictuelle, géopolitique (nationalismes, territorialités, terrorisme, extrémisme...) ou sociétale (débat sociaux, controverses violentes...) peuvent impliquer des risques directs pour les chercheurs impliqués dans ces recherches.

Cambriolages

Un laboratoire travaille sur des sujets de territorialités et un chercheur, de nationalité étrangère, y travaille sur des questions sensibles touchant directement son pays d'origine. Ce chercheur est l'objet à son domicile d'une série de cambriolages très ciblés. La perte des documents est, selon la direction du laboratoire, « inestimable, car ce sont 20 ans de recherches et de documentation qui sont perdus ».

Prendre conscience des menaces possibles. S'assurer de l'existence de sauvegardes en des lieux différents. Informer le service du FSD et le cas échéant les services de police de tout incident constaté ou de suspicion grave.

Vols de portable

Un chercheur en sciences sociales engagé dans des recherches ultrasensibles touchant à la mafia, à la police, à la justice et au pouvoir, dans un pays étranger, s'est fait dérober dans ce pays son ordinateur portable (et d'autres pièces compromettantes : agenda, carnet d'adresses, notes de terrain...).

L'ordinateur contenait l'ensemble des données recueillies depuis plusieurs années, la boîte mail et de nombreuses données à caractère personnel.

Un chiffrage solide du portable aurait pu au moins limiter les risques de compromission de données sensibles mettant en péril la sécurité du chercheur.

Menaces

Un chercheur mène des travaux sur un sujet objet de vives mises en cause sociétales. Ses publications dérangent et sont vivement contestées par des groupes de pression. Sous menaces de mort, bien entendu anonymes, il est invité à renoncer à ses recherches et à faire publiquement son autocritique...

Il n'est pas question de céder au chantage mais les chercheurs impliqués dans des travaux à vive contestation sociétale doivent intégrer ce risque et faire part du moindre incident au service du FSD et aux services de police spécialisés.

► Mises en cause personnelles

Dans le cadre d'un contentieux politique impliquant un sociologue et philosophe de renom, une collaboratrice qui prit publiquement fait et cause pour lui est l'objet de graves menaces. L'attaque prend la forme d'une inondation par mails (« mail bombing »), ce qui conduit à paralyser la messagerie de cette personne.

Le service du FSD a été immédiatement informé et le relais a pu être assuré auprès des services de police spécialisés.

Saisir le service FSD de tout incident ou de mise en cause personnelle grave (ce qui n'exclut pas bien sûr de prévenir tout d'abord les services juridiques ou du personnel.)

► Atteintes à la protection de la vie privée

Un thésard réalise une enquête sur les clients de constructeurs automobiles. Il s'appuie pour ce faire sur des fichiers commerciaux de clients fournis par des entreprises. Ces fichiers et le fichier d'ensemble constitué par le thésard n'ont pas été déclarés à la CNIL. Un « client » informé de cette enquête menace de porter plainte. Ce cas n'est pas unique.

Les recherches en sciences humaines s'appuient parfois sur des enquêtes dont certaines peuvent revêtir un caractère « personnel », s'il y a identification possible des individus objets de l'enquête.

Une vigilance est de mise pour éviter de porter atteinte à des libertés individuelles et pour protéger les chercheurs et responsables du CNRS de poursuites pénales.

Il est utile de consulter les informations en ligne sur les obligations découlant de la loi Informatique et Libertés, sur le site de la CNIL et sur celui de la Direction des Systèmes d'Information du CNRS (<http://www.dsi.cnrs.fr/cnil/declarer/declarer2.htm>). Il est conseillé également de prendre contact directement avec la DSI et de solliciter si nécessaire le service du FSD et la Direction des Affaires Juridiques du CNRS

► Hameçonnage fructueux

L'article de Denis Duperray « Sécuriser l'information dans une MSH » évoque un cas de piratage par phishing et les conséquences pour le laboratoire.

Plus récemment encore, mais selon le même processus, un directeur de recherche en sciences sociales reçoit un mail d'un service informatique l'incitant à remettre son identifiant et son mot de passe. Il s'empresse évidemment de répondre !

La compromission immédiate du poste entraîne une émission massive de spams à partir du serveur du centre du CNRS concerné. La messagerie du centre est bloquée pendant près de deux heures, le temps au service informatique de procéder au nettoyage.

Ces attaques dites par « phishing » ou « hameçonnage » sont très fréquentes. Quelques jours plus tôt, deux chercheurs d'un laboratoire ... de mathématiques du CNRS avaient mordu de façon strictement identique, avec les mêmes conséquences immédiates.

Malgré des mises en garde diffusées à l'ensemble des laboratoires du CNRS, mais aussi des alertes parues dans la presse (suite à des tentatives d'arnaque au nom de France Telecom), d'autres « prises de poison » ont encore été constatées au sein du CNRS, au cours de l'été.

Ne jamais transmettre d'informations confidentielles en clair par internet, encore moins à des personnes ou services inconnus et qui plus est lorsque la rédaction est ponctuée d'expressions suspectes. Dans le doute consulter le vrai « service informatique »

► Incident informatique dans une maison des Sciences de l'Homme

Une grave attaque informatique ciblée contre une Maison des Sciences de l'Homme a donné lieu à une plainte du laboratoire, sans information du service du FSD, ni de la Direction des Affaires Juridiques. Un reformage ultérieur des disques durs a conduit à se priver d'éléments de preuve utiles.

La connaissance des incidents informatiques permet au service du FSD de réagir et de formuler des conseils de gestion des incidents.

**

Ces quelques exemples sont illustratifs de menaces liées à l'utilisation de l'outil informatique, elles n'ont malheureusement pas prétention à l'exhaustivité. La vigilance reste de mise, avec l'appui des services informatiques de proximité et des responsables de la sécurité des systèmes d'information au CNRS. ■

Joseph.Illand[à]cnrs-dir.fr

»»» suite de la page 1

► Sensibilité et travaux ne portant pas sur des questions de défense

En fait il faut se garder d'identifier uniquement « sensibilité » et « défense ».

Certains travaux concernant la défense n'ont aucun caractère de sensibilité, alors qu'on peut trouver des sujets d'une grande sensibilité dans d'autres secteurs d'investigations des sciences humaines et sociales. Sans doute faut-il tenter une définition des informations « sensibles »

Ce sont les informations dont la compromission, l'altération, le détournement ou la destruction serait de nature à porter atteinte aux intérêts fondamentaux de l'État (défense nationale, patrimoine scientifique et technique), à des intérêts économiques ou industriels, ou à des personnes.

En d'autres termes, est « sensible » une donnée, une activité, une structure, une personne qui par une atteinte sous quelque forme qu'elle soit peut encourir un grave préjudice. Cela renvoie à une notion de menaces mais aussi de vulnérabilité et d'effet.

Point de risque sans menaces (au rang desquelles on rangera les menaces naturelles), et point de risque sans conséquence dommageable identifiable.

Il est classique de quantifier le risque par l'équation

$$R = P \times V \times E$$

(où R est le risque, P la probabilité d'occurrence de la menace, V le facteur de vulnérabilité et E l'effet induit par la réalisation de la menace).

La probabilité d'atteinte physique d'un chercheur en mission à l'étranger est d'autant plus grande que le pays est dangereux. La vulnérabilité quant à elle est fonction de l'in-souciance ou au contraire de l'état d'esprit de vigilance du missionnaire.

La problématique du portable du chercheur rempli d'informations sensibles (confidentielles) peut s'analyser de la même façon : l'effet est important voire catastrophique, la vulnérabilité peut être grande mais aussi très atténuée par des mesures d'attention, et plus encore par des solutions telles que le chiffrement de l'ordinateur.

La probabilité peut être fonction de l'intérêt de l'ennemi supposé à acquérir les données dans une attaque ciblée. Elle doit aussi intégrer la possibilité que l'ordinateur, pris lors d'un vol crapuleux ou même simplement perdu, pourra être marchandé pour atterrir *in fine* dans des mains beaucoup plus dangereuses.

Pour ce qui est de l'atteinte aux données, on rappelle que les trois cibles classiques du risque touchent l'intégrité, la disponibilité et la confidentialité.

L'atteinte à l'**intégrité** (modification du contenu) soulève des problèmes notamment de propriété intellectuelle qui mériteraient un développement particulier. L'atteinte à la **disponibilité** est elle-même cruciale lorsque des données, difficiles ou impossibles à reconstituer, sont irrémédiablement perdues, alors qu'aucune sauvegarde n'existe ou que les sauvegardes elles-mêmes ont été compromises. La **confidentialité** reste manifestement l'atteinte privilégiée.

Il est clair que travailler sur contrat avec le ministère de la défense sur le niveau moyen d'instruction des conscrits sous la troisième république, malgré un facteur V (vulnérabilité) probablement élevé, ne conduira pas à l'identification d'un risque majeur.

En revanche, certaines recherches sans nul lien avec le monde de la défense comportent de graves risques qui justifient une attention particulière des services de protection et une forte sensibilisation des acteurs correspondants.

Peut-on ainsi dresser une typologie des informations « sensibles » en SHS ?

On peut certainement distinguer une sensibilité par nature : certaines données à caractère personnel sont même d'une telle sensibilité que leur protection est assurée par des textes spécifiques. On peut retrouver de telles données dans les fichiers de personnels, dans les fichiers médicaux, mais aussi dans les travaux d'enquêtes menées par exemple par des sociologues.

Les risques liés à la cybersurveillance sont aussi à prendre en compte dans le sens de la protection des intérêts des individus. En ce sens, la gestion des traces de connexion informatique d'utilisateurs dans tout laboratoire, y compris en sciences sociales, doit faire l'objet d'un cadrage conforme aux procédures retenues par le CNRS en liaison avec la CNIL.

Les données de déplacements d'un chercheur se rendant dans un pays à risques sont éminemment confidentielles et doivent être protégées avec attention. C'est pourquoi le dispositif de suivi des agents en mission à l'étranger du CNRS (application SAME) est hautement protégé. On aura l'occasion de revenir sur cette question particulière dans un prochain bulletin.

La sensibilité peut aussi être liée à la finalité du recueil et du traitement de l'information¹.

Il est clair que tout sujet de recherche touchant à de graves intérêts divergents ou à des

conflits doit faire l'objet d'attention et intégrer les risques liés, qu'il s'agisse de divulgations non souhaitées ou de mises en cause du chercheur avec risques graves pour la personne. C'est notamment le cas pour des sujets tels que les nationalismes, les territorialités, le terrorisme, les religions, les sectes, les réseaux maffieux, les relations de pouvoirs, certains enquêtes sur la justice (des enquêtes de terrain sur les « crimes d'honneur » ou encore « les attentats suicides » sont à considérer comme pouvant faire courir des risques évènements à l'enquêteur).

Une sensibilité de situation est également perçue lorsque le contexte ou l'environnement géographique s'avèrent facteurs de risques. C'est ainsi que des laboratoires du CNRS du domaine SHS ont pu à une époque être classés ultra sensibles, du seul fait de leur emplacement géographique, alors que les thèmes de recherche étaient tout à fait anodins.

Au-delà de la caractérisation de la nature de l'information, le « degré » de sensibilité reste à apprécier, en fonction de nombreux critères dont le contexte, la préexistence de menaces identifiées, l'espérance de gain de l'ennemi, que celui-ci soit mû par l'argent, l'idéologie ou le simple nihilisme.

En l'occurrence, dans toute approche de sensibilité et de recherche de parades, la prise de conscience et le bon sens sont souvent les meilleurs alliés.

Il ne s'agit pas d'entrer dans un univers paranoïaque propre à inhiber toute recherche mais de savoir prendre, en situation de risques, les mesures indispensables à la protection des données et des personnes. Au CNRS, la mission du service du Fonctionnaire de Sécurité de Défense est justement de sensibiliser et de conseiller les chercheurs en ce sens. ■

joseph.illand[à]cnrs-dir.fr

SÉCURITÉ DE L'INFORMATION

Sujets traités : tout ce qui concerne la sécurité informatique. Gratuit.
Périodicité : 4 numéros par an.
Lectorat : toutes les formations CNRS.

Responsable de la publication :

Joseph Illand
Fonctionnaire de Sécurité de Défense
Centre national de la recherche scientifique
3, rue Michel-Ange, 75794 Paris cedex 16
Tél. : 01 44 96 41 88
Courriel : joseph.illand[à]cnrs-dir.fr
http://www.sg.cnrs.fr/fsd

Rédacteur en chef :

Joseph Illand
Fonctionnaire de Sécurité de Défense
Courriel : joseph.illand[à]cnrs-dir.fr

Impression : Bialec, Nancy (France) - D.L. n° 74480

ISSN 1257-8819

La reproduction totale ou partielle des articles est autorisée sous réserve de mention d'origine.

1. Se reporter dans ce bulletin à l'article d'Isabelle de Lamberterie.