www.jusletter.ch

Dr. Sylvain Métille

Les enseignements à tirer de la surveillance illicite de magistrats et fonctionnaires par un service informatique

Commentaire de l'affaire jurassienne du Pornogate

Des agents de l'Etat jurassien consultant des sites non-professionnels ont démissionné ou ont été sanctionnés administrativement. La surveillance informatique qui a mis à jour ces faits était pourtant illégale. Sylvain Métille commente la décision de la Commission cantonale à la protection des données et utilise cette affaire pour décrire la procédure à suivre dans un tel cas et surtout les mesures à prendre préalablement (sous forme de loi pour le secteur public et de directive interne pour le secteur privé).

Domaine(s) juridique(s): Délits contre l'honneur, la sphère secrète et privée; Contributions

Proposition de citation: Sylvain Métille, Les enseignements à tirer de la surveillance illicite de magistrats et fonctionnaires par un service informatique, in: Jusletter 3 septembre 2012

ISSN 1424-7410, www.jusletter.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77 Editions Weblaw

Table des Matières

I. L'affaire dite du Pornogate

1. La surveillance des magistrats et fonctionnaires

1.1 Des recherches préliminaires liées à la saturation du réseau

[Rz 1] Des lenteurs et des dysfonctionnements dans l'accès à Internet ont été constatés lors de la diffusion de la session du Parlement jurassien à l'automne 2008. Afin d'en déterminer la cause, le Service de l'informatique du canton du Jura (SDI) a procédé à une analyse technique des journaux d'accès à Internet, sur une période de 5 jours, week-end compris. Le SDI a alors découvert dans ces journaux d'accès les noms de sites pornographiques, dont il a considéré que certains pouvaient éventuellement contenir de la pornographie dure au sens de l'article 197 CP.

[Rz 2] Le SDI a choisi de ne pas transmettre l'information aux autorités judiciaires et policières compétentes pour mener une enquête pénale ou aux autorités administratives pour mener une enquête disciplinaire. Il a préféré continuer seul et étendre l'examen à une période d'un mois.

1.2 Une investigation menée par le SDI

[Rz 3] Au vu du volume important que représentaient les journaux d'accès à Internet de l'ensemble de l'administration durant cette période, le SDI a engagé les services d'une société privée hors canton pour établir la liste des sites pornographiques et les postes informatiques qui avaient accédé plus de cent fois à ces sites. Les adresses IP permettaient d'identifier le service et la plupart du temps le poste informatique utilisé. Des doutes subsistaient dans certains cas, par exemple si l'ordinateur avait été remplacé ou si la machine était accessible par plusieurs personnes.

[Rz 4] Assez rapidement, le SDI a cessé de chercher l'origine de la surcharge du réseau et le moyen de l'éviter pour se concentrer sur la recherche des utilisateurs qui avaient accédé à des sites jugés inappropriés par le SDI.

[Rz 5] Poursuivant son investigation, le SDI a par la suite contacté une à une les personnes connectées sur chacun des 56 postes concernés et leur a demandé par téléphone l'autorisation d'accéder au poste à distance. Pour obtenir l'accord (techniquement nécessaire) de l'utilisateur, le SDI a utilisé une ruse et a fait croire à la nécessité d'effectuer une opération de maintenance. Une fois l'accès obtenu par le SDI, l'entreprise privée est entrée en scène et a procédé à une recherche de mots-clés dans le fichier « index.dat » situé sur le disque dur de l'ordinateur. Elle a également relevé les identifiants de connexion et enregistré les preuves de visites des sites visés par cette enquête. La recherche ne s'est pas limitée aux sites pornographiques au sens pénal, mais des mots-clés plus larges comme « sex » ont été recherchés.

[Rz 6] Un rapport a finalement été établi par le SDI le 11 février 2009 avec une liste nominative. Aucune procédure administrative n'était ouverte à ce stade, mais plusieurs chefs de services et de département ont été informés de manière informelle. Le rapport a été transmis au Gouvernement qui en a pris connaissance lors de sa séance du 17 février 2009.

1.3 Des sanctions disciplinaires

[Rz 7] Le Gouvernement jurassien a ouvert les 17 et 24 février 2009 des enquêtes disciplinaires à l'encontre de 27 collaborateurs soupçonnés de consulter des sites non-professionnels et a nommé une commission d'enquête disciplinaire, alors que le Conseil de surveillance de la Magistrature a ouvert une enquête disciplinaire à l'encontre de deux magistrats le 27 février 2009. La commission d'enquête a informé les personnes concernées le 5 mars 2009 et a procédé à des saisies de disques durs.

[Rz 8] Au final, neuf personnes ont été transférées dans une classe de traitement inférieure, onze ont reçu un blâme ou une amende inférieure à 300.- et trois personnes ont spontanément démissionné. Aucune infraction pénale n'a été constatée ou dénoncée.

[Rz 9] Trois personnes seulement ont saisi la Commission cantonale à la Protection des données à caractère personnel (CPD) : le secrétaire du Parlement, le procureur général et un inspecteur principal adjoint à la police cantonale. Si les deux premiers ont préalablement démissionné de leur poste, le troisième a recouru au tribunal cantonal contre la sanction prononcée par le Gouvernement. La procédure a été suspendue jusqu'à droit connu sur la procédure devant la CPD et vient de reprendre. Apparemment, aucune des personnes

concernées n'a dénoncé pénalement le SDI ou ses employés pour infraction contre le domaine secret ou privé.

1.4 D'une surcharge de réseau à la recherche d'auteurs d'infractions

[Rz 10] En revoyant le déroulement des faits, on constate un changement évident du but de la récolte de données par le SDI, que l'on peut qualifier dans le jargon du droit de la protection des données et de la sphère privée de changement de finalité. De manière générale, un tel changement est problématique, car il signifie que les données ne sont plus utilisées dans le but pour lequel elles ont été récoltées. Aussi l'autorisation initiale de traiter ces données (le consentement de la personne concernée, une loi ou éventuellement un motif justificatif spécifique) n'est plus utilisable et il faut une nouvelle autorisation en fonction du nouveau but fixé.

[Rz 11] Pour atteindre le but initial, des mesures moins attentatoires à la sphère privée étaient envisageables : un blocage de l'accès à certains sites considérés comme problématiques ou une simple limitation du débit de téléchargement depuis les sites trop gourmands en bande passante aurait suffi à résoudre le problème. Un tel blocage aurait respecté l'exigence de proportionnalité et pouvait être mis en place sans grande difficulté.

[Rz 12] D'une démarche initiale visant à localiser la source d'un gros volume de données, indépendamment de leur contenu, le SDI s'est retrouvé dans un rôle d'enquêteur cherchant à prouver la commission d'infractions pénales. Une telle démarche n'était pas de la compétence du SDI, mais des autorités de poursuite pénales. A la décharge du SDI, on relèvera que la situation juridique n'était pas des plus claires. Le fait que les informations étaient sensibles et que parmi les agents de l'Etat se trouvaient des membres de la justice, du ministère public et de la police était aussi de nature à rendre la tâche du SDI difficile et à le pousser à agir seul.

[Rz 13] Le rapport du SDI n'a démontré aucune infraction pénale liée à la consultation des sites Internet, mais des violations administratives. On se retrouve donc à la fin avec une récolte de données utilisées dans un troisième but : il ne s'agit ni de la fluidité du réseau ni de la poursuite d'infractions pénales, mais du respect des prescriptions techniques et administratives encadrant l'activité des agents de l'Etat.

2. La protection des données

2.1 La décision de la Commission cantonale de la protection des données à caractère personnel

[Rz 14] La CPD a rendu une décision le 29 mars 2012[1] longue de 49 pages (!) dans laquelle elle constate premièrement qu'un certain nombre d'analyses sont intervenues avant l'ouverture d'enquêtes disciplinaires et sans instruction des autorités compétentes pour ouvrir une telle enquête. Il s'agit en particulier des analyses des fichiers journaux d'accès Internet et index.dat des postes informatiques des membres de la fonction publique, en vue d'identifier les postes informatiques ou leurs utilisateurs à l'origine de connexions à des sites Internet à caractère pornographique, ainsi que le nom des sites consultés, le nombre et les horaires de connexions de ceux-ci. Cela constitue un traitement de données illicite, le SDI n'étant pas compétent pour décider de placer les membres de la fonction publique sous surveillance informatique.

[Rz 15] Deuxièmement, la CPD retient que la recherche et l'enregistrement des preuves effectués au moyen d'une prise en main à distance des postes informatiques des membres de la fonction publique suspectés d'utilisation abusive d'Internet, en cachant la nature exacte de cette opération à l'utilisateur ou en prétextant un motif de télémaintenance, contrevenaient au principe de la bonne foi et étaient donc illicites au sens de la Loi jurassienne sur la protection des données[2].

[Rz 16] Troisièmement, la CPD ordonne la destruction par le SDI de toutes les données collectées au moyen de la prise en main à distance des postes informatiques des membres de la fonction publique, et de manière générale interdit toute collecte de données qui serait effectuée au moyen d'une prise en main à distance des postes informatiques des membres de la fonction publique, sans qu'il soit indiqué à la personne concernée la finalité exacte du traitement de données.

[Rz 17] Finalement, la CPD interdit toute analyse des fichiers journaux ou des fichiers index.dat pouvant être mise en relation avec des postes informatiques des membres de la fonction publique ou leurs adresses IP qui n'interviendrait pas dans le cadre d'une procédure de mutation, de résiliation ou de suspension au sens de la Loi sur le personnel de l'Etat, respectivement d'une procédure disciplinaire au sens de la Loi d'organisation judiciaire s'agissant de magistrats de l'ordre judiciaire, et sur instruction de l'autorité compétente pour mener de telles procédures.

2.2 Quelques questions que la CPD n'a pas examinées

[Rz 18] Les tous premiers actes d'enquête du SDI ne respectaient déjà pas le principe de proportionnalité. Si le but était effectivement de vérifier les problèmes de bande passante constatés lors de la diffusion de la session du Parlement le mercredi, cela ne justifiait pas de consulter les journaux d'accès du week-end. Lorsque le SDI constate que des sites non-professionnels sont consultés, il ne doit pas étendre la durée de surveillance. Si le but est de limiter l'accès à des sites non-justifiés qui limitent les ressources de l'administration,

[1] Disponible à l'adresse http://goo.gl/h35Mf

[2] Loi jurassienne sur la protection des données à caractère personnel du 15 mai 1986 (LPD-JU, RSJU 170.41).

il peut alors simplement bloquer l'accès à ces sites. Si le but est de découvrir des infractions pénales, le SDI ne doit pas remplacer la police et la justice, mais dénoncer les faits constatés à l'autorité compétente pour ordonner la poursuite de la surveillance.

[Rz 19] Le président de la CPD a été consulté à fin janvier 2009 par le SDI pour donner son appréciation. Il a considéré que le processus utilisé par le SDI était conforme, sous réserve de la prétendue maintenance qui violerait le principe de la bonne foi. Il semble pourtant que déjà à ce stade le SDI avait dépassé ses compétences et que le président de la CPD aurait pu ouvrir une procédure d'office, voire transmettre une dénonciation pénale au ministère public.

[Rz 20] La CPD n'a pas n'ont plus abordé la question de la transmission de données personnelles par le SDI à une entreprise privée, alors que l'on peut se demander si les conditions légales étaient remplies et si les mesures nécessaires ont été prises pour s'assurer de la confidentialité de ces données.

[Rz 21] La CPD aurait également pu se demander si une surveillance globale de tous les fonctionnaires durant plusieurs jours était vraiment proportionnée, d'autant plus que la surveillance a porté sur le contenu des communications et non seulement sur le volume. Il en est de même de la surveillance d'une personne précise en raison de manquements administratifs (aucune infraction pénale n'a été constatée).

3. Les conséquences

[Rz 22] Le scandale du Watergate avait conduit à de longues auditions devant le Sénat américain et à l'ouverture par le Congrès de la procédure de destitution du chef de l'État (impeachment), amenant finalement le Président Nixon à la démission. Dans le Jura la situation est bien différente. Trois employés de l'Etat ont démissionné, quelques jours après que l'affaire a été annoncée publiquement. Deux d'entre eux figurent parmi ceux qui ont porté l'affaire avec succès devant la CPD. La condamnation populaire sur la base de faits non avérés aura été plus forte que le respect de la présomption d'innocence et de la procédure.

[Rz 23] Le Parlement a refusé à une courte majorité l'ouverture d'une enquête parlementaire et apparemment aucune procédure judiciaire ou administrative n'a été ouverte contre les responsables de la surveillance informatique. Il y aurait pourtant eu de quoi envisager une violation des articles 179ss CP (infractions contre le domaine privé), ce qui aurait pu amener à une condamnation pénale ceux qui ont initié, conduit ou encore validé les mesures illégales. Des sanctions administratives auraient également pu être envisagées.

[Rz 24] L'affaire du Pornogate démontre aussi le manque d'informations juridiques compréhensibles auquel un service technique peut faire face et la difficulté à gérer correctement des données sensibles. Le seul moyen de gérer de telles situations est de les avoir anticipées et nous allons voir quels enseignements peuvent être tirés, sur la manière dont ce cas aurait dû être résolu et sur les mesures que devraient prendre les employeurs du domaine privé et public.

II. La procédure à suivre

1. Dans le cas du Pornogate

1.1 Par le SDI

[Rz 25] Le SDI devait chercher à identifier les problèmes d'accès en se contentant au maximum de détecter les problèmes de volume de trafic et en bloquant les sites posant problèmes. S'il avait des doutes sur la commission d'infractions pénales ou de comportements susceptibles d'être sanctionnés administrativement, il devait en référer à l'autorité compétente. Il pouvait éventuellement suggérer des démarches techniques ou proposer son assistance. En aucun cas en revanche il ne devait prendre l'initiative de conduire des mesures de surveillance.

[Rz 26] L'autorité disciplinaire, voire le SDI, pouvait transmettre les dossiers aux autorités de poursuite pénale, qui auraient eu, elles, le droit et les moyens d'investiguer.

1.2 Par l'autorité de surveillance

[Rz 27] Le Conseil de la magistrature et le Gouvernement devaient ouvrir des procédures disciplinaires à l'encontre des personnes suspectées pour violation des devoirs de services. Alors seulement des mesures d'enquête telles que les analyses effectuées spontanément par le SDI auraient pu être ordonnées. L'autorité de surveillance pouvait également dénoncer les fonctionnaires aux autorités pénales et coordonner leurs actes d'enquête. La surveillance des communications Internet dans le cadre d'une enquête pénale doit en outre recueillir l'autorisation du Tribunal des mesures de contrainte (précédemment la Chambre d'accusation).

[Rz 28] Parallèlement l'autorité de surveillance aurait dû sanctionner, voire dénoncer pénalement, les auteurs de mesures de surveillance illicites.

2. Dans le secteur public en général

2.1 L'exigence d'une loi formelle pour traiter des données

[Rz 29] Dans ce cadre, les lois cantonales de protection des données sont généralement assez similaires à la Loi fédérale sur la protection des données (LPD)[3] et les mêmes principes s'appliquent. C'est en particulier le cas de l'exigence d'une

[3] Loi fédérale du 19 juin 1992 sur la protection des données (LPD, RS 235.1).

base légale pour traiter des données personnelles figurant à l'article 17 LPD. Une base légale formelle est exigée pour que les données sensibles ou les profils de personnalité puissent être traités. Des exceptions sont possibles par exemple si l'accomplissement d'une tâche clairement définie dans une loi au sens formel l'exige absolument ou si la personne concernée a donné son consentement express ou a rendu ses données accessibles à tout un chacun et ne s'est pas opposée formellement au traitement.

[Rz 30] Le traitement de données relatives aux communications et au contenu de communications, de même que la conservation de fichiers journaux (log files) nécessitent également une base légale formelle. Au niveau fédéral, les nouveaux articles 57i ss de la Loi sur l'organisation du gouvernement et de l'administration (LOGA)[4] entrés en vigueur le 1er avril 2012 jouent désormais ce rôle. Ils cèdent le pas aux lois spéciales comme le Code de procédure pénale[5], qui s'appliquerait en cas d'enquête pénale.

2.2 L'exemple des articles 57i ss LOGA

[Rz 31] Dans un souci de prévisibilité, une loi formelle doit indiquer quelles données sont traitées par qui et dans quel but. Au-delà de ce principe général, cela signifie également que les mesures de surveillance des employés et du réseau informatique doivent être prévues. La LOGA distingue ainsi différents types d'analyse : analyse ne se rapportant pas aux personnes (art. 57m), analyse non nominale se rapportant aux personnes (art. 57n) et analyse nominale se rapportant aux personnes (art. 57o).

[Rz 32] L'analyse non nominale se rapportant aux personnes concerne les cas d'analyse par sondage dans le but de contrôler l'utilisation de l'infrastructure électronique ou de contrôler le temps de travail du personnel.

[Rz 33] Une analyse en rapport avec des personnes et de manière nominale peut avoir lieu pour analyser les perturbations de l'infrastructure électronique, ainsi qu'y remédier ou parer aux menaces concrètes qu'elle subit, pour fournir des prestations indispensables, pour saisir les prestations effectuées et les facturer ; et pour contrôler le temps de travail de personnes déterminées. Une telle analyse peut aussi servir à élucider un soupçon concret d'utilisation abusive ou poursuivre un cas d'utilisation abusive, mais dans ce cas la personne doit être informée par écrit préalablement à l'analyse.

2.3 Les compétences du service informatique et de l'autorité disciplinaire

[Rz 34] La répartition des compétences entre les différents organes doit être clairement établie. Les procédures disciplinaires seront traitées par l'autorité compétente, après ouverture d'une procédure en bonne et due forme, alors que les infractions pénales seront traitées exclusivement par les autorités judiciaires.

[Rz 35] Quant au service informatique, ses compétences doivent être définies précisément. En reprenant les distinctions proposées par la LOGA, le service informatique pourrait par exemple procéder à des analyses ne se rapportant pas aux personnes ou des analyses non nominales.

[Rz 36] Si le service informatique souhaite procéder à l'analyse de données nominales en cas de soupçon d'abus, il doit soit informer la personne concernée préalablement, soit transmettre le dossier à l'autorité disciplinaire, qui pourra alors ouvrir une procédure et procéder aux mesures de surveillance nécessaires. Il revient encore au service informatique de tenir à jour la liste de l'état du parc informatique et d'être en mesure d'identifier les adresses IP des machines et leurs utilisateurs.

3. Dans le secteur privé en général

[Rz 37] La situation est un peu différente en droit privé où l'exigence de la base légale est remplacée par la recherche du consentement de la personne concernée. L'employeur privé peut en outre faire valoir des motifs justificatifs au sens de l'article 13 LPD, contrairement à l'Etat. Ces motifs justificatifs permettent, en cas de soupçons d'infractions pénales ou d'atteinte grave aux intérêts de l'entreprise, de procéder à une surveillance même si l'employeur n'a pas informé le personnel spécifiquement ou globalement (par un règlement de surveillance par exemple).

[Rz 38] Le Préposé fédéral à la protection des données et à la transparence (PFPDT) a publié plusieurs guides consacrés au traitement des données personnelles dans le secteur du travail en général[6] et plus spécifiquement à la question de la surveillance d'Internet et du courrier électronique sur le lieu de travail[7]. La doctrine a eu l'occasion de confirmer et développer ces principes[8].

[Rz 39] L'article 26 de l'Ordonnance 3 relative à la loi sur le

---

[4] Loi fédérale du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (LOGA, RS 172.010).

[5] Code de procédure pénale suisse du 5 octobre 2007 (CPP, RS 321.0)

[6] PFPDT, Guide pour le traitement des données personnelles dans le secteur du travail (traitement par des personnes privées) du 24 mai 2011, disponible à l'adresse : http://www.edoeb.admin.ch/dokumentation/00445/00472/00535/index.html?lang=fr.

[7] PFPDT, Guide relatif à la surveillance de l'utilisation d'internet et du courrier électronique au lieu de travail (à l'intention des administrations publiques et de l'industrie privée) du 22 janvier 2010, disponible à l'adresse : http://www.edoeb.admin.ch/dokumentation/00445/00472/00532/index.html?lang=fr.

[8] Voir par exemple Philippe Meier, Protection des données, fondements, principes généraux et droit privé, Berne 2011, pp 685-722 ; Giordano Costa, Internet-und E-Mail-Überwachung am Arbeitsplatz, in : Jusletter 9 janvier 2012 ; Alexandre Staeger / Philippe Meier, Surveillance vidéo sur le lieu de travail – quelques enseignements tirés de l'Arrêt du TF 9C_785/2010 du 10 juin 2011 in : Jusletter 16 avril 2012.

travail[9] interdit d'utiliser des systèmes de surveillance ou de contrôle destinés à surveiller le comportement des travailleurs à leur poste de travail. Les systèmes de surveillance ou de contrôle qui sont nécessaires pour d'autres raisons sont néanmoins licites, s'ils sont conçus et disposés de façon à ne pas porter atteinte à la santé et à la liberté de mouvement des travailleurs.

[Rz 40] En matière de surveillance des moyens de communication, la surveillance doit en plus répondre à des intérêts légitimes de l'employeur, respecter les principes de la LPD et les employés doivent avoir été informés préalablement.

[Rz 41] Il est donc très vivement recommandé à tout employeur d'élaborer un règlement sur l'utilisation des moyens de communications au travail. La pratique montre que tant les employés que les employeurs ne sont pas au clair sur ce qui est autorisé et à quelles conditions[10]. Un tel règlement permet de prendre les mesures de surveillance précitées, mais devrait être conçu de manière plus large afin d'anticiper les éventuels abus en définissant les règles et les limites applicables au sein de l'entreprise. Il faudra en particulier régler les questions liées à l'utilisation de moyens personnels (« bring your one device », sécurité, responsabilité, frais), l'utilisation à titre privée de l'infrastructure de l'employeur (en particulier téléphone et adresse électronique professionnels) ainsi que l'accès à Internet, l'utilisation des réseaux sociaux, de blogs, et autres services en ligne comme Twitter. En fonction de l'activité de l'entreprise et de la position occupée par les travailleurs, la présence sur les réseaux sociaux pourrait être interdite ou recommandée mais avec un cadre précis. Cette présence pourrait être à titre privée ou au nom de l'entreprise. Il est judicieux de prévoir déjà à ce stade qui est titulaire des comptes Twitter, Facebook ou Google+, qui les contrôle et en est responsable, et ce qu'il en advient en cas de cessation des rapports de travail. De telles règles sont également bienvenues pour la messagerie électronique.

III. Conclusion

[Rz 42] L'affaire du Pornogate a sanctionné les fonctionnaires consultant des sites non-professionnels, mais pas ceux qui ont mis en place des mesures de surveillance illégales. Un service informatique, même s'il a accès à un grand nombre de données pour des raisons techniques, ne jouit pas pour autant d'une immunité.

[Rz 43] Cette affaire a montré le manque de sensibilité à ces questions et le besoin de clarifier et adapter le cadre légal. Pour les entreprises privées, il s'agit d'une forte incitation à développer de bonnes pratiques sous forme de règlements ou directives précisant les usages admis et les usages proscrits sur le lieu de travail, ainsi que les compétences des différents intervenants, les mesures de surveillance admissibles et les sanctions.

Sylvain Métille est docteur en droit et collabore au sein de l'Etude id est avocats à Lausanne (idest.pro), où il s'intéresse principalement aux questions liées à la protection des données, aux mesures de surveillance, aux télécommunications et aux technologies. Il a publié «Mesures techniques de surveillance et respect des droits fondamentaux» (éd. Helbing Lichtenhahn, 2011) et commente régulièrement des sujets actuels sur son blog «Nouvelles technologies et droit» (ntdroit.wordpress.com).

---

* * *

[9] Ordonnance 3 du 18 août 1993 relative à la loi sur le travail (OLT 3, RS 822.113).

[10] PFPDT, 19ème rapport d'activités 2011/2012, pp 79-80.