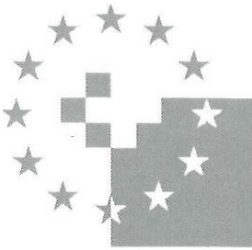

Astrid Epiney/Tobias Fasnacht/Gaëtan Blaser (Hrsg./éds)

30

Instrumente zur Umsetzung des Rechts auf informationelle Selbstbestimmung

Instruments de mise en œuvre du droit à l'autodétermination informationnelle

UNIVERSITAS FRIBURGENSIS

Schulthess §

Jurisprudence actuelle en matière de protection des données

Surveillance, infiltration et transmission de données à un tiers : quelques atteintes à la sphère privée qui ont occupé récemment les tribunaux

Sylvain Métille

Sommaire

A. Introduction

Si l'année 2012 a vu la publication officielle de l'arrêt du Tribunal fédéral dans l'affaire *Google Street View* (ATF 138 II 346) et sa traduction en fran-

çais (JdT 2013 I pp 71),[1] notre attention se portera plutôt sur des décisions rendues par des instances judiciaires cantonales et fédérales, qui ont toutes rappelé les principes cardinaux de la protection des données, comme l'exigence de la base légale (pour mettre en place une surveillance des fonctionnaires et magistrats),[2] l'accès sans condition à ses propres données (même si les informations obtenues peuvent servir dans une procédure judiciaire ultérieure),[3] et l'application de normes spécifiques de la LPP (qui interdisent de transmettre des données à l'employeur).[4]

Début 2013, ce sont les conditions de surveillance des employés qui ont été rappelées, avec la précision que les preuves recueillies illégalement ne peuvent pas justifier un licenciement abusif.[5] Deux autres décisions ont encore été rendues sur la base du droit de la personnalité, mais en lien étroit avec la protection des données. Elles ont précisé l'obligation pour un hébergeur de retirer le contenu de l'article d'un blog portant atteinte à la personnalité, même s'il n'est pas l'auteur du contenu[6] et l'illicéité de l'infiltration de membres d'une association.[7]

Les atteintes à la personnalité et à la sphère privée peuvent prendre autant de formes que la vie quotidienne présente de situations différentes. Les tribunaux ont eu à juger d'atteintes exprimées au travers d'un blog, d'un extrait LPP, de la surveillance informatique ou encore de l'infiltration d'une association. Pour les spécialistes, ces différentes affaires n'ont rien de révolutionnaire et elles ne font que confirmer ce que disait déjà la loi. Elles n'en sont pas inutiles pour autant et elles démontrent le chemin qui doit encore être fait pour que le droit soit correctement appliqué.

Premièrement, la défense de la sphère privée n'est pas un acquis et les violations sont nombreuses. Si ces principes, pourtant consacrés, étaient admis et largement appliqués, les plus hautes instances judiciaires n'auraient pas besoin de les répéter. Le faible nombre de cas portés devant les tribunaux ne tient pas à une situation idéale mais aux embûches, notamment financières, pour faire valoir les droits garantis par la LPD. Deuxièmement, la protection des données ne se limite pas à la LPD. De nombreuses autres lois doivent être prises en compte et appliquées. La protection des données ne doit pas être traitée comme une branche en tant que telle ou comme un domaine juridique fermé, mais au contraire la protection de la sphère privée et

1 Cette décision a déjà été abondamment commentée.
2 Voir titre B, ci-dessous.
3 Voir titre D, ci-dessous.
4 Voir titre C, B, ci-dessous.
5 Voir titres F, et G, ci-dessous.
6 Voir titre E, ci-dessous.
7 Voir titre H, B, ci-dessous.

de la personnalité doit être appréhendée de manière horizontale et ses principes appliqués dans tous les domaines du droit et toutes les situations. Il n'y a plus guère de domaine qui puisse prétendre ne pas être concerné. Troisièmement, les décisions récentes confirment le travail de sensibilisation et de formation qui doit encore être effectué. Rares sont les violations de la LPD qui sont commises dans le but de nuire. Il s'agit le plus souvent d'une méconnaissance des limites ou des possibilités d'agir conformément à la loi, ou d'un manque de sensibilité au fait qu'un certain comportement, même s'il est banal ou coutumier, peut porter atteinte aux droits de la personnalité.

B. Décision de la Commission cantonale jurassienne de la protection des données à caractère personnel du 29 mars 2012 (« pornogate »)[8]

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 des ordinateurs utilisés par les juges et magistrats, sur une période de 5 jours, week-end compris. Le SDI a 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.

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 et a préféré continuer seul et étendre l'examen à une période d'un mois. Il a ensuite engagé les services d'une société privée pour établir la liste des sites pornographiques et les postes informatiques qui avaient accédé plus de cent fois à ces sites. 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 a procédé à la recherche de certains mots-clés dans le fichier « index.dat » situé sur le disque dur de l'ordinateur.

[8] Voir également *Sylvain Métille*, Les enseignements à tirer de la surveillance illicite de magistrats et fonctionnaires par un service informatique, in : Jusletter, 3.9.2012.

Un rapport est établi et transmis au Gouvernement alors qu'aucune procédure administrative n'a encore été ouverte. Le Gouvernement a finalement ouvert des enquêtes disciplinaires à l'encontre de 27 collaborateurs et le Conseil de surveillance de la Magistrature à l'encontre de deux magistrats. 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. Trois personnes seulement ont saisi la Commission cantonale à la Protection des données à caractère personnel (CPD) et aucune des personnes concernées n'a dénoncé pénalement le SDI ou ses employés pour infraction contre le domaine secret ou privé.

La CPD a rendu une décision le 29 mars 2012 dans laquelle elle constate d'abord 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.

La CPD retient ensuite 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.

Par conséquent, elle 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.

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.

C. Arrêt du Tribunal administratif fédéral du 10 avril 2012, Préposé fédéral à la protection des données et à la transparence PFPDT c. AXA Fondation de prévoyance professionnelle Winterthur et Département fédéral de l'intérieur DFI[9]

Le Préposé fédéral à la protection des données (PFPDT) ayant eu connaissance que AXA Fondation de prévoyance professionnelle Winterthur (ci-après AXA) transmettait les certificats de prévoyance par le bais de l'employeur avec la seule mention « confidentielle », il a considéré que la protection des données des employés assurés n'était pas respectée et a émis une recommandation à l'encontre d'AXA. Celle-ci a rejeté la recommandation et le PFPDT a demandé au Département fédéral de l'Intérieur (DFI) de rendre une décision ordonnant à AXA de se conformer à la recommandation. Le DFI a refusé de suivre l'avis du PFPDT, qui a donc recouru au Tribunal administratif fédéral.

Les art. 85a ss LPP contiennent des règles spéciales plus strictes en matière de traitement et de communication des données dans le domaine de la prévoyance professionnelle obligatoire et doivent être appliquées en premier lieu, la LPD demeurant applicable à titre supplétif. L'art. 86 LPP prévoit en particulier une obligation de garder le secret à l'égard des tiers.

L'employeur doit être considéré comme un tiers au sens de l'art. 86 LPP, même s'il a des obligations en matière de prévoyance professionnelle et que des informations peuvent lui être transmises. Doivent être considérés comme tiers tous ceux pour qui la transmission des données personnelles n'est pas requise pour l'exécution de leurs devoirs.

Si l'absence de séparation entre la fonction d'employeur et d'organe peut conduire à la connaissance d'informations qui ne sont pas nécessaires, ces informations ne devraient pas être utilisées et communiquées au sein de l'entreprise. L'institution de prévoyance devrait être organisée de manière à ce que le représentant de l'employeur n'ait pas accès aux informations contenues dans le certificat personnel et qu'il ne reçoive pas de données lui

[9] ATAF 2012/14 ; voir également *Stephan Fuhrer*, Pensionskassenausweise, in : HAVE 2012, 298 ss.

permettant de calculer d'autres éléments que ceux liés à son obligation de cotisation.

L'employé doit avoir la possibilité d'obtenir des informations sans que l'employeur n'en soit informé. Le montant de la prestation de libre passage, l'utilisation d'un montant pour l'accession à la propriété ou le versement à un ex-conjoint sont des informations sans utilité pour les obligations de l'employeur, que rien ne justifie de lui transmettre.

Ni la LPD ni les art. 85b ss LPP ne prévoient d'exception à l'obligation de garder le secret vis-à-vis des tiers au sens de l'art. 86 LPP. Le TAF a encore rappelé que conformément à l'article 8 CEDH, l'Etat a non seulement une obligation négative, mais également une obligation positive de protéger de manière efficace et concrète les données personnelles contre un accès indu. La possibilité de déposer une plainte ou un recours est insuffisante à cet égard.

Le Tribunal administratif fédéral a donc suivi le PFPDT et a considéré que la mention « confidentielle » ne protégeait pas contre la copie ou la prise de connaissance par l'employeur. Si AXA souhaite transmettre les certificats de prévoyance par le biais de l'employeur, elle doit prendre les mesures nécessaires, par exemple en utilisant des enveloppes individuelles fermées. Ces mesures sont simples à mettre en place et n'engendrent pas de coûts disproportionnés.

D. Arrêt du Tribunal fédéral du 17 avril 2012, Banque X (Credit Suisse) c. A. Y. et B. Y.[10]

A. et B. possédaient des comptes bancaires auprès du Credit Suisse et reprochent à cet établissement bancaire d'avoir procédé à des opérations sans en avoir été instruit par A. et B., opérations qui se sont soldées par des pertes. Ils ont demandé à la banque de leur remettre la documentation interne les concernant, y compris leurs profils et objectifs de placement.

Si le traitement de données personnelles n'était pas remis en cause, l'application de la LPD était contestée par la banque car l'art. 2 al. 2 lit. c LPD prévoit qu'elle ne s'applique pas aux procédures pendantes, notamment civiles. Le Tribunal fédéral a rappelé qu'une procédure civile n'est pendante qu'une fois que le tribunal (y compris un juge de paix) a été saisi et qu'il n'y a pas de raison d'étendre la notion de procédure pendante à l'activité préalable consistant à rassembler des informations et des preuves et à évaluer les

[10] ATF 138 III 425; *Nicolas Bracher*, Das Auskunftsrecht nach DSG – Inhalt und Einschränkung im Vorfeld eines Zivilprozesses, in: SJZ 2013, 45 ss.

chances d'un procès. Ce n'est pas non plus parce que le code de procédure permet, à certaines conditions, d'obtenir des preuves à futur que la LPD s'efface et qu'une telle demande doit être déposée.

Le droit d'accès de l'art. 8 LPD est inconditionnel et celui qui l'exerce n'a pas à donner de motifs. L'abus de droit est réservé. Pourrait constituer un abus de droit une utilisation contraire au but de la protection des données (par exemple pour éviter de devoir payer des frais qui seraient normalement dus), un exercice chicanier sans intérêt au résultat, ou une demande dont le but est exclusivement d'obtenir des informations et des preuves sur la partie adverse qui ne pourraient pas être obtenues autrement.

Dans le cas d'espèce, les clients avaient un intérêt à accéder à leurs données et à en contrôler la véracité. Que ce contrôle soit aussi effectué dans l'optique d'un éventuel procès en dommages et intérêts ne rend pas encore la demande abusive.

Le maître du fichier peut également faire valoir des intérêts prépondérants pour refuser ou restreindre la communication des renseignements demandés. Sont considérés comme des intérêts prépondérants la crainte d'un espionnage économique, le risque d'atteinte aux droits de la personnalité du maître du fichier ou des intérêts financiers (par exemple le besoin de recourir à un tri onéreux d'archives). En revanche, les règles de procédure qui permettraient de refuser de transmettre des documents ne sont pas applicables car aucune procédure n'est pendante et ce n'est pas le rôle de la LPD d'offrir une protection similaire.

Le tribunal n'a pas retenu d'intérêts prépondérants permettant à la banque de s'opposer, en particulier parce qu'il n'y avait pas de preuve d'une « fishing expedition » interdite et que les données demandées concernaient les données personnelles liées à la gestion de leurs comptes bancaires, données qui peuvent aussi être obtenues en application des règles sur le mandat même si le mandataire risque de faire ensuite l'objet d'une action en dommages et intérêts (reddition de comptes, art. 400 CO).

Une banque, comme n'importe quel maître du fichier, peut ainsi être contrainte de livrer des informations internes (à l'exception des notes personnelles prises par les employés) aux clients victimes de mauvais placements, y compris si ceux-ci envisagent d'engager ensuite contre lui une action civile.

E. Arrêt du Tribunal fédéral du 14 janvier 2013, X. (« Tribune de Genève ») contre A et B[11]

Cette affaire a pour origine l'article « Banque cantonale : nous exigeons toute la vérité! » publié par le président du MCG Eric Stauffer sur son blog hébergé par la Tribune de Genève, article dans lequel il accuse un ancien responsable de la Banque Cantonale de Genève d'avoir contribué à la déconfiture de cette banque.

La personne visée par l'article avait obtenu des mesures provisoires ordonnant à la Tribune de Genève (l'hébergeur) et à Eric Stauffer (l'auteur) de retirer l'article en question et leur interdisant de le publier. Ces mesures provisoires ont ensuite été confirmées par le Tribunal de première instance de Genève qui a constaté le caractère illicite de l'atteinte. Les frais et dépens ont été mis à la charge de l'auteur pour ¾ et de l'hébergeur pour ¼.

L'hébergeur a recouru contre la décision, contestant avoir la légitimation passive dans les actions défensives du droit de la personnalité. Il fait valoir le fonctionnement des blogs, la législation et la jurisprudence étrangère en la matière, et soutient que l'hébergeur ne peut pas « participer » à une éventuelle atteinte à la personnalité et qu'il ne doit pas « répondre du contenu des blogs qu'il héberge ».

Le Tribunal fédéral est d'un avis différent et rappelle que si l'auteur est à l'origine de la lésion aux intérêts personnels, celui qui lui a fourni l'espace Internet sur lequel il a pu créer son blog a permis la diffusion du billet incriminé auprès du public et d'un large cercle de lecteurs. S'il n'est pas l'auteur de l'atteinte, il a contribué à son développement et y a participé au sens de l'art. 28 al. 1 CC.

Le Tribunal souligne ensuite qu'il n'est pas question de contrôler constamment le contenu de tous les blogs hébergés, ni de dommages-intérêts ou en réparation du tort moral. Dans le cas d'une action en réparation du dommage, il faut une faute. Alors qu'ici il s'agit d'une action en cessation de l'atteinte, qui peut être dirigée contre toute personne qui y participe. L'hébergeur d'un blog devra supprimer un article qui porte atteinte à l'honneur comme le responsable d'un panneau d'affichage pourra être obligé de retirer une affiche, même s'il n'en est pas l'auteur.

Cette décision ne crée pas un devoir de contrôle de l'hébergeur, mais elle confirme que celui qui participe à une atteinte à la personnalité et qui est

[11] TF, arrêt du 14.1.2013, 5A_792/201; voir également *Alexander Kernen*, Volle Verantwortlichkeit des Host Providers für persönlichkeitsverletzende Handlungen seines Kunden, in : Jusletter, 4.3.2013 ; *Sébastien Fanti*, Arrêt du Tribunal fédéral du 14 janvier 2013 (5A_792/2011), in : Medialex 2013, 78 ss.

techniquement en mesure de la faire cesser doit donner suite à une telle requête. La victime peut choisir librement contre qui elle souhaite diriger sa requête (auteur, hébergeur, éventuellement fournisseur d'accès, ...). Le Tribunal conclut qu'il n'appartient pas à la justice, mais au législateur, de réparer les « graves conséquences » pour Internet et pour les hébergeurs de blogs auxquelles pourrait conduire l'application du droit actuel.

On cerne mal les « graves conséquences » pour Internet de cette décision qui concerne le cas d'une demande de suppression d'un contenu portant atteinte à la personnalité et qui ne s'applique pas à n'importe quel contenu illicite. L'art. 28 CC prévoit en effet que celui qui subit une atteinte illicite à sa personnalité peut agir en justice pour sa protection contre toute personne qui y participe, et non seulement contre l'auteur comme c'est le cas pour d'autres contenus illégaux. Peut-être en irait-il différemment si le Tribunal avait considéré que les fournisseurs d'accès participaient également à l'atteinte.

Comme la LPD renvoie aux art. 28 ss CC s'agissant des actions concernant la protection de la personnalité (art. 15 al. 1 LPD), cette jurisprudence s'applique également en cas d'atteinte basée sur la LPD. Soulignons encore que la victime n'est pas obligée de s'être adressée préalablement au site avant de saisir la justice mais qu'il lui est recommandé de le faire, comme il est recommandé au site de donner déjà suite à la requête de la victime sans attendre une décision judiciaire (sauf s'il y a des doutes sérieux sur le fait que la publication constitue une atteinte), cela en particulier pour éviter des frais judiciaires.

F. Arrêt du Tribunal fédéral du 17 janvier 2013, Consortium de la protection civile Z. c. X.[12]

Le Consortium de la protection civile soupçonnait un de ses employés d'utiliser à des fins personnelles les ressources informatiques mises à sa disposition. Le Consortium a installé pendant plus de trois mois et à l'insu de l'employé un logiciel espion qui a révélé que l'employé avait consacré une part considérable de son temps de travail à des activités privées ou au moins étrangères à son activité professionnelle.

Grâce à des copies d'écran, effectuées à intervalles réguliers, le contrôle a également permis de prendre connaissance du contenu des pages Internet consultées et des messages électroniques, y compris des informations privées comme des opérations e-banking en relation avec la fonction de

[12]ATF 139 II 7 ; voir également SJ 2013 I pp 177 ss.

membre du conseil municipal de l'intéressé. En se basant sur les résultats de la surveillance informatique, l'employeur a résilié les rapports de travail avec effet immédiat.

Le Tribunal fédéral a retenu que l'utilisation clandestine d'un logiciel espion était illicite et constituait une mesure prohibée par l'art. 26 al. 1 de l'Ordonnance 3 du 18 août 1993 relative à la loi sur le travail (OLT 3), en tant qu'elle est assimilable à un système de contrôle destiné essentiellement à surveiller le comportement d'un travailleur. Cette mesure était au surplus disproportionnée.

L'employeur a un intérêt légitime à lutter contre les abus et peut y parvenir à l'aide de moyens moins invasifs, comme le blocage à titre préventif de certains sites Internet, ou une analyse conformément aux modalités indiquées par le Préposé fédéral à la protection des données et à la transparence.

Vu la possibilité pour l'employeur de recourir à des moyens légaux pour défendre ses intérêts, le Tribunal fédéral a considéré que la surveillance était illégale et que les preuves recueillies l'étaient également, ce qui ne permettait pas de fonder le licenciement immédiat.

G. Arrêt de la Cour administrative du Tribunal cantonal jurassien du 25 février 2013, X. c. le Gouvernement de la République et Canton du Jura[13]

La Cour devait se prononcer sur le recours d'un fonctionnaire qui avait été déclassé suite à la consultation de sites non professionnels (affaire du « pornogate » voir B, ci-dessus). Elle a retenu que la surveillance n'avait pas été autorisée ni prévue par la loi et que les preuves recueillies étaient illicites. Procédant à une pesée d'intérêts, la Cour estime que l'intérêt du recourant à bénéficier d'une instruction conforme au droit, respectant la protection de sa sphère privée prime sur l'intérêt de l'autorité disciplinaire à l'établissement de la vérité, et cela d'autant plus vu que l'atteinte à la sphère privée est importante alors que l'usage abusif d'Internet est en général une faute d'importance mineure (dans le cas d'espèce une faute moyenne).

Les preuves illicites sont donc inutilisables, de même que les déclarations du recourant qui ont suivi les analyses illicites. Faute de preuves exploitables, le Gouvernement ne pouvait constater un usage abusif d'Internet de la part du recourant, que ce soit durant ses heures de travail ou en dehors. Partant, il ne pouvait prononcer une quelconque sanction disciplinaire à son encontre.

[13] ADM 92/2009.

H. Jugement du Tribunal civil d'arrondissement de Lausanne du 25 janvier 2013, B. et consorts c. N. et consorts (« Nestlégate »)

« Sara Meylan » a été chargée par son employeur Securitas SA d'infiltrer la section vaudoise d'Attac-Suisse dont certains membres préparaient un livre sur Nestlé. Les rapports étaient destinés à Nestlé SA. Les membres concernés et l'association ont agi contre les deux entreprises précitées en protection de leur personnalité sur la base de l'art. 28 CC et de la LPD. Le Tribunal devait essentiellement décider si le fait de participer à des réunions sous une fausse identité et d'obtenir ainsi des informations était contraire au droit civil. Des infractions pénales n'avaient pas pu être établies.

Le juge a écarté l'application de la LPD, en particulier de l'art. 8 garantissant le droit d'accès, aux motifs que l'existence d'un fichier (art. 3 lit. g LPD) n'était pas démontré et que les rapports transmis ne contenaient pas de données sensibles (art. 3 lit. c LPD) ou de profils de la personnalité (art. 3 lit. d LPD). Ce raccourci est probablement un peu rapide car la LPD s'applique à tout traitement de données personnelles, même si certaines dispositions ne visent que le maître du fichier (droit d'accès, devoir d'information en cas de collecte de données sensibles ou de profils de la personnalité, déclaration de fichiers). En revanche, les principes (art. 4 ss LPD) s'appliquent à toute personne qui traite des données. Le résultat n'aurait cependant pas été très différent puisque la LPD renvoie aux art. 28 ss CC pour les actions concernant la protection de la personnalité.

Le Tribunal a retenu qu'en se présentant sous une fausse identité, « Sara Meylan » a trompé intentionnellement les demandeurs et transgressé le principe de la bonne foi. Elle a eu accès à des faits et des données qui se rapportent à la sphère privée des demandeurs et que ceux-ci n'auraient, selon toute vraisemblance, pas voulu partager avec elle s'ils avaient connu sa véritable identité et mission. Entrer en contact avec des militants associatifs, adhérer à leur association en leur donnant à penser que l'on est des leurs afin de gagner leur confiance, en dissimulant sa mission et son but réel est un procédé déloyal qui comporte une atteinte à la liberté personnelle (et à la sphère privée) en privant les victimes du choix de partager ou non de telles informations avec la personne infiltrée, qui agit avec dissimulation.

Il n'y a pas de motifs justificatifs à l'atteinte car les tâches de sécurité par l'acquisition préventive d'informations sont en principe clairement étatiques et il n'y avait en l'espèce pas de risque sérieux ou grave. Le tribunal n'a pas non plus retenu de consentement des victimes. Le consentement doit être éclairé et requiert d'être informé pour se décider en conséquence. Les demandeurs n'avaient pas conscience d'être infiltrés. Les rapports au sein de

l'association et du groupe de travail étaient fondés sur la confiance et une certaine communauté d'idées. Si les demandeurs avaient su que « Sara Meylan » agissait pour le compte des défenderesses, ils ne l'auraient pas admise dans le groupe de travail. L'atteinte illicite à la personnalité est donc admise par le tribunal, qui accorde également une indemnité à titre de réparation morale.