Vie privée : un enjeu politique et économique

Alors que, pour la première fois, un accord du gouvernement aborde frontalement la question du respect de la vie privée comme un des enjeux de cette législature, force est de constater que, dans une société de plus en plus technologique, l'équilibre entre ses velléités sécuritaires et ses bonnes intentions va être difficile à trouver.

Combat contre les violences domestiques et secret professionnel **une relation tendue**

Aude Meulemeester

Tant sur le plan international que national, on observe depuis plusieurs années une évolution législative qui tend à reconnaitre la violence domestique comme une violence d'ordre public et non plus seulement comme relevant de la sphère privée. Cette volonté s'inscrit dans le postulat que les violences domestiques qui accablent le plus souvent des femmes, sont le symptôme d'une société où persistent des attitudes patriarcales et machistes en profonde contradiction avec les valeurs sur lesquelles la société contemporaine doit se construire. Si ces violences interviennent dans le cadre de la vie privée des victimes, les réponses qui doivent y être apportées sont de l'ordre et de l'intérêt public général.

On ne peut que se réjouir de cette évolution car elle a également pour conséquence d'obliger les pouvoirs publics à mettre en œuvre de grandes campagnes de sensibilisation sur le sujet et d'ainsi s'inscrire en priorité dans un axe préventif.

Par ailleurs, l'ouverture publique de ce phénomène pose des questions quant à l'aide qui doit être apportée aux victimes. Combattre les violences domestiques ne peut bénéficier du même statut de débat public lorsqu'il s'agit d'aide et d'assistance aux victimes. Les violences domestiques interviennent dans le cadre de la vie privée de la victime, certes. Mais les combattre et protéger les victimes en reconnaissant cette violence comme une atteinte à

l'ordre public signifie-t-il que la victime ne dispose plus de vie privée ?

Droit de parole

Depuis le 1er aout 2014, la convention d'Istanbul est entrée en vigueur. Cette convention du Conseil de l'Europe, ratifiée par la Belgique en septembre 2012, fixe des normes globales pour prévenir et combattre la violence à l'égard des femmes. Dans ce cadre, nous retrouvons notamment l'article 28 de la convention précisant qu'il convient à l'État signataire de faciliter le cadre légal permettant le signalement des cas de violences à l'égard des femmes par les professionnels composant les services sociaux spécialisés en la matière.

En droit belge, cette facilité a vu le jour via la récente modification de l'article 458 bis du code pénal en matière de droit de parole des intervenants professionnels. En effet, depuis le 1er mars 2013, les professionnels qui, par état ou par fonction, sont soumis au secret professionnel (article 458 du code pénal) disposent désormais d'un droit de parole et donc de signalement, élargi aux cas de violences domestiques.

Cet élargissement du droit de parole qui, dans le cas des violences domestiques, prendrait la forme d'un avertissement du procureur du Roi par un professionnel soumis au secret professionnel, peut-il être compris comme une forme de violation de la vie privée de la victime ? Et si c'est le cas, est-ce souhaitable dans le cadre de l'aide et de l'assistance aux victimes ?

Pour y répondre nous devons revenir sur plusieurs éléments touchant notamment à la fonction du secret professionnel et du droit de parole.

Un signalement à double tranchant

Le secret professionnel garantit la confidentialité dans le cadre d'une relation d'aide entre un particulier et un professionnel tel qu'un avocat, un travailleur social, un médecin. Cette confidentialité est essentielle puisqu'elle permettra l'instauration d'une relation de confiance entre le professionnel et la personne aidée. Rappelons à ce titre également que le secret professionnel s'inscrit dans une disposition pénale (article 458 du code pénal), ce qui démontre une volonté du législateur à inscrire la relation de confiance comme une notion d'intérêt général sans laquelle la société ne peut fonctionner.

Cette obligation de taire les informations auxquelles un professionnel a accès dans l'exercice de sa fonction connait pourtant quelques exceptions, et c'est le cas de l'article 458 bis du code pénal qui encadre un droit de parole. Ce droit doit être entendu comme une faculté et non comme une obligation « d'informer le procureur du Roi soit, lorsqu'il existe un *danger grave et imminent* [c'est nous qui soulignons] pour l'intégrité physique ou mentale du mineur ou sur la personne vulnérable visée, et qu'elle n'est pas en mesure, seule ou avec l'aide d'un tiers, de protéger cette intégrité, [...] ». En effet, certaines situations de violences domestiques pourraient amener un professionnel aidant une victime à ne pouvoir envisager que ce signalement afin de remplir sa mission d'aide. Néanmoins, il est fondamental qi'il soit relatif à un danger réel, imminent et grave, qu'il relève d'une appréciation au cas par cas (non systématique) et uniquement après que toutes les autres tentatives d'aide aient été envisagées, au risque de porter une atteinte irréversible à la relation de confiance nécessaire à toute relation d'aide entre un professionnel et une personne vulnérable. Et si cette relation de confiance est brisée, comment encore envisager que nous nous trouvions dans une relation d'aide agissant pour la protection de la victime ?

Surveillance de masse et lanceurs d'alerte après Snowden

Pierre-Arnaud Perrouty

Il y aura un avant et un après Snowden. Non que la surveillance électronique, la collecte et le stockage massifs de données soient des phénomènes nouveaux. L'affaire Echelon, du nom de ce programme d'écoutes mondiales conduit par les États-Unis et leurs alliés des Five Eyes, l'affaire Swift qui concernait les données bancaires européennes ou encore les accords de transfert de données des passagers aériens (Passenger Name Record) avaient suscités des débats importants en Europe depuis les années 1990. En Belgique, la révélation par la presse en 1998 de l'existence de la base de données nationale générale (BNG), où 1,6 million de Belges étaient fichés, avait mis à jour de graves carences d'encadrement et de contrôle. Mais ces questions ont pris une tout autre dimension avec les documents divulgués par Edward Snowden en juin 2013 : ils révèlent une surveillance et une collecte de données menées par les États-Unis à une échelle sans précédent.

Contrôle global

À travers des programmes comme PRISM, la NSA (National Security Agency) a atteint une capacité de surveillance quasi totale. Dans son témoignage devant le Parlement européen en mars 2014, Edward Snowden a affirmé que dans le cadre de ses fonctions, il pouvait avoir accès à toutes les communications privées de n'importe quel citoyen ordinaire dand le monde. Des milliards d'appels téléphoniques, fax, courriels et sms transitent ainsi chaque jour sur les serveurs de la NSA. Certaines de ces données sont conservées pour des périodes plus ou moins longues, voire indéfiniment. Les déplacements d'une personne peuvent également être reconstitués de manière très précise, notamment grâce à l'identifiant MAC (Media Access Control) unique émis par un téléphone portable, un ordinateur ou une tablette.

La NSA défend ses programmes en invoquant la nécessité de protéger les Américains et leurs alliés du terrorisme et en rejetant l'accusation de violation de la vie privée, argüant du fait que les données sont simplement collectées et non consultées. Ces arguments ne tiennent pas. D'abord, parce que jamais les services américains n'ont été en mesure de prouver qu'une collecte de renseignement indistincte à une telle échelle a permis d'empêcher une attaque terroriste. Ensuite, parce que les agissements de la NSA violent allègrement les lois américaines, européennes et belges de protection de la vie privée : c'est bien la collecte qui constitue l'infraction, indépendamment de savoir si les données sont effectivement consultées ou pas. S'il était permis de collecter sans consulter, pourquoi ne pas installer une caméra de surveillance dans toutes les maisons ? En raison des multiples infractions au droit à la vie privée que ces programmes comportent, la Ligue des droits de l'Homme, la Fédération internationale des ligues des droits de l'Homme (FIDH) et quelques personnes individuelles ont déposé une plainte pénale contre x à Bruxelles en novembre 2013.

Protéger les lanceurs d'alerte
L'affaire Snowden a également montré la nécessité de protéger les lanceurs d'alerte des foudres des gouvernements ou de leur employeur. À la frontière de la liberté d'expression et de la désobéissance civile, ces personnes prennent des risques sérieux en dénonçant une situation qui porte atteinte à l'intérêt général. Or les dispositifs légaux de protection sont généralement limités (dans le cadre de dénonciations fiscales par exemple) et épars, quand ils ne sont pas tout simplement inexistants. Dans une recommandation du 30 avril 2014, le Comité des ministres du Conseil de l'Europe invite les États membres à adopter un « cadre normatif, institutionnel et judiciaire pour protéger les personnes qui, dans le cadre de leurs relations de travail, font des signalements ou révèlent des informations concernant des menaces ou un préjudice pour l'intérêt général ». La définition de l'intérêt général doit au moins inclure les violations des droits fondamentaux ainsi que les risques pour la sécurité publique, la santé et l'environnement. Point intéressant, un droit à l'erreur est reconnu au lanceur d'alerte — la protection lui reste acquise même s'il a commis une erreur d'appréciation des faits ou si la menace ne s'est pas matérialisée — pour autant qu'il ait eu « des motifs raisonnables de croire » en la véracité de cette menace.

Les révélations successives de ces dernières années attestent de violations répétées et massives du droit à la vie privée. Il est dès lors hautement nécessaire de renforcer à la fois les règles légales qui encadrent ce type d'activités et les mécanismes de contrôle démocratique par des organes indépendants. Mais l'histoire montre que les agences de surveillance ne s'embarrassent guère du respect des lois. Il est d'ailleurs plus que probable qu'un certain nombre de programmes secrets de surveillance soient toujours en cours. C'est sans doute là le principal enseignement des révélations d'Edward Snowden : l'urgence et la gravité interdisent d'attendre que la solution vienne de l'État. La meilleure manière de nous protéger efficacement à court terme est de généraliser l'usage du cryptage pour toutes les communications. Ce qui n'empêcherait pas les agences spécialisées d'intercepter ni de décoder le contenu de certains messages ciblés, mais rendrait impossible une surveillance généralisée à un cout supportable.

Vers un droit à l'oubli numérique

François Danieli

Ce n'est ni un secret ni un scoop, nos informations personnelles circulent à travers la mondiale : des photos, des commentaires, laissés par l'internaute lui-même ou par un tiers à son propos, sur un blog, sur un forum ou à la suite d'un article de presse. Accéder à ces informations est désormais facilité par les moteurs de recherche et par leur référencement de pages web : en « googelisant » son nom, on aura un aperçu de sa « notoriété » sur le Net.

Depuis 1998, si l'on invoque des raisons sérieuses et légitimes tenant à sa situation particulière, chacun peut faire usage de son droit d'opposition et s'adresser au

responsable du traitement pour mettre fin au traitement de données personnelles. Une démarche qui s'entreprend sans trop de difficulté dans l'environnement *offline*..., mais qui se complique lorsqu'il s'agit de stopper la diffusion de données personnelles reprises à foison sur différents sites internet.

Depuis l'arrêt de la Cour de justice de l'Union européenne du 13 mai 2014, « lorsque, à la suite d'une recherche effectuée à partir du nom d'une personne, la liste de résultats affiche un lien vers une page web qui contient des informations sur la personne en question, la personne concernée peut s'adresser directement [au moteur de recherche] ou, lorsque celui-ci ne donne pas suite à sa demande, saisir les autorités compétentes pour obtenir, sous certaines conditions, la suppression de ce lien de la liste de résultats ». Faisant face à plus de 90 000 requêtes en deux mois et demi, Google se plie aux exigences de la jurisprudence européenne.

Oubli partiel

Trois importants bémols néanmoins : d'une part, une telle requête acceptée par Google aura certes pour effet de supprimer le référencement..., mais pas d'effacer les données personnelles à la source ! Pour cela, l'internaute devra compléter la requête adressée à Google par un droit d'opposition exercé auprès du site responsable de la publication. D'autre part, une telle requête acceptée par Google aura pour effet de supprimer le référencement sur les serveurs européens du moteur de recherche. Ce qui signifie qu'en « googelisan »t son nom sur la version américaine ou canadienne, les données personnelles apparaissent encore.

Par ailleurs, Google informe l'internaute que « certains résultats peuvent avoir été supprimés conformément à la loi européenne sur la protection des données ». Or, en comparant les résultats dans les différentes versions du moteur de recherche (.be, .com, .ca), on peut aisément identifier l'internaute qui a exercé son droit à l'oubli... lequel pourrait subir l'effet Streisand (effet pervers où la victime encourage malgré elle l'exposition d'une publication en tentant d'en empêcher la divulgation). Le Groupe 29, organe consultatif composé des autorités de protection des données des vingt-huit États membres de l'UE, travaille actuellement sur des lignes directrices afin d'encadrer le traitement des requêtes par les moteurs de recherche, tout en assurant la cohérence et la mise en œuvre uniforme de la décision de justice européenne

En plus de la jurisprudence, il faut également noter que le projet de règlement général sur la protection des données, qui se négocie actuellement au sein du Conseil européen, bétonne le droit à l'oubli dans un texte de loi : plusieurs conditions et modalités y sont reprises afin que la personne concernée puisse obtenir la cessation de la diffusion de ses données personnelles.

Tant le contrôleur européen à la protection des données que la Commission vie privée ont salué l'ambition d'une telle disposition, mais ils épinglent aussi, entre autres, le manque de clarté et les difficultés pratiques de sa mise en œuvre. Dans le cadre du processus législatif, le Parlement européen a quelque peu amendé le projet et il reste aux trois instances, Commission, Conseil, Parlement (à savoir, le trilogue) à trouver un consensus en vue d'une adoption finale du texte.

Article référencé

Lorsqu'il est fait état de données personnelles dans un article de presse, l'exercice du droit à l'oubli s'avère délicat dans la mesure où les données étaient exactes lorsqu'elles ont été publiées, et que le droit à l'information constitue précisément le travail du journaliste. C'est ce qu'illustre le cas délicat d'un ancien militant d'extrême droite qui voudrait

faire table rase de son passé car ses accointances politiques bloquaient ses perspectives d'emploi.

Dans ce genre de cas, le recours au droit de réponse pourrait être envisagé de manière plus systématique. Car, à l'instar de Charles Baudelaire qui revendiquait le droit de se contredire, l'internaute a le droit d'apporter, avec la même portée médiatique, un éclairage actuel à une situation ancienne qui le concerne.

Cela ne peut toutefois pas faire oublier la responsabilité qu'endosse l'internaute lui-même. Il perd la maitrise du contenu lorsqu'il publie un commentaire ou une photo : n'importe qui peut en enregistrer une copie et la republier à nouveau. Et lorsque cet internaute s'engage politiquement ou médiatiquement, il s'agit aussi pour lui d'assumer ses actes.

Rétention de données **un recours contre des mesures disproportionnées**

Raphaël Gellert

En novembre 2013, la Ligue des droits de l'Homme s'est associée à la Liga voor Mensenrechten et à la NURPA (Net Users' Rights Protection Association) pour déposer un recours en annulation devant la Cour constitutionnelle contre la loi sur la conservation des données de communication — la loi « data retention ». Cette loi et son arrêté d'exécution transposent en droit belge la directive européenne de rétention des données (2006/54/CE).

Cette directive oblige les opérateurs de télécommunication et les fournisseurs d'accès à internet à conserver les données des communications des usagers pour une durée allant de six mois à deux ans au motif de lutter contre la criminalité « grave ».

De même que l'adoption de cette directive n'a pas fait l'objet d'un réel débat de fond vu l'émotion qui prévalait après les attentats de Londres et Madrid, la loi belge a été adoptée dans l'urgence durant l'été 2013. Le délai de transposition de la directive étant dépassé, le Parlement a, sur demande du gouvernement, suivi une procédure d'urgence.

La loi belge prévoit donc la conservation de toutes ces données pour une période d'un an, extensible à deux dans certains cas. Elles doivent être accessibles de manière illimitée aux autorités compétentes et transmises à ces dernières sur simple demande de leur part.

Des métadonnées fort bavardes

Les données de communication, plus communément appelées « métadonnées », désignent toute une série de données liées de près ou de loin aux communications. Dans le cadre de communications « classiques », il s'agit par exemple des durée, heure, date de l'appel ou encore de l'emplacement des terminaux. Il s'agit également des données de trafic internet (adresse IP d'un ordinateur) ou de l'emplacement GPS d'un téléphone portable (et ses déplacements).

Bien que ces métadonnées ne révèlent pas le contenu des communications, leur

regroupement et leur analyse ne sont pas anodins : elles permettent d'avoir une idée du contenu de la communication ainsi que d'autres détails privés entourant cette dernière. Ces observations ne sont pas neuves : la Cour européenne des droits de l'homme avait déjà eu l'occasion de les exprimer en 1984 dans le cadre de l'arrêt *Malone*.

C'est ainsi que le recours a fait valoir plusieurs violations de droits et libertés fondamentaux.

Présomption de culpabilité et chilling effect

Ce qui choque avant tout, c'est le caractère disproportionné de la mesure dès lors qu'il n'y a pas de discrétion ou de jugement possible en fonction des cas d'espèce. Les opérateurs doivent conserver les données en toutes circonstances. Ce manque de proportionnalité fait peser de graves risques sur la vie privée des citoyens, mais également sur leur liberté d'expression (les gens ne vont-ils pas s'autocensurer s'ils savent que leurs communications sont analysées — le fameux « chilling effect » ?), sur leurs libertés de réunion et d'association, mais également sur le secret professionnel et/ou des sources. Ce manque de proportionnalité est d'autant plus choquant que jusqu'à présent l'efficacité de ce type de mesure n'a toujours pas été démontrée !

En outre, la facilité avec laquelle ces informations sont transmises aux autorités met à mal la présomption d'innocence, qui est partie intégrante du droit à un procès équitable.

Ce recours a été l'occasion d'une importante campagne de sensibilisation qui a vu la création d'un site y dédié : www.stopdataretention.be. Outre des explications relatives au recours et à la problématique de façon plus générale, cette plateforme a permis à plusieurs personnalités du monde socioculturel belge de soutenir la campagne (Thomas Gunzig, Eva Brems, Pierre Mertens, Lucas Belvaux…) et de partager leurs réflexions personnelles sur la montée de la surveillance en Europe. Le recours a également reçu le soutien d'un nombre important d'associations belges et européennes (EDRI, AKVorrat, Association des journalistes professionnels, Ordre des médecins…). Enfin, ce site a permis de mettre en œuvre un mécanisme de « crowdfunding » (financement participatif) aux fins de payer les avocats qui ont rédigé le recours. C'est une première en Belgique et également un succès dès lors que 114 % des fonds demandés ont été récoltés.

À l'heure d'écrire ces lignes, la Cour constitutionnelle ne s'est toujours pas prononcée. Il faut toutefois avoir à l'esprit que ce recours, loin d'être isolé, s'inscrit dans une vague de fond européenne. En effet, de nombreux recours ont été engagés, et souvent avec succès : c'est le cas en Allemagne, Bulgarie, République Tchèque, Roumanie, parmi d'autres. L'obstacle le plus sérieux à la rétention des données provient de la Cour de justice de l'Union européenne elle-même qui, en avril 2014, a déclaré la directive incompatible avec la Charte européenne des droits fondamentaux. Reste à espérer que les autorités politiques prendront la mesure de ces salutaires rappels de constitutionnalité.

Big Brother Awards **de l'importance de la vie privée au quotidien**

Bram Wets et Caroline Van Geest

La vie privée est un droit fondamental qui vise à protéger l'individu, mais aussi la société dans son ensemble. Sa protection constitue un droit « défensif » : en se plaçant entre le citoyen et les autorités publiques, le droit à la vie privée s'érige en garantie visant à limiter les possibilités d'intrusion d'autorités publiques ou d'entreprises privées (via le monitoring, le profilage ou le data mining) dans l'intimité des citoyens.

Au travers de la cérémonie des Big Brother Awards (BBA), la Liga voor Mensenrechten tente de sensibiliser les citoyens à l'importance de la vie privée en mettant sous le feu des projecteurs des candidats, choisis avec soin, qui violent ce droit. Et, ce faisant, de concrétiser un concept plutôt abstrait en illustrant ses effets dans le quotidien.

Voici les lauréats de l'année 2014 et les motivations de leur nomination.

Prix du public : Yves Liégeois
Ex-procureur général d'Anvers, pour ses déclarations concernant la nécessité de créer une base de données pour récolter les données ADN de tous les nouveau-nés en Belgique.

« M. Liégeois doit réaliser la portée de ses paroles. Dans sa fonction, il est essentiel de prendre en considération l'ensemble des droits fondamentaux. Si les hauts magistrats subordonnent le droit au respect de la vie privée aux intérêts qu'ils servent, nous n'aurons plus qu'à lancer une bouée de sauvetage pour préserver les droits fondamentaux. Lors des premiers débats sur le stockage de l'ADN, il y a dix ou vingt ans, l'on rencontrait davantage de réticence. Aujourd'hui il y a une tolérance grandissante vis-à-vis de propositions allant dans ce sens. Yves Liégeois nourrit ce changement de perspective et cultive une attitude apathique envers la vie privée. »

Prix du jury : le smartphone
Le jury d'experts des BBA a choisi le smartphone, cet « espion dans votre poche », comme lauréat de son prix en 2014. Où sommes-nous ? Que faisons-nous ? Avec qui sommes-nous en contact ? « Les smartphones enregistrent ces informations personnelles grâce à la nonchalance de l'utilisateur moyen qui ne voit dans les applications que le plaisir sans voir les risques concernant ses données personnelles. D'autant que, en matière de collecte de ces données, la devise "le plus sera le mieux" semble être devenue la norme. Un usage irréfléchi de la technologie et de ses attrayantes parures réduit la vie privée à une illusion. Chaque utilisateur contribue à cet état de fait. Le smartphone ouvre la voie à une société du contrôle. Une voie que nous construisons nous-mêmes. »

Les nominés des années précédentes sont consultables sur les sites de la Liga (www.mensenrechten.be) et de la LDH (www.liguedh.be).