

11 Septembre 2011 : bienvenue dans l'ère du soupçon

Au nom de la lutte antiterroriste, les Etats ont développé leur arsenal de prévention, sacrifiant au passage quelques droits fondamentaux. Petit récapitulatif des libertés qui ont disparu en France depuis le 11 septembre 2001.

Souvenez-vous. Il fut un temps où aucun militaire ne patrouillait, Famas en bandoulière, sur le parvis de Notre-Dame de Paris, un temps où vos e-mails avaient peu de risques d'être interceptés, où votre mine déconfitée sur le trajet du bureau n'était pas immortalisée chaque jour par des dizaines de caméras, une époque révolue où embarquer un flacon de shampoing à bord d'un avion était encore un geste anodin... C'était avant le 11 Septembre 2001.

Ce jour-là, lorsque les tours jumelles du World Trade Center tombent en poussière, la puissance symbolique des Etats-Unis est ébranlée, ainsi qu'une certaine idée de la liberté. Un mois plus tard, le Patriot Act est signé par George W. Bush. Au nom de la sécurité, quelques-unes des libertés fondamentales si chères aux Américains sont sacrifiées.

Au "pays de la liberté", une brèche vient de s'ouvrir. La plupart des Etats de la planète vont s'y engouffrer. En 2002, l'Union européenne emboîte le pas à l'administration Bush et produit une Décision cadre, qui incite les États membres à rapprocher leurs législations et établit des règles pour lutter contre la menace terroriste. La France, "initiée" aux attentats dès les années 80, s'était déjà engagée sur cette voie en adoptant une première loi antiterroriste en 1986. L'ère qui vient de s'ouvrir avec le 11-Septembre va accélérer cette dynamique, généralisant les mesures d'exception qui transformeront le paysage urbain et le code pénal.

"La guerre contre le terrorisme est une guerre à durée indéterminée contre un ennemi inconnu. Elle a permis d'introduire des lois d'exception dans le droit commun avec l'assentiment de la population, souligne Dan van Raemdonck, vice-président de la FIDH. On a banalisé la notion de contrôle. Les gens ont fini par accepter d'être tracés, contrôlés, sous prétexte qu'ils n'ont rien à cacher. On est entré dans l'ère du soupçon".

Petit tour d'horizon, non exhaustif, de quelques mesures "temporaires" qui ont durablement transformé votre quotidien en France :

• **L'armée dans la ville**

Des soldats patrouillant en rangers, l'arme au poing, dans les gares, les aéroports et les lieux touristiques. L'image est devenue banale. Elle est l'une des conséquences les plus visibles de la lutte contre le terrorisme, incarnée par le plan Vigipirate.

Conçu en 1978 alors que l'Europe était confrontée à une vague d'attentats, ce plan est entièrement repensé au lendemain du 11 septembre 2001 et sera maintenu en "niveau rouge" de façon continue à partir des attentats de Londres en 2005. La dernière version du plan, en vigueur depuis janvier 2007, est fondée sur un postulat clair : *"la menace terroriste doit désormais être considérée comme permanente"*. Vigipirate définit dès lors un socle de mesures appliquées en toutes circonstances, *"même en l'absence de signes précis de menaces"*.

Un millier de militaires des trois armées sont donc mobilisés en permanence pour appuyer les forces de gendarmerie et de police. Ils effectuent des patrouilles dans les gares, les aéroports, les ports, ainsi qu'un certain nombre de points sensibles comme les sites touristiques.

• **Internet sous surveillance**

La France, championne d'Europe de la surveillance des télécommunications ? C'est la Commission européenne qui le dit dans l'annexe d'un rapport datant d'avril 2011. En 2009, le "pays des droits de l'homme" a procédé à pas moins de 514 813 demandes d'accès aux "logs" (qui a téléphoné ou envoyé un mail à qui, quand, d'où, pendant combien de temps ?) conservées par les opérateurs de téléphonie fixe ou mobile, et les fournisseurs d'accès à Internet (FAI). La surveillance des télécommunications est encadrée au niveau communautaire. Mais à titre de comparaison, le pays le plus peuplé de l'UE, l'Allemagne, n'en a réalisé que 12 684, soit 42 fois moins que la France.

La volonté de surveiller les internautes se concrétise deux mois à peine après les attentats du 11-Septembre. Le 15 novembre 2001, le gouvernement Jospin modifie dans l'urgence son projet de loi relative à la sécurité quotidienne (LSQ), qui intègre divers moyens de lutte contre le terrorisme. Parmi eux, l'amendement 2, qui donnera naissance au fameux article 29, invite les fournisseurs d'accès à Internet à stocker pendant un an les "logs", c'est-à-dire les données de connexion de leurs abonnés.

En raison de son caractère exceptionnel, la mesure était censée durer jusqu'au 31 décembre 2003,

avant d'être éventuellement prolongée après un rapport d'évaluation. Mais un amendement déposé par Christian Estrosi au projet de Loi sur la sécurité intérieure (LSI), le 21 janvier 2003, la rendra définitive. Censée prévenir les menaces d'attentats, la surveillance des internautes est aujourd'hui totalement séparée de l'existence ou non d'une menace terroriste.

Un pas de plus est franchi en 2006 : la loi relative à la lutte contre le terrorisme (LCT) présentée par le ministre de l'intérieur, Nicolas Sarkozy, élargit l'obligation de conservation des "données de trafic" aux cybercafés. Elle permet en outre aux services antiterroristes de pouvoir y accéder en dehors de tout contrôle de l'autorité judiciaire, après avis d'une personnalité qualifiée *"placée auprès du ministre de l'intérieur"*. La surveillance d'Internet échappe désormais à toute procédure judiciaire pour se placer sous le contrôle direct de l'Etat.

• Les "fadettes"

Les communications téléphoniques ont subi le même traitement. Jusqu'à récemment, la communication par les opérateurs de téléphonie des factures détaillées (les "fadettes") de leurs clients aux services de police était encadrée par l'article 22 de la loi du 10 juillet 1991. Elle imposait notamment à la police une procédure d'autorisation, soit par un juge, soit par la Commission nationale de contrôle des interceptions de sécurité (CNCIS).

La loi contre le terrorisme de 2006 a tout changé : une simple réquisition permet désormais au parquet de consulter les "fadettes", sans que la CNCIS ait son mot à dire. Le texte prévoit en outre que ces "données de connexions" téléphoniques (qui appelle qui, où, quand, combien de temps) puissent être stockées pendant un an.

En conséquence, une *"avalanche de réquisitions s'abat, sans contrôle, sur les opérateurs"*, rapporte le *Canard enchaîné* du 7 septembre 2011. Interrogé par l'hebdomadaire, le porte-parole du CNCIS admet que ces demandes lui *"échappent totalement"*. *"Seul le législateur peut changer cet état de fait"*, ajoute-t-il. *"La loi de 1991 était jugée trop lente. On a accéléré les procédures dérogatoires au nom de l'antiterrorisme en maintenant un niveau minimum de légalité"*, souligne Christophe André, maître de conférence à Sciences Po et auteur de *Droit pénal spécial*. *"Le problème, c'est que ces procédures finissent par devenir la norme..."*

Peter Hustinx, contrôleur européen à la protection des données, n'est pas loin de partager cet avis. Qualifiant la conservation des "logs" d'*"atteinte massive à la vie privée"*, il estime que la directive européenne ayant généralisé cette surveillance des télécommunications constitue *"sans aucun doute l'instrument le plus préjudiciable au respect de la vie privée jamais adopté par l'Union européenne eu égard à son ampleur et au nombre de personnes qu'elle touche"*.

• Transport aérien

Sans surprise, le transport aérien a été le secteur le plus touché par les mesures de sécurité prises au lendemain du 11-Septembre. Et à chaque nouvelle tentative d'attentat, une nouvelle mesure de sécurité a été inventée :

- **Objets tranchants** : Les terroristes ayant détournés les quatre avions du 11-Septembre étaient armés de simples cutters. Couteaux, tondeuses, coupe-ongles et autres pinces à épiler sont donc désormais proscrits en cabine.

- **Chaussures** : Depuis l'attentat raté de Richard Reid, l'homme aux *"chaussures explosives"*, qui avait caché 250 grammes de Pentrite dans ses souliers sur un vol en décembre 2001, tout voyageur peut être amené à devoir se déchausser avant d'embarquer.

- **Liquides** : En août 2006, les autorités britanniques découvrent qu'un groupe d'hommes auraient eu l'intention de faire exploser des avions en dissimulant des explosifs liquides dans des biberons et des flacons de shampoing. L'embarquement en cabine de produits liquides sera dorénavant strictement encadré. Ils peuvent être emportés en cabine sous réserve d'être conditionnés dans des contenants ne dépassant pas 100 mL, et doivent ensuite être contenus dans des sacs plastiques transparents et fermés ne dépassant pas 20 cm sur 20 cm. Exit donc : parfum, crèmes solaires, dentifrice, mousse à raser, déodorant en spray, shampoing, sodas, alcools, confiture, produits laitiers...

Scanners corporels : En décembre 2009, un passager du vol Lagos-Amsterdam-Detroit tente de faire exploser un bloc de penthrite artisanale collée sur sa jambe. Plusieurs aéroports européens s'équipent aussitôt de scanners corporels. Le 6 juillet, le Parlement européen se prononce pour une utilisation très encadrée de cette technologie dans les aéroports. La Commission européenne doit proposer un projet d'ici à la fin de l'année pour que les Etats s'équipent avant la levée des restrictions sur les liquides fin 2013.

• Transfert de données

Après les attentats du 11-Septembre, l'administration Bush exige des compagnies européennes qu'elles lui transmettent les données personnelles de leurs passagers en partance vers les Etats-Unis. En cas de refus, ces dernières se verraient interdire d'atterrissage sur le territoire américain. Bruxelles négocie aussitôt un accord, que la cour de justice européenne s'empresse de juger illégal. Le superviseur européen pour la protection des données fait lui aussi part de ses *"doutes sérieux quant à [sa] compatibilité avec les droits fondamentaux"* en vigueur en Europe.

Ces fichiers, dits PNR (Personal Name Record), seront pourtant diffusables à toutes les agences associées au Département de la sécurité intérieure, comme la CIA et le FBI, qui pourront les conserver pendant quinze ans. Les données en question peuvent comprendre : votre nom, votre adresse, votre numéro de carte de crédit, ainsi que vos habitudes alimentaires...

• **Biométrie**

Les attentats de Londres en 2005 accélèrent la mise en oeuvre des projets internationaux de contrôle électronique des flux migratoires. Dès le lendemain de l'attaque, le gouvernement français annonce la généralisation progressive du visa biométrique. Un fichier comportant les données biométriques des passagers des aéroports (Parafes) est créé par un décret paru le 7 août 2007. Désormais, les voyageurs désireux d'éviter l'attente à la douane pourront communiquer librement les empreintes digitales de huit de leurs doigts, leur état civil, leur lieu de naissance, leur nationalité et leur adresse.

Dans un premier avis, la CNIL identifie des risques pour la protection des données. Elle dénonce également un *"champ d'application (...) potentiellement beaucoup plus large que la population officiellement visée"* puisqu'il n'est pas *"précisément défini dans le projet de décret"*. Dans un deuxième avis, elle estime qu'*"un sujet d'une telle importance devait passer devant le Parlement et nous n'avons pas obtenu les éléments qui permettent de justifier la création de cette banque de données"*. La CNIL note que la France va plus loin que la réglementation européenne, et juge que le dispositif français comporte *"des risques d'atteintes graves à la vie privée et aux libertés individuelles"*.

Ces réserves n'ont pas empêché une proposition de loi sur la mise en place d'une nouvelle carte d'identité biométrique. Si cette nouvelle carte d'identité est validée, elle devrait conduire à la constitution d'un vaste *"fichier central biométrique"* contenant toutes les données des titulaires, soit *"potentiellement 45 à 50 millions de personnes"*.

• **Vidéosurveillance**

Les caméras de vidéosurveillance ne datent pas d'hier, puisque l'installation des systèmes de vidéosurveillance dans les lieux ouverts au public est encadré par la loi du 21 janvier 1995. Mais avec l'augmentation de la menace terroriste, leur nombre a explosé depuis dix ans.

La loi contre le terrorisme de 2006 prévoit explicitement de *"développer la vidéosurveillance"* en facilitant l'implantation de caméras et l'enregistrement des images. L'adoption en 2010 de la loi de programmation pour la performance de la sécurité intérieure (*Loppsi 2*), va plus loin : l'Etat pourra désormais imposer aux municipalités l'installation de caméras dans trois cas : *"La prévention des actes de terrorisme, les sites d'importance vitale, ou les intérêts fondamentaux de la nation"*. L'Etat ambitionne de multiplier par trois le nombre de caméras, qui passeront de 20 000 à 60 000 d'ici à 2011, dont un millier à Paris.

Au fil des années, un changement sémantique s'opère : le gouvernement parle de *"vidéoprotection"*, un terme jugé moins agressif que celui de vidéosurveillance.

Le [collectif Démocratie et libertés](#) publie des cartes des implantations de caméras prévues d'ici fin 2011 à Paris.

• **La procédure pénale**

- **Mandat d'arrêt** : C'est la principale révolution juridique des dix dernières années. Le 11 juin 2002, une décision cadre de l'UE instaure le "mandat d'arrêt européen", qui sera transcrit en droit français en 2004. Ce mandat remplace une vieille tradition, la procédure d'extradition, en imposant à chaque autorité judiciaire nationale de reconnaître, *ipso facto*, la demande de remise d'une personne formulée par l'autorité judiciaire d'un autre Etat membre.

L'objectif affiché est la construction d'un espace de *"liberté, de sécurité et de justice"* au sein de l'UE, à travers une procédure plus simple, plus efficace et plus rapide. Pour ses détracteurs, loin d'unifier le droit au niveau de l'UE, il étend au contraire à toute l'UE le champ d'application des procédures d'exception et lois liberticides, spécifiques à chaque Etat membre.

Le cas d'Aurore Martin, une militante basque de 32 ans sous le coup d'un mandat d'arrêt européen émis par l'Espagne, illustre cette ambiguïté : cette jeune femme est poursuivie en Espagne pour *"participation*

à une organisation terroriste", en raison de son appartenance à Batasuna, une organisation politique interdite au-delà des Pyrénées. Le problème est le suivant : en France, une telle activité, qui relève du militantisme politique, est parfaitement licite, et Batasuna présente même des candidats aux élections locales. Aurore Martin pourrait donc être expulsée vers l'Espagne, et y être jugée, pour une activité relevant de l'exercice des libertés fondamentales en France.

Depuis 2004, 1 567 personnes ont été remises à la France, qui en a de son côté remis 1 950, dont 400 Français, précise le ministère de la justice.

- **Garde à vue** : En droit commun, la garde à vue dure 24 heures, renouvelable une fois sur autorisation du ministère public. Seuls les suspects de terrorisme "bénéficient" d'un régime spécial depuis 1986, avec une garde à vue de quatre jours maximum. Mais cette mesure dérogatoire va progressivement gagner du terrain, l'exception devenant peu à peu la norme. En 2004, la loi Perben II étend le régime de garde à vue des présumés "terroristes" à d'autres crimes, comme les affaires de délinquance organisée, de proxénétisme aggravé ou de trafic de stupéfiants. Depuis 2006, lorsqu'*"il existe un risque sérieux de l'imminence d'une action terroriste"*, la garde à vue des suspects peut a été portée à six jours.

"Le problème, c'est que toutes ces procédures dérogatoires introduites au nom de l'antiterrorisme ont fini par devenir la norme, souligne Christophe André, l'auteur de Droit pénal spécial. Puisqu'elles se révèlent efficaces contre ce monstre qu'est le terrorisme, elles sont donc employées pour combattre d'autres monstres et ont fini par contaminer l'ensemble du droit pénal".

Soren Seelow

Source : publié sur lemonde.fr - 10.09.2011

http://www.lemonde.fr/newsletter/en_ligne/afficher/1570252.html