NOUVELLES TECHNOLOGIES, DROIT ET SÉCURITÉ PUBLIQUE

Numérique, police et justice

Patrick Kineider

« En France, le citoyen s'en remet pour l'ordre public, la sécurité des personnes et des biens et la défense des droits individuels lorsqu'elle pose difficulté, aux acteurs démocratiques d'une part, sécuritaires civils, police et gendarmerie, d'autre part judiciaires, avec des rouages et développements complexes.

Jusqu'à la fin du XXe siècle, ces ensembles constituaient des organisations cloisonnées, réputées d'une compétence et d'une légitimité (en raison de la séparation des pouvoirs) à l'abri de toute critique de fond, malgré des moyens souvent empiriques. Avec l'avènement du numérique, on assiste à :
1/ une professionnalisation des enquêtes (police scientifique, ADN) ;
2/ un accès culturel de tous à de très nombreux éléments de droit ;
3/ une couverture médiatique de certains faits juridiques à caractère public, pouvant remettre en cause d'anciennes affaires et
4/ une extension de divers domaines de sécurité et de justice au domaine international et européen, en particulier depuis 2001 après les premiers attentats terroristes de type « islamiste », aux États-Unis, puis en Europe.
Cet article essaie de voir clair dans ces évolutions.

JURIDIQUE : PAPIER ET NUMÉRIQUE DEPUIS 1980

La France est un pays démocratique, très administré depuis plus de deux siècles : de l'État régalien découle la notion de « sécurité publique ». Il existe une inflation législative et un socle juridique impressionnant: pas moins de 80 codes (si l'on inclut les annexes), un Journal officiel de 15 000 pages annuelles.

Depuis la fin du 20e siècle, si la Constitution et les droits fondamentaux des citoyens restent dictés par des principes simples et de bon sens, le développement du numérique engendre, non seulement des progrès dans les procédures, mais aussi, une problématique importante vis-à-vis des droits d'expression et des libertés sur Internet. Concernant le droit d'auteur sur les documents et les œuvres, ainsi que le droit individuel à voir publiées ou utilisées des infos personnelles ou photos, des contentieux multiples surgissent avec les GAFA (sigle général des sociétés « Google, Apple, Amazon, Facebook »), souvent suivis de textes de lois nationaux ou surtout européens en la matière.

Le « Code pénal » et le « Code de Procédure Pénale » actuels

Code pénal

Créé à l'époque napoléonienne, le « Nouveau Code pénal » français de 1994 est surtout une refonte de type structurel du document original.
La partie législative définit la nature des peines, les infractions (contravention, délit, crime) contre : les personnes et les biens, les libertés institutionnelles, l'État. La partie réglementaire décline le type de peine appliquée. Les deux parties introduisent des notions modernes telles que : atteintes aux libertés publiques (expression, identité), atteintes à la confiance de l'État, à la sécurité publique, diffamation, discriminations diverses (origine, religion, race...), terrorisme, crimes contre l'humanité...

Code de procédure pénale

Les premières éditions remontent à la IVe République. Les modifications sont permanentes, les plus récentes s'attachent surtout aux améliorations de fond et de forme suivantes :

- accroître la liberté individuelle ;
- renforcer l'autorité des magistrats (juges et procureurs), des auxiliaires de justice, des avocats ;
- renforcer l'efficacité de la procédure pénale ;
- bien délimiter les domaines de compétence et les «actions des divers acteurs de police et de justice.

La Loi « PERBEN II » (2002 et 2004) et la Loi « LOPPSI II » (2011)

Loi PERBEN II et numérique

En 2004 est promulguée la « loi portant sur l'adaptation de la justice aux évolutions de la criminalité » dite « loi PERBEN II ».
Très générale, elle permet d'organiser les actions sécuritaires dans les affaires contentieuses. Ceci inclut les infiltrations et écoutes via des systèmes informatiques et de télécommunications, en cas de suspicion ou identification, des atteintes avérées ou potentielles à l'ordre public, en particulier dans le cas de cybercriminalité dite « organisée ».
Une conséquence de la loi PERBEN II : l'existence d'un « fichier des auteurs d'infractions sexuelles et violentes ».

Loi LOPPSI II et numérique

La Loi du 14 mars 2011, dite « d'orientation et de programmation pour la performance de la sécurité intérieure », est une évolution de la version « LOPPSI » de 2002. Outre la cybercriminalité et les fraudes informatiques, elle vise des infractions et délits généraux (sécurité routière, vols et cambriolages, sécurité privée).
La lutte contre la criminalité informatique a pour objectif général, la « traque » et la sanction de tous les sites « déviants » au sens de l'éthique, citons : usurpation d'identité, pédopornographie, escroqueries et trafics divers, immigration irrégulière, prosélytismes subversifs... Selon cette loi, la Police, sur autorisation du juge des libertés, peut utiliser tout moyen pour s'introduire dans des ordinateurs privés et en extraire toutes données illicites aux fins d'enquête.

Bien évidemment, les tenants de « droits maximaux » sur Internet, tels que « La Quadrature du Net », n'ont pas manqué de s'élever contre ce qu'ils considèrent comme une atteinte aux libertés fondamentales.

Pénétration des moyens informatiques dans le circuit judiciaire

Si la numérisation des tâches judiciaires paraît inévitable, compte tenu de la diversité et des finalités très diverses des gestes des acteurs (magistrats, avocats, justiciables...), les projets d'informatisation de la Justice deviennent rapidement de véritables « usines à gaz ». À noter qu'ils découlent bien souvent d'applications informatiques du type général « G(estion) E(lectronique) de D(ocuments) », couramment utilisées dans les entreprises et les administrations.

« Packweb »

La principale application existante dans l'Intranet judiciaire est le « Packweb » qui autorise au Bureau de la Direction des Services Judiciaires un partage de données sur un périmètre restreint. Elle facilite le suivi d'une affaire, mais ne permet pas de recherche plus élargie par mots-clefs. Pour imaginer des indexations pertinentes des fichiers à cet effet, il conviendrait de revoir la notion de dossier judiciaire.

Numérisation des dossiers des magistrats

C'est un projet RH destiné aux membres du CSM, et aux commissions d'avancement. Il nécessite un travail important de numérisation, et de définition des indexations.

Instruction assistée par ordinateur

Une centaine de magistrats utilisent cette application, assez ancienne et relativement performante, qui permet également une historisation des actes.

L'ENQUÊTE

À la suite d'une infraction à la loi, une enquête est confiée à une autorité de sécurité (Police Nationale ou Municipale en zone urbaine, Gendarmerie en zone rurale), éventuellement étayée par un service très spécialisé : douane, police de l'air et des frontières, antiterrorisme, services de cybersécurité, services de protection des hautes personnalités...

L'enquête est destinée à réunir tous les éléments autour de l'infraction afin de rechercher les auteurs et de les déférer à la justice : constatations physiques, recueil d'indices, témoignages. Elle peut être « de fragrance » au voisinage spatial et temporel des faits ; le juge peut également décider d'une enquête préliminaire qui, malgré son nom, est décalée par rapport aux faits, puis divers compléments d'enquête, y compris en cours d'instruction ou de procès, parfois même une fois les jugements prononcés.

Les gestes des enquêteurs sont encadrés par le Code de procédure pénale ; par exemple, il ne peut y avoir à l'heure actuelle de contrôle d'identité que si la personne contrôlée est fortement présumée d'être reliée aux faits (pas nécessairement suspectée).

Une phase toute particulière des enquêtes est la « garde à vue » qui concerne des personnes soupçonnées de crimes ou délits susceptibles d'emprisonnement : c'est une mesure policière ou judiciaire de privation temporaire de liberté, destinée à faciliter le recueil d'indices ou de preuves tout en empêchant le prévenu d'organiser des concertations externes. De plus, le prévenu peut être assisté d'un avocat dans certaines conditions, mais sans « accès au dossier ». Ces dernières années, de nombreuses voix se sont élevées en France sur la pertinence du « périmètre » des infractions ainsi que sur les conditions d'accès au dossier pénal lors des gardes à vue.

LES ÉVOLUTIONS NUMÉRIQUES

Le fichier « EDVIGE »

Un décret du Ministère de l'Intérieur du 27 juin 2008 portait création du fichier « Exploitation Documentaire et Valorisation de l'Information GEnérale ». Sous l'autorité de la Police Judiciaire, ce fichier était appelé à recenser les individus, groupes ou personnes morales, dont le comportement pouvait porter atteinte à l'ordre public, en particulier ceux appelés à exercer une fonction politique, syndicale ou religieuse.
Les types de données collectées étaient : état civil, identité, immatriculations des véhicules, déplacements, antécédents judiciaires.
À la suite d'examens par la CNIL, par une Commission des Lois et surtout, là encore, par des organisations de défense des libertés individuelles, un décret de fin 2009 a annulé l'existence de ce fichier. Un autre fichier plus restreint fut créé dans le cadre de la Loi LOPPSI II.

Casier judiciaire, fichiers « STIC » et « JUDEX »

Créé sous la II^{e} République, le casier judiciaire est un fichier contenant les condamnations pénales d'un individu, prononcées soit par la justice pénale, soit par la justice commerciale, et l'évolution de ces peines (amnistie, retrait, réhabilitation...). Seul un type d'extrait réduit peut être communiqué à l'intéressé ou à son représentant légal, les données complètes n'étant accessibles qu'à des autorités dûment habilitées.

Mis en œuvre par la DGPN depuis 1985, mais d'utilisation effective entre 1995 et 2001, le fichier STIC « Système de Traitement des Infractions Constatées » contient des données sur les diverses infractions concernant les auteurs ou les victimes. Il a un homologue à la Gendarmerie Nationale, le fichier JUDEX, fichier « JUdiciaire de Documentation et d'Exploitation ».
Ces deux fichiers sont énormes et contiennent des données sur environ 4 millions de « mis en cause » mais également sur environ 30 millions de victimes. Leur durée de conservation est de 20 ans pour les auteurs, 15 ans pour les victimes. Diverses analyses, notamment de la CNIL, ont pointé des défauts d'actualisation des situations enregistrées. Depuis 2002, les fichiers évoluent vers un fichier global, appelé ARIANE ou fichier d'« Application de Rapprochement, d'Identification et d'Analyse pour les Enquêteurs », dont on connaît peu d'éléments quant à sa pertinence actuelle.

Le fichier des « auteurs d'infractions sexuelles ou violentes » ou FIJAIS

Le fichier des Personnes Recherchées – la « fiche S »

Créé en 1969, le FPR « Fichier des Personnes Recherchées » comporte plus de 400 000 noms, qu'il s'agisse de mineurs en fugue, d'évadés de prison, de membres du grand banditisme, de personnes interdites de quitter le territoire, mais aussi de militants politiques ou écologistes (anarchistes, antinucléaires, etc.). Il comporte l'état civil et diverses informations.
Les catégories du fichier sont matérialisées par des lettres majuscules :

- E (police générale des étrangers) ;
- IT (interdiction du territoire) ;
- R (opposition à résidence en France) ;
- TE (opposition à l'entrée en France) ;
- AL (aliénés) ;
- M (mineurs fugueurs) ;
- V (évadés).

En particulier, la catégorie S signifie « Sûreté de l'État » et concerne entre autres les terroristes avérés ou potentiels.

Le SIS « Système d'Information SCHENGEN »

Les accords de 1985 instaurent entre les pays de l'Union Européenne (dont la liste a évolué depuis), ainsi qu'un petit nombre d'autres États européens, un « principe général de libre circulation des biens et des personnes à l'intérieur d'une frontière générale extérieure commune », qui remplace les frontières traditionnelles entre États (la contrepartie de cette liberté résidant dans une coopération policière renforcée entre ces États).

Cette coopération s'appuie sur un fichier mis à jour et consultable par les autorités des pays. Il comprend : état civil complet, présence d'armes ou de véhicules volés, caractère violent ou non de l'individu, données biométriques. Le système évolue d'un référentiel d'identité à une base de données de signalements à des fins policières et juridiques, ceci d'autant plus que les contrôles aux frontières ont disparu. Des autorités européennes (CEPD, G29) ou nationales (CNIL) contrôlent l'accès au fichier.

En France, le SIS est mis à jour à partir du fichier du FPR décrit plus haut.
En 2006, le fichier recensait 11 millions d'individus. La coopération internationale, par exemple dans le domaine du crime international, doit en permanence s'adapter aux langues et évolutions judiciaires diverses.

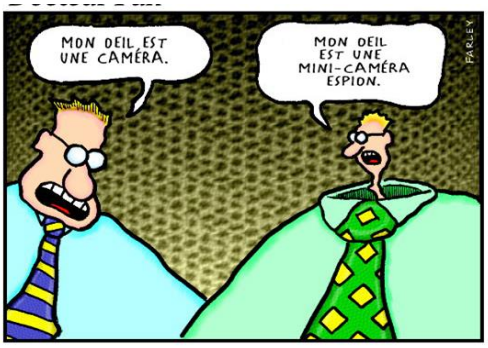
LA DIFFICILE PROBLÉMATIQUE SECURITÉ /LIBERTÉS

Globalement, la mise en œuvre des outils policiers, pénaux et judiciaires « ordinaires » précédents, développés au fur et à mesure de l'évolution de la criminalité sous ses nouveaux aspects (nouvelles technologies, délinquance, trafics d'influence, corruption, terrorisme), n'a pas engendré auprès du public ou des associations et mouvements libertaires de protestations ou réactions d'envergure. Mais une nouvelle donne intervient en 2015.
À la suite des attentats terroristes sur Paris et banlieue en janvier 2015, ainsi que de plusieurs autres attaques réputées d'origine « djihadiste » (Bruxelles, Villejuif, etc.), au vu de l'émotion générale suscitée, le gouvernement de Manuel Valls a rédigé et fait adopter par le Parlement au premier semestre 2015, une « Loi sur le Renseignement ». Promulguée le 24 juillet 2015, elle vise essentiellement à renforcer le cadre juridique national du renseignement en France qui relève d'un Service rattaché au Ministère de l'Intérieur, la DGSI « Direction Générale de la Sécurité Intérieure ».

Cette loi prévoit la mise en place de plusieurs mesures controversées telles que l'installation chez les opérateurs de télécommunications de dispositifs, surnommés « boîtes noires », visant à détecter les comportements suspects à partir des données de connexion. On peut considérer qu'elle étend, sur le fond et à un périmètre correspondant à la complexité de la nouvelle menace, les mesures des dispositifs antérieurs « PERBEN II » et « LOPPSI II ».

L'ensemble est « régulé » par une entité, la « Commission Nationale de Contrôle des Techniques de Renseignement », composée de hautes personnalités dont des magistrats. En outre, le Premier ministre ainsi que le Conseil d'État assurent une régulation et une supervision au deuxième niveau.

À titre d'exemple d'école, toute activité Internet faisant une grande place à l'utilisation du mot « djihadiste » entraînera un filtrage et une identification de l'entité ou de la (des) personne(s) présumée(s) émettrice(s), ainsi qu'une surveillance, qui peut être suivie de mesures plus répressives (blocage des outils, arrestations, mises en examen des auteurs).



Sur le plan des réactions de l'opinion publique, on connaissait l'Association « Quadrature du NET » qui avait déjà principalement mené des actions :

- de contestation de la loi « HADOPI 2 » de prévention et répression des piratages des œuvres sur Internet (2008 à 2012) ;
- en faveur de la « Neutralité du NET », en prônant un accès identique à tous les citoyens aux données du NET, indépendamment des systèmes de connexion.

En l'espèce, ce mouvement s'élève, concernant le dispositif Renseignement décrit plus haut, contre les risques de « flicage » de la vie privée et de restriction des libertés.

Un exemple controversé d'échanges internationaux de données à des fins sécuritaires : le « PNR »

Le « Passenger Name Record » - en français : données des dossiers passagers – consiste dans l'enregistrement, la consultation, éventuellement les échanges entre acteurs concernés et administrations centrales des pays (Police, Justice), de données à la fois personnelles (nom, prénom, habitudes diverses) et circonstancielles (références et lieux des modes de transport, hébergements...).
À l'origine, un prestataire de services (agence de voyages, plateforme de réservation hôtelière) renseigne le système via un outil centralisé, les données étant ensuite partagées sur d'autres outils et par d'autres entités consultantes.
À l'heure actuelle, le Royaume-Uni et les États-Unis possèdent des systèmes de PNR étendus au domaine de sécurité publique, autorisant la consultation par des autorités administratives.

L'Union Européenne quant à elle, et en particulier le G29 (groupe de travail sur la protection des données), s'engage très progressivement, pour les pays y figurant, dans la démarche, avec d'importantes réserves quant à la consultation d'éléments dans le cadre des libertés publiques (et ce, essentiellement en raison des législations différentes suivant les États).

CONCLUSIONS

Globalement, les nouvelles technologies ont un apport positif sur la sécurité et les libertés publiques :

- fonctionnement acceptable, malgré des lourdeurs et des cumuls de textes législatifs, de la Police et de la Justice, respectant les valeurs démocratiques et les droits des personnes ;
- sur le plan des lois encadrant le « numérique » :
  - concernant le système de surveillance HADOPI, après quelques années de mises au point et de pratique, le petit nombre de contrôles et de sanctions ne permet pas d'identifier, une dérive d'ensemble véritable ;
  - a priori également, de vifs débats au Parlement donnent en partie raison à la pertinence de la Loi sur le Renseignement, qui d'une manière générale, selon divers sondages d'opinion, a un impact rassurant sur la population.

patrick.kineider@hotmail.fr