Mehr Transparenz: Die Revision des Bundesgesetz über den Datenschutz

Jean-Philippe Walter

Dr. iur., Stellvertreter des Eidg. Datenschutz- und Öffentlichkeitsbeauftragter

Résumé: ***Le 1er janvier 2008 entre en vigueur une révision de la loi fédérale sur la protection des données. Cette révision permet à la Suisse de ratifier le protocole additionnel à la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, de revoir le régime des communications de données à l'étranger, d'encourager le recours à la certification en matière de protection des données et la mise en place de conseiller à la protection des données et d'accorder un droit de recours au préposé fédéral à la protection des données et à la transparence contre les décisions de l'administration fédérale ne donnant pas suite à ses recommandations. L'un des objectifs majeurs de la révision est en outre de renforcer la transparence des traitements, notamment en introduisant une obligation d'informer les personnes concernées lors de la collecte de données sensibles ou de profils de la personnalité.***

Am 24. März 2006 hat die Bundesversammlung eine Änderung des Bundesgesetzes über den Datenschutz sowie einen Bundesbeschluss verabschiedet, der den Bundesrat zur Ratifizierung des Zusatzprotokolls vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung ermächtigt. Die Revision des DSG verfolgt zwei Hauptziele: Einerseits sollte der Motion 98.3529 «Erhöhter Schutz für Personendaten bei Online-Verbindungen» der Geschäftsprüfungskommission des Ständerats und der Motion 00.3000 «Erhöhte Transparenz bei der Erhebung von Personendaten» der Kommission für Rechtsfragen des Ständerats Folge geleistet werden. Andererseits musste das DSG im Hinblick auf die Ratifizierung des Zusatzprotokolls zum Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (STE Nr. 108) an die Anforderungen dieses Zusatzprotokolls angepasst werden.

Stellung der Betroffenen gestärkt

Das revidierte Gesetz stärkt die Stellung der betroffenen Personen, indem es mehr Transparenz bei der Bearbeitung von Personendaten schafft, insbesondere durch die Einführung einer Informationspflicht gegenüber den betroffenen Personen beim Beschaffen von besonders schützenswerten Personendaten und Persönlichkeitsprofilen. Die grenzüberschreitende Datenbekanntgabe wird neu geregelt; dabei wird namentlich auf die Meldepflicht für die Übermittlung von Datensammlungen ins Ausland verzichtet. Die Bestimmungen über die Anmeldung von Datensammlungen werden an die Verpflichtung zu erhöhter Transparenz angepasst. Eine neue und innovative Bestimmung führt die Möglichkeit ein, dass Datenverarbeitungsprodukte und -systeme zur Bearbeitung von Personendaten zertifiziert werden, und ermutigt die Inhaber von Datensammlungen dazu, Datenschutzverantwortliche zu bezeichnen. Und nicht zuletzt ist der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte berechtigt, gegen Verfügungen der Bundeskanzlei und der Departemente Beschwerde zu führen, wenn eine von ihm abgegebene Empfehlung abgelehnt wird. Diese Änderungen werden am 1. Januar 2008 in Kraft treten. Ein Ziel dieser ersten wichtigen Änderung des Bundesgesetzes über den Datenschutz war, durch die Verbesserung der Transparenz der Datenbearbeitungen die Position der Bürger und Bürgerinnen, über die Personendaten bearbeitet werden, zu stärken. Das Gesetz regelt neu die Information der betroffenen Personen in zwei Bestimmungen.

Erkennbarkeit

Erstens sieht *Artikel 4 Absatz 4* (neu) vor, dass die Beschaffung von Personendaten und insbesondere der Zweck ihrer Bearbeitung für die betroffene Person erkennbar sein müssen. Diese Bestimmung konkretisiert den in Artikel 4 Absatz 2 genannten Grundsatz von Treu und Glauben. Dieses Erfordernis der Erkennbarkeit bestand schon ausdrücklich für Bundesorgane bei der Bearbeitung von besonders schützenswerten Personendaten sowie von Persönlichkeitsprofilen. Es wird damit auf alle Arten von Daten ausgedehnt und gilt auch für den privaten Bereich. Es handelt sich dabei nicht um eine Informationspflicht. Artikel 4 Absatz 4 bedeutet, dass es für die betroffene Person unter normalen Umständen erkennbar sein muss, dass Daten, die sie betreffen, beschafft wurden oder möglicherweise beschafft werden (Grundsatz der Voraussehbarkeit). Sie muss den Zweck der Datenbearbeitung kennen oder feststellen können. Die Anforderungen, die erfüllt sein müssen, damit die Beschaffung als erkennbar gilt,

***Zusammenfassung:** Am 1. Januar 2008 tritt eine Revision des Bundesgesetzes über den Datenschutz in Kraft. Diese Revision erlaubt es der Schweiz, das Zusatzprotokoll zum Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten zu ratifizieren. Sie ändert die Regelung der grenzüberschreitenden Datenflüsse und fördert die Datenschutzzertifizierung und die Bezeichnung von Datenschutzverantwortlichen. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte erhält die Möglichkeit, gegen Verfügungen der Bundesverwaltung Beschwerde zu führen, wenn eine von ihm abgegebene Empfehlung abgelehnt wird. Eines der Hauptziele der Revision ist ausserdem die Stärkung der Transparenz der Datenbearbeitungen, insbesondere mit der Einführung einer Informationspflicht gegenüber den betroffenen Personen bei der Beschaffung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen.*

sind nach den Umständen sowie nach den Grundsätzen der Verhältnismässigkeit und von Treu und Glauben zu beurteilen. Je nach Situation kann der Inhaber der Datensammlung auch verpflichtet sein, die betroffene Person aktiv zu informieren.

Informationspflicht

Zweitens verpflichtet *Artikel 7a* die Inhaber von Datensammlungen, die besonders schützenswerte Personendaten (*Art. 3, Bst. c*) oder Persönlichkeitsprofile (*Art. 3, Bst. d*) beschaffen, die betroffene Person darüber zu informieren. Diese Pflicht besteht nicht nur dann, wenn die Daten direkt bei der betroffenen Person beschafft werden, sondern auch bei der Beschaffung bei Dritten. Mit dieser Informationspflicht erreicht man eine Angleichung an die europäische Gesetzgebung, insbesondere an die Richtlinie 95/46/EG und an die Empfehlungen des Europarats. Der neue Artikel 7a unterscheidet sich aber insofern von den europäischen Erlassen, als er die Informationspflicht auf besonders schützenswerte Personendaten und Persönlichkeitsprofile beschränkt. Die europäischen Regelungen gelten für jegliche Beschaffung von Personendaten, unabhängig von der Art dieser Daten. Die Informationspflicht stärkt aber auch in ihrer eingeschränkten Form die Stellung der betroffenen Personen, die so einfacher und schneller ihre Rechte geltend machen und sich einer Bearbeitung, die ihnen nicht gerechtfertigt scheint, widersetzen können. Die Informationspflicht zwingt auch die Inhaber von Datensammlungen, wachsamer zu sein und keine besonders schützenswerten Personendaten oder Persönlichkeitsprofile zu beschaffen und zu bearbeiten, wenn diese zur Erfüllung der Aufgaben nicht unbedingt erforderlich sind. *Artikel 7a Absatz 2* legt den Umfang der Informationspflicht fest. Mitzuteilen sind alle wesentlichen Informationen, mit deren Hilfe sich die betroffene Person eine Vorstellung von der Datenbearbeitung machen und gegebenenfalls ihre Rechte geltend machen kann. Sind zusätzliche Informationen erforderlich, damit sich die betroffene Person ein Bild machen kann, muss der Inhaber der Datensammlung gemäss dem Grundsatz von Treu und Glauben der betroffenen Person auch diese Zusatzinformationen liefern. So ist gegebenenfalls darüber zu informieren, ob die Datenbeschaffung obligatorisch oder freiwillig ist und welche Folgen die Weigerung hat, bestimmte Fragen zu beantworten.

Die betroffene Person muss auch informiert werden, wenn die Daten nicht bei ihr beschafft werden. Die Information hat spätestens bei der Speicherung der Daten zu erfolgen oder, wenn die Daten nicht gespeichert werden, bei der ersten Bekanntgabe an Dritte (*Art. 7a Abs. 3*). Der Inhaber der Datensammlung muss die betroffenen Personen nur insoweit informieren, als sie nicht bereits informiert wurden (*Art. 7a Abs. 4*). Er hat ebenfalls keine Informationspflicht, wenn die Speicherung oder die Bekanntgabe der Daten ausdrücklich durch das Gesetz vorgesehen ist (*Art. 7a Abs. 4 Bst. a*) oder wenn die Information nicht oder nur mit unverhältnismässigem Aufwand möglich ist (*Art. 7a Abs. 4 Bst. b*). Schliesslich kann der Inhaber der Datensammlung die Information auch verweigern, einschränken oder aufschieben, wenn eine der Bedingungen nach Artikel 9 erfüllt ist.

Form der Information

Das DSG schreibt die Form der Information nicht vor. Die betroffene Person muss nicht schriftlich informiert werden, möglich ist auch eine mündliche Information. Aus Beweisgründen wird dennoch die schriftliche Form empfohlen. Denn wer vorsätzlich seine Informationspflicht missachtet, kann bestraft werden (Art. 34 Abs. 1 Bst. b Ziff. 1). Die Form der Information muss auch den Umständen angemessen sein. Denkbar sind insbesondere eine Veröffentlichung, ein Aushang, ein Prospekt, eine Aufnahme in die Allgemeinen Bedingungen, ein Schreiben an die betroffenen Personen oder ein Anhang zu einem Vertrag oder einer Rechnung. Die Information kann auch auf der Einstiegsseite eines Internet-Angebots stehen. Wichtig ist, dass die Information gut sichtbar und dass sie verständlich und lesbar ist.

Übergangsfrist

Die Inhaber von Datensammlungen haben eine Frist von einem Jahr ab Inkrafttreten des Gesetzes, um die notwendigen Massnahmen zur Information der betroffenen Personen zu ergreifen (Übergangsbestimmung). Die Informationspflicht gilt nicht im Fall von Daten, die vor Inkrafttreten des revidierten DSG erhoben wurden, ausser wenn in Zusammenhang mit einer bestehenden Datensammlung neue Daten gesammelt werden oder wenn eine Person von dieser Sammlung noch nicht betroffen war. ■

La nouvelle loi fédérale sur la protection des données (LPD): pragmatique ou lacunaire?

Philippe Meier

Docteur en droit et avocat, professeur ordinaire à l'Université de Lausanne

Zusammenfassung: ***Das revidierte Datenschutzgesetz tritt am 1. Januar 2008 in Kraft. Verstärkt wurde das Transparenzprinzip. Trotzdem ist der Gesetzgeber nicht so weit gegangen, seit langem im EU-Recht anerkannte Regeln einzuführen. Es wäre denn auch die Gelegenheit gewesen, ein klares Signal zu setzen und das Prinzip der Datensparsamkeit der Daten wie auch die Rahmenbedingungen für die private und öffentliche Videoüberwachung einzuführen. Begrüsst wird dafür die Technikneutralität des Gesetzes, die eine flexible Anwendung an neue Sachverhalte erlaubt. Bedauerlich ist aber, dass das Sanktionensystem nicht verbessert wurde, da es, neben der Unbekümmertheit der Bevölkerung, mitverantwortlich für die geringe Effektivität der Regelung ist.***

Introduction

La LPD du 19 juin 1992 a fait l'objet d'une première révision d'importance adoptée le 22 mars 2006, qui entrera en vigueur le 1er janvier 2008.

Fruit d'un travail législatif de longue haleine dès les années septante, la LPD a souvent été jugée dépassée, et ce dès son entrée en vigueur, notamment parce qu'elle n'avait pas intégré les développements technologiques alors déjà en cours.

L'évolution juridique s'est elle aussi poursuivie: adoption en 1999 de l'art. 13 al. 2 Cst. féd. qui, en dépit de son texte maladroit, garantit un véritable droit à l'autodétermination informationnelle, adoption de la Directive communautaire 95/46 du 24 octobre 1995 relative à la protection des données, inscription dans la Charte des droits fondamentaux de l'Union européenne d'une disposition spécifique consacrée à la protection des données (art. 8), conclusion des Accords bilatéraux Schengen/Dublin (qui obligeront à reprendre le contenu de la Directive 95/46 pour le premier pilier communautaire): c'était là l'occasion de procéder à une mise à jour plus que ponctuelle de la législation suisse.

Nous verrons à partir de quelques exemples précis (limités au traitement des données par des personnes privées) si tel a été le cas et, dans la négative, s'il faut ou non le regretter.

Renforcement de la transparence?

La révision a été déclenchée par deux motions émanant de Commissions du Conseil des États, l'une relative aux liaisons online dans l'administration fédérale, l'autre visant au «Renforcement de la transparence lors de la collecte de données personnelles».

Cette dernière a amené l'ancrage dans la loi du principe de reconnaissabilité (art. 4 al. 4: «*la collecte de données personnelles, et en particulier les finalités du traitement, doivent être reconnaissables pour la personne concernée*»), qui à notre sens pouvait déjà se déduire du principe de la bonne foi (et donc de la transparence) posé à l'art. 4 al. 2.

Est-ce suffisant?

L'ignorance et/ou l'indifférence des citoyens-consommateurs face au traitement de leurs données personnelles sont unanimement considérées comme les causes principales du peu d'effet pratique de la législation. Or on a longtemps longtemps soutenu que le droit d'accès prévu à l'art. 8 LPD était le pivot de l'entier de la réglementation: seul pourra faire valoir les droits qui lui sont octroyés celui qui peut accéder à ses données personnelles.

Mais encore faut-il que dans un monde où chacun accomplit quotidiennement de très nombreuses transactions, notamment sur l'Internet, l'attention des intéressés soit attirée sur le fait même que leurs données personnelles sont convoitées par les tiers.

La Directive l'a compris, qui prévoit un *devoir général d'information* pour toute collecte de données personnelles.

Le législateur suisse en est resté au strict cadre de la motion et n'a introduit un tel *devoir d'information exprès et actif* que pour les données sensibles et les profils de la personnalité. Lorsque l'on sait que le Conseil national avait dans un premier temps voté le ren-

Meier | La nouvelle loi fédérale sur la protection des données (LPD): pragmatique ou lacunaire?

Résumé: *La révision de la loi fédérale sur la protection des données entrera en vigueur le 1er janvier 2008. Le principe de transparence a été renforcé. Le législateur s'est toutefois arrêté à mi-chemin, en renonçant à inscrire dans la loi des règles que le droit communautaire connaît de longue date. Il aurait également dû profiter de l'occasion pour donner un signal clair en ancrant dans la loi le principe de minimisation des données, d'une part, et en prévoyant un cadre légal général pour la vidéosurveillance, publique et privée, dont l'extension ne laisse d'inquiéter, d'autre part. La neutralité technologique que la révision a conservée pour le reste doit en revanche être saluée, car elle permet une adaptation aux multiples développements en cours. On regrettera cependant qu'il n'ait pas été remédié à la faiblesse du mécanisme des sanctions, à l'origine – aux côtés de l'indifférence et/ou de l'ignorance de l'individu – du peu d'efficacité de la réglementation.*

voi de l'entier du projet (déjà très allégé avant même sa mise en consultation) au Conseil fédéral en lui demandant de se limiter à la mise en œuvre des deux motions, le résultat mitigé s'explique politiquement, mais ne convainc pas.

Qui plus est, lorsque l'information est obligatoire (art. 7a), elle doit porter «au minimum» sur l'identité du maître du fichier, sur les finalités du traitement et sur les catégories de destinataires, mais rien dans la loi n'oblige à mentionner des informations supplémentaires telles que le fait de savoir si la réponse aux questions est obligatoire ou facultative et les conséquences éventuelles d'un défaut de réponse, pas plus que l'existence du droit d'accès. Or ces informations doivent être fournies selon la Directive communautaire, lorsqu'elles sont nécessaires à assurer un traitement loyal des données. Il faudra donc déduire cette obligation du principe général de la bonne foi, alors qu'il eût été bien simple de la prévoir expressément dans la loi.

Le processus de décision individuelle automatisée, appelé à devenir de plus en plus fréquent («scoring» informatique de la personne, notamment en matière d'octroi de crédit), est expressément visé par l'art. 15 de la Directive européenne. Le projet du Conseil fédéral prévoyait pour sa part que «la personne concernée doit être expressément informée du fait qu'une décision produisant des effets juridiques à son égard ou l'affectant de manière significative est prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de la personnalité», sans aller jusqu'à garantir à l'intéressé – contrairement à la réglementation européenne – une sorte de droit d'être entendu dans la procédure. Refus regrettable du Parlement, ici aussi, au motif notamment que la règle pourrait avoir à s'appliquer à chaque retrait d'un Bancomat et que le risque d'erreur de la machine n'est pas plus grand qu'une décision humaine prise selon des directives schématiques!

Le maintien de la neutralité technologique

La LPD originelle était empreinte de «neutralité technologique». La loi révisée conserve ce même trait: on y cherchera en vain les notions de spyware, de données biométriques, de vidéosurveillance, de RFID (Radio Frequency Identification), de PNR (Passenger Name Records), de data-warehousing ou encore de scrambling.

Ce pragmatisme a toutefois du bon: les principes fondamentaux de la protection des données sont à notre sens à la fois suffisamment contraignants et souples pour réglementer la mise en œuvre de ces moyens technologiques et de ceux encore à venir.

Nous émettrons toutefois trois regrets:

– que l'on n'ait pas précisé le principe de proportionnalité (comme on l'a fait pour celui de la bonne foi) en posant une règle de «Datensparsamkeit» (ou minimisation des données) générale, qui apparaît d'autant plus essentielle que les capacités de stockage deviennent extensibles à souhait (cf. le § 3a de la loi allemande);
– que l'on n'ait pas obligé l'auteur du traitement à utiliser et à intégrer à son système, à chaque fois que cela est possible sans frais disproportionnés, les PET (Privacy Enhancing Technologies) existantes;
– que l'on n'ait pas posé une norme-cadre sur la vidéosurveillance. Il est vrai que le principe de proportionnalité ne fera admettre la mise en œuvre de cette technique qu'en dernier recours et permettra d'influer sur le délai de conservation des images. Mais depuis le malheureux ATF 133 I 77 (certes postérieur de 9 mois à l'adoption de la loi révisée) rendu au sujet du règlement de police de la ville de St-Gall, qui avalisait un délai de conservation allant jusqu'à 100 jours, le réflexe sécuritaire a le champ libre. Le législateur vaudois a encore été relativement raisonnable (l'art. 22 al. 5 de la nouvelle loi, adoptée le 11 septembre 2007, fixe le délai à 96 h), mais l'art. 54 al. 4 du projet de loi sur le transport des voyageurs du 9 mars 2007 fait passer le délai actuel de 24 heures à ... 100 jours! Un bien mauvais signal pour tous les autres cas de vidéosurveillance par des organes fédéraux (le rapport «Vidéosurveillance exercée en vue d'assurer la sécurité dans les gares, les aéroports et les autres espaces publics» publié par le Département fédéral de justice et police au mois de septembre dernier ne laisse pas de doute à cet égard), mais aussi pour les privés, qui ne sont quant à eux «encadrés» que par les principes généraux de la loi.

La certification comme incitatif et avantage concurrentiel?

La nouvelle loi entend favoriser la certification des systèmes et des procédures de traitement des données, avec à la clef certains allègements administratifs (dispense de déclaration de fichiers). Mais, conscient du peu d'efficacité de la déclaration des fichiers (les devoirs des maîtres de fichiers privés ont d'ailleurs été sensiblement réduits en ce domaine), le législateur entend convaincre les entreprises des avantages *concurrentiels* (en terme d'image) que cette solution peut présenter.

Le label n'émanera toutefois pas de l'autorité fédérale elle-même, mais de sociétés privées qui auront elles-mêmes été accréditées par l'État. Cela enlève à notre sens une grande partie de sa portée à cette faculté. Quant à l'argument selon lequel le consommateur choisira de préférence l'entreprise ainsi labellisée plutôt qu'une autre, nous nous permettons d'en douter. Comme on a pu le voir avec les certifications ISO, la généralisation des labels a vite fait ressembler le tout à un exercice de style, dont l'utilité interne (dans la documentation des processus) est indéniable, mais les effets externes peu significatifs; de plus, le consommateur préférera probablement se concentrer sur les différences de prix ou sur les concerts de rock stars offerts gratuitement par son commerçant préféré plutôt que sur le point de savoir si celui-ci est certifié GoodPrivacy ou d'un autre label de protection des données! Il n'est évidemment pas dans notre propos de critiquer des démarches qui viseraient à sensibiliser les maîtres de fichiers à la protection des données, mais les effets pratiques risquent d'être limités.

Une loi toujours aussi peu efficace au chapitre des sanctions

Hormis quelques compétences procédurales supplémentaires, la nouvelle loi n'a pas élargi le pouvoir d'intervention du Préposé fédéral.

On ne peut s'empêcher de penser que le législateur s'accommode d'une situation dans laquelle une réglementation détaillée et complexe ne peut en réalité pas être mise en oeuvre convenablement, en tout cas pour les fichiers privés, faute de compétences matérielles (mais aussi faute de ressources financières suffisantes) de l'organe de contrôle.

Les moyens juridiques existent certes pour le consommateur, mais ils supposent, une fois le droit d'accès exercé, de recourir au juge, qui plus est dans une procédure ordinaire. Beaucoup de frais, beaucoup de désagréments que le consommateur aura vite fait de mettre en balance avec l'atteinte effective et personnelle qu'il a subie.

Le libéralisme ambiant explique aisément que le législateur n'ait pas envisagé de doter le Préposé fédéral d'un pouvoir sanctionnateur (amendes administratives par ex.). Mais des mécanismes simples connus dans d'autres domaines auraient certainement permis d'améliorer la position du lésé dans la procédure judiciaire: une procédure simple et gratuite, un droit d'action des organisations de consommateurs (comp. art. 10 al. 2 LCD) ou la faculté pour le tribunal de condamner à des indemnités forfaitaires (comme les connaissent les art. 336a et 337c al. 3 CO pour les licenciements abusifs et les licenciements immédiats injustifiés). Il n'en a pourtant pas été question.

Conclusion

Une révision pragmatique et lacunaire tout à la fois! Compte tenu des valeurs en jeu (plus personne ne conteste sérieusement que la protection des données soit une valeur-clef d'un ordre démocratique, qui doit être prise en compte au-delà de la sensibilité, souvent peu développée, de chaque individu), l'on peut regretter que le législateur suisse ne soit pas allé plus loin. A en croire le Conseil fédéral, qui a annoncé, si ce n'est promis, une révision plus ambitieuse dans son Message (FF 2003 1915 ss, p. 1923), ce ne serait que partie remise. Espérons qu'il en aille ainsi, même si, à l'aune du temps législatif helvétique, une occasion perdue, ou qui n'a été saisie que partiellement, ne se représente malheureusement qu'à intervalles fort éloignés! ■