SOMMAIRE

avant-propos

Une « liste noire » est dans le langage courant un fichier recensant des personnes indésirables. Si aucune disposition légale ou réglementaire n'interdit la constitution de telles listes, en revanche, le risque d'exclusion et de marginalisation des personnes fichées est réel.

Qu'ils soient constitués sur l'initiative de particuliers, d'entreprises ou d'organismes professionnels, la multiplication de ce type de fichiers peut, selon leur contenu et leur diffusion, nuire aux personnes physiques concernées par ces inscriptions, dans les actes de leur vie quotidienne.

En effet, de tels fichiers sont très largement dérogatoires aux principes généraux de la protection des données personnelles : loin de demeurer confidentielles, les informations en cause sont partagées, c'est-à-dire portées à la connaissance des acteurs professionnels concernés. Par leur fonctionnement même, ces fichiers paraissent contraires à la philosophie du « droit à l'oubli » puisque va être attaché à une personne un de ses comportements passés afin d'alerter l'ensemble d'un secteur professionnel. Enfin, l'inscription est parfois utilisée comme un moyen de pression qui peut s'apparenter à une forme de chantage.

Le fichage d'une personne présente, en outre, comme caractéristique d'affecter par nature les intérêts d'une catégorie de citoyens au bénéfice d'une autre, représentant le plus souvent un secteur professionnel donné. L'équilibre à trouver pour garantir le respect des droits des particuliers d'une part et la protection des intérêts des professionnels d'autre part est éminemment délicat et relève, si ce n'est d'un choix de société, tout au moins d'un débat largement politique. Un tel fichage a un effet stigmatisant et dangereux dès lors qu'il est susceptible de

priver des individus, au quotidien, du bénéfice des prestations les plus indispensables à la vie courante (transports, télécommunications, etc.), voire de porter atteinte à des droits fondamentaux de la personne (l'accès à certains services, tels l'assurance, le crédit, la téléphonie, n'étant pas sans répercussions sur la possibilité d'exercer une activité professionnelle ou de se loger).

Par le passé, la CNIL a bien sûr eu à se prononcer à plusieurs reprises sur la problématique des « listes noires » et elle s'est attachée à la définition de préconisations propres aux finalités déclarées de ces fichiers.

Cependant, la généralisation et le développement exponentiel du fichage des « mauvais payeurs » ou des « fraudeurs » par des acteurs privés, quel que soit le secteur d'activité concerné, conduisent la CNIL à s'interroger sur la pérennité de ses préconisations, sur les conséquences de l'absence de législation spécifique, ainsi que sur les mesures à adopter afin de préserver les libertés individuelles.

La prévention du risque ne peut en effet justifier l'instauration d'une « société à deux vitesses » excluant la frange de la population la plus défavorisée de la protection accordée à la vie privée et aux libertés individuelles.

Le présent rapport fait le point sur les constats, préconisations et perspectives dégagés sur ces questions par la CNIL au cours de l'année 2002.

Chapitre 1

un nouveau contexte économique et juridique : la nécessaire remise en perspective de la doctrine de la CNIL

Sans nul doute, le développement de ce qu'il est convenu d'appeler « *la société du risque et de l'instantané* » a entraîné la multiplication des initiatives privées de constitution de fichiers de « personnes à risques ». Face à cette actualité, l'évolution du contexte juridique permettra un meilleur encadrement et une plus grande protection des libertés et droits des personnes physiques.

1 L'ÉVOLUTION DU CONTEXTE ÉCONOMIQUE : LE DÉVELOPPEMENT DE LA « SOCIÉTÉ DU RISQUE »

La gestion du risque sous les formes diverses de « capitalisation de l'information », de « segmentation », de « géomarketing », d'« hyperciblage », est devenue aujourd'hui impérative pour les entreprises, en quête d'optimisation de l'usage de l'information collectée et de production d'informations nouvelles. L'apport incontestable des NTIC [1] dans la gestion de la relation client porte sur les possibilités d'interconnexion, d'automatisation de processus de traçabilité et d'optimisation des tâches, et enfin le

1 Nouvelles technologies de l'information et de la communication.

partage de l'information. Sur internet, l'unicité des portails de collecte d'informations (par exemple un service immobilier en ligne proposera l'achat d'un bien, mais aussi le déménagement, le crédit, l'assurance...) favorise la mutualisation des données tous secteurs confondus.

La prolifération de ces fichiers s'explique ainsi en partie par la définition de nouveaux outils de marketing, l'instantanéité croissante des transactions commerciales et la collecte d'informations venant de tous horizons. Ce phénomène est particulièrement frappant dans le secteur bancaire au sein duquel apparaissent de nouvelles règles prudentielles incitant à prendre en compte le risque juridique, le risque de fraude, les erreurs humaines, les risques fiscaux, le risque de défaillance de l'emprunteur... et désormais le risque de blanchiment, tous difficilement quantifiables en l'état de la méthodologie et des données accessibles.

Alors que des informations sont accessibles pour le risque de marché ou de crédit, par exemple au moyen du fichier des surendettés ou du fichier bancaire des entreprises, le risque opérationnel ne peut pas être évalué à partir de fichiers extérieurs. Les établissements bancaires et financiers vont donc avoir l'obligation de se doter d'outils de mesure [2] de ce type de risque.

2 À côté des risques traditionnels – le risque de marché, le risque de crédit (supposés être mesurables selon des formules mathématiques), la prise en compte du « risque opérationnel » sera désormais incluse dans le calcul de l'adéquation des fonds propres. Le comité de Bâle qui réunit de façon informelle les régulateurs du secteur bancaire des principaux États afin d'édicter des recommandations propres à assurer la solvabilité des établissements bancaires et financiers (règles prudentielles) a édicté de nouvelles recommandations (Bâle II) visant à intégrer le risque opérationnel dans le calcul du ratio de solvabilité (ratio Cooke qui devient le ratio Mac Donough). Elles devraient entrer en vigueur en 2007, mais les établissements bancaires et financiers ont choisi d'anticiper en intégrant d'ores et déjà la réforme Bâle II dans leur processus interne de contrôle et en développant des outils de mesure du risque. La réforme de Bâle II renvoie précisément à l'utilisation de la segmentation, du « géomarketing », aux contrôles de cohérences, et à la mutualisation de ces outils, y compris la détection de la fraude.

Toutefois, le développement de la « société du risque » n'est pas uniquement le fruit de l'évolution méthodologique liée aux nouvelles technologies, mais aussi de l'importance croissante de la « fraude organisée » qui tire bénéfice de ces mêmes instruments. Ainsi, les carences en matière de sécurisation des paiements sur internet incitent les commerçants en ligne ou certains prestataires à développer des systèmes de détection de la fraude [3]. Les opérateurs en matière de crédit décrivent avec insistance, mais sans en chiffrer les conséquences, la fréquence du recours à des prêtes-noms, faussement domiciliés, pour des financements de véhicules, sans valeur réelle après accident, mais dont la carte grise a été recyclée. De même, la participation de vendeurs à des « surfinancements » est dénoncée.

Dans le même temps, les phénomènes de concentration, de création de sociétés financières *ad hoc* entre un établissement financier et un commerçant, d'externalisation de la gestion des crédits à la consommation, de constitution de groupes à géométrie variable et de partenaires multiples conduisent à des rapprochements de données et à la constitution de fichiers dont la légitimité et les garanties apportées apparaissent d'autant plus improbables que le nombre de sociétés concernées est important.

Le développement de ces outils d'analyse s'effectue le plus souvent dans le cadre d'un traitement globalisé sans différenciation entre les finalités, qu'il s'agisse de prévention de la fraude, de mesure du risque ou d'un simple outil marketing, instaurant de fait un système de sanctions civiles opaque et arbitraire. Cependant, les évolutions à venir du cadre juridique sont de nature, au moins partiellement, à permettre un meilleur encadrement de ces fichiers.

3 C'est le cas d'une société de courtage en assurance qui distribue une offre d'assurance au bénéfice des commerçants en ligne associée à un outil de détection de la fraude consistant en un fichier recensant et analysant l'ensemble des bons de commande afin de détecter des profils d'internautes à risques.

2
UN NOUVEAU CONTEXTE JURIDIQUE

La transposition de la directive européenne 95/46 du 24 octobre 1995 [4], les travaux d'harmonisation de son application au sein du « groupe article 29 », qui réunit les commissaires européens à la protection des données, ainsi que les textes européens en préparation vont modifier le contexte juridique actuel dans un sens allant vers une plus grande protection des personnes et des pouvoirs renforcés des autorités de protection.

<A> La directive du 24 octobre 1995 relative à la protection des données

La CNIL ne dispose pas, sur le fondement de la loi du 6 janvier 1978, du droit de s'opposer à la mise en œuvre de fichiers constitués par le secteur privé. L'existence de tels fichiers n'est en effet pas subordonnée à son examen préalable, comme c'est le cas pour les fichiers relevant du secteur public, mais à une simple déclaration à la CNIL contre délivrance d'un récépissé qui ne constitue en aucun cas un agrément et n'exonère le déclarant d'aucune de ses responsabilités.

Hormis quelques lois particulières intervenues dans le domaine du crédit et des moyens de paiement ayant confié la gestion des traitements à une personne de droit public (la Banque de France), il n'existe pas d'encadrement spécifique du fonctionnement des fichiers d'enregistrements d'impayés ou de « fraudes ».

4 Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *Journal officiel n° L 281 du 23 novembre 1995 p. 0031 -0050.*

Partant d'un régime de relative liberté pour le secteur privé (à l'exception notable des fichiers recensant des infractions et du secret qui s'applique à certains enregistrements d'informations, notamment en matière bancaire), la transposition de la directive européenne du 24 octobre 1995 va avoir pour effet de modifier ce contexte sur deux orientations.

En premier lieu, les pouvoirs de la CNIL à l'égard des traitements mis en œuvre par le secteur privé vont être renforcés. La directive accorde ainsi une attention particulière aux « *traitements susceptibles de présenter des risques particuliers au regard des droits et des libertés des personnes concernées* », parmi lesquels figurent ceux ayant pour finalité « *d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat* » [5]. Les États membres sont ainsi invités à « *précise[r] les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées* » et doivent « *veille[r] à ce que ces traitements soient examinés avant leur mise en œuvre* » [6].

Le projet de loi de transposition [7] soumet à autorisation préalable « *les traitements automatisés ayant pour finalité de sélectionner les personnes susceptibles de bénéficier d'un droit, d'une prestation ou d'un contrat alors que les personnes en cause ne sont exclues de ce*

5 Considérant (53) de la directive 95-46 : *« considérant que, cependant, certains traitements sont susceptibles de présenter des risques particuliers au regard des droits et des libertés des personnes concernées, du fait de leur nature, de leur portée ou de leurs finalités telles que celle d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat ou du fait de l'usage particulier d'une technologie nouvelle ; qu'il appartient aux États membres, s'ils le souhaitent, de préciser dans leur législation de tels risques ».*

6 Article 20 de la directive 95-46 : contrôles préalables.

7 Projet de loi adopté par l'Assemblée nationale en première lecture le 30 janvier 2002 relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

bénéfice par aucune disposition légale ou réglementaire » [8], ainsi que ceux ayant pour objet « *l'interconnexion de fichiers relevant d'autres personnes* [autres que publiques] *et dont les finalités principales sont différentes* [9] ».

Ces dispositions sont de nature à soumettre à un régime d'autorisation préalable les fichiers comportant des informations sur les « mauvais payeurs » ou destinés à prévenir la fraude, dès lors qu'ils sont destinés à la sélection de personnes présentant un profil de risque particulier.

D'autre part, venant compléter les dispositions de l'actuel article 27 de la loi du 6 janvier 1978 prévoyant l'information des personnes sur les destinataires des informations collectées, l'article 11 de la directive impose l'information [10] des personnes en cas de collecte indirecte (c'est-à-dire lorsque les données n'ont pas été collectées auprès de la personne concernée), « *dès l'enregistrement des données ou si une communication de données à un tiers est envisagée, au plus tard lors de la première communication de données* ».

8 Nouvel article 25 – I -4°).

9 Nouvel article 25 – I -5°) alinea 2.

10 Est prévue l'information des personnes portant au moins sur les éléments suivants, s'ils n'ont pas été portés à sa connaissance antérieurement :
a) l'identité du responsable du traitement et, le cas échéant, de son représentant ;
b) les finalités du traitement ;
c) toute information supplémentaire telle que :
– les catégories de données concernées ;
– les destinataires ou les catégories de destinataires des données ;
– l'existence d'un droit d'accès aux données la concernant et de rectification de ces données, dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont collectées, ces informations supplémentaires sont nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données.
Le paragraphe 1 ne s'applique pas lorsque, en particulier pour un traitement à finalité statistique ou de recherche historique ou scientifique, l'information de la personne concernée se révèle impossible ou implique des efforts disproportionnés ou si la législation prévoit expressément l'enregistrement ou la communication des données. Dans ces cas, les États membres prévoient des garanties appropriées.

<B> Les travaux du groupe européen des commissaires à la protection des données

En avril 2001, le groupe des commissaires européens à la protection des données créé par l'article 29 de la directive du 24 octobre 1995, dit « groupe de l'article 29 », décidait de réaliser une étude portant sur les multiples aspects des listes noires. Cette entreprise avait pour objectifs d'analyser la réalité couverte par la notion de « traitements à risques » évoquée par le considérant 53 de la directive et de contribuer à une application homogène de la directive en ce domaine, ce qui correspond à la mission du « groupe de l'article 29 ». Cette étude a abouti à l'adoption d'un document de travail sur les listes noires, publié en 2002 [11].

Après avoir comparé les différentes expériences des autorités européennes de protection des données, le « groupe de l'article 29 » a conclu que, dans tous les pays d'Europe, l'existence de listes noires, et plus particulièrement de fichiers mutualisés d'impayés ou de prévention de la fraude, a une incidence indéniable sur la vie privée et sociale des individus et qu'il était important de disposer de critères uniformes et harmonisés afin que les personnes dont les données sont traitées se voient reconnaître les mêmes droits et garanties dans tous les pays de l'Union européenne.

À cet effet, le « groupe de l'article 29 » a rappelé l'importance particulière des éléments suivants :

– La définition des types de données pouvant être traitées, la finalité du traitement, les garanties accordées aux personnes, les conditions et les circonstances dans lesquelles de tels fichiers peuvent être autorisés

11 Document de travail sur les listes noires adopté le 3 octobre 2002 11118/02/EN WP 65 page 5, disponible à l'adresse suivante :
http://europa.eu.int/comm/internal_market/fr/dataprot/wpdocs/wpdocs-2002.htm

doivent être précisément déterminées dans le cadre des principes rappelés par l'article 7 [12].

– La mise à jour de l'information est fondamentale, aussi le « groupe de l'article 29 » a-t-il rappelé l'importance de définir des critères généraux permettant d'uniformiser les délais de conservation des données enregistrées dans les fichiers.

– Tout aussi fondamental est le droit de l'intéressé à être informé du traitement des données à caractère personnel qui le concernent, car seule cette information permet de rendre effectif l'exercice par la personne de ses droits d'accès, de rectification, d'annulation et d'opposition.

– Enfin, l'instauration de mesures de sécurité techniques et d'organisation est soulignée comme étant extrêmement importante, ainsi que la détermination des conditions d'accès aux fichiers en cause. Ces mesures, qui relèvent des obligations classiques des responsables de traitements en vertu de la directive, revêtent une dimension particulière dans le contexte de fichiers mutualisés, à partir desquels les possibilités de dissémination d'informations sont plus nombreuses que pour les fichiers « internes », mis en œuvre par une seule partie à son seul usage.

---

12 Section II principes relatifs à la légitimation des traitements de données – Article 7 : les États membres prévoient que le traitement de données à caractère personnel ne peut être effectué que si :
a) la personne concernée a indubitablement donné son consentement ou ;
b) il est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ou ;
c) il est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ou ;
d) il est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée ou ;
e) il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées ou ;
f) il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er paragraphe 1.

<C> La proposition de directive européenne relative au crédit à la consommation

Les travaux du « groupe de l'article 29 » ont pris une dimension supplémentaire quand a été publiée une proposition de directive du Parlement européen et du Conseil relative à l'harmonisation des dispositions législatives, réglementaires et administratives des États membres en matière de crédit à la consommation [13].

L'article 8 de la proposition de directive prévoit en effet de rendre obligatoire la création, dans chaque État membre de l'Union, de bases de données centralisées ayant pour but l'enregistrement des consommateurs et des garants auxquels sont imputables des incidents de paiement. Les prêteurs devront consulter cette base préalablement à tout engagement du consommateur ou du garant. La création de cette base serait, dans l'esprit du législateur européen, de nature à éviter un endettement excessif des consommateurs, ce qui correspond à sa volonté de consacrer la notion de « prêt responsable ».

Dans un avis en date du 2 juillet 2002, le « groupe de l'article 29 » s'est prononcé de manière générale sur cette disposition en souhaitant qu'une référence à la directive 95/46 soit faite dans le texte final, ou qu'à défaut, des propositions plus élaborées soient faites au regard de la protection des données. Le « groupe de l'article 29 » sera associé à l'évolution de la proposition de directive, mais en tout état de cause, les principes et critères établis dans le document de travail précité du groupe restent pertinents.

En effet, un rapport de la Commission européenne sur l'application de la directive 87/102 du Conseil du 22 décembre 1986 relative au crédit à

13 Proposition de directive relative à l'harmonisation **des dispositions législatives, réglementaires et administratives des États membres en matière de crédit aux consommateurs** COM (2002) 443 final, version française, p. 14.

la consommation [14] faisait état de l'existence de problèmes spécifiques en ce qui concerne la protection de la vie privée du consommateur de crédit. Les problèmes identifiés étaient relatifs à la nature des données pouvant être enregistrées (incidents de paiement ou encours de crédit), aux personnes pouvant en avoir connaissance, à la réalisation de profils, à l'utilisation des données à d'autres fins que celles de l'opération de crédit, à la protection de la sphère privée du consommateur, à la durée de conservation de ces données et enfin au traitement des plaintes.

La proposition de directive met l'accent sur une autre source de préoccupation : l'absence d'effectivité du droit d'opposition. Partant du constat que « *l'accord du consommateur* [sur l'utilisation à des fins commerciales] *est souvent obtenu à l'aide d'un formulaire de demande de crédit ou d'une clause figurant dans le contrat de crédit ou de sûreté et dans des circonstances ne permettant pas au consommateur de refuser réellement, compte tenu du risque que court alors celui-ci de se voir refuser l'octroi du crédit ou les facilités de paiement. Le plus souvent le consommateur n'est même pas conscient du fait qu'il a souscrit pareille clause* » [15] pour retenir le principe de l'interdiction d'utilisation des données collectées à des fins étrangères à l'appréciation de la situation financière des consommateurs [16] dans le cadre de la réalisation ou de la gestion d'un contrat de crédit.

Il ressort de ce tour d'horizon que les préoccupations dont la CNIL a pu faire état jusqu'à présent sur ces sujets se poseront avec encore plus d'acuité après transposition de la directive du 24 octobre 1995 et ce d'autant qu'il existe une grande diversité dans les fichiers constitués par des acteurs également variés.

14 Commission européenne, rapport sur l'application de la directive 87/102/CEE COM (95) 117 final du 11 mai 1995.

15 Article 7 de la proposition de directive.

16 En l'occurrence de l'emprunteur ou du garant.

Au-delà des dispositions susceptibles d'entrer en application dans le cadre de la transposition de cette directive, une intervention législative s'avère nécessaire pour encadrer de manière satisfaisante le fichage des « mauvais payeurs » et surtout celui des « fraudeurs », le législateur étant le plus à même d'apprécier l'opportunité et la proportionnalité de ces outils, en en autorisant la création et en précisant les principes édictés par la loi du 6 janvier 1978.

Chapitre 2

la diversité des fichiers centraux portant sur des « personnes à risques »

La CNIL a vite été confrontée à la difficulté d'appréhender la notion de « liste noire ». Les travaux du « groupe de l'article 29 » regroupant les autorités de contrôle européennes ont mis en lumière la diversité des finalités et du contenu de ces listes internes ou mutualisées, constituées dans tous les domaines et allant au-delà du simple inventaire des impayés. En effet, les « listes noires » recensées par la CNIL et le « groupe de l'article 29 » comportent aussi bien des informations sur des impayés, des comportements pénalement répréhensibles ou encore des « anomalies ». Il s'agit ainsi de la tenue de fichiers concernant aussi bien des « auteurs d'obtentions irrégulières de crédit ou tentatives de telles obtentions », que des « clients douteux », des « personnes présentant des risques aggravés », d'« auteurs d'actes répréhensibles », de personnes pour lesquelles des « anomalies » ou « incohérences » sont détectées, que des « personnes indésirables ».

L'expérience de la CNIL conduit à établir une classification selon les finalités déclarées ou réelles (« fichiers d'impayés » ou « fichiers de fraudeurs ») par une approche prenant en compte des critères organisationnels propres aux entités procédant à la tenue des « listes noires ».

1
DES OBJECTIFS DISTINCTS
MAIS CONVERGENTS

<A> Obtenir le règlement de la créance ou écarter les mauvais payeurs

Si deux finalités principales président à la constitution de fichiers centraux, à savoir le recensement de « mauvais payeurs » à des fins d'obtention du paiement et la prévention du risque d'impayé ou de fraude, en pratique ces deux finalités tendent à se confondre.

La CNIL a toujours manifesté une grande vigilance à l'égard des échanges d'informations relatives aux risques présentés par les personnes, notamment lorsqu'elles sont auteurs d'impayés, qui alimentent des traitements automatisés dits d'alerte ou « listes noires ».

Son attention s'est portée plus particulièrement sur la nature, les modalités de collecte, la durée de conservation et les destinataires de ces données, ainsi que sur l'exercice des droits des personnes concernées.

Des « garde-fous » ont ainsi été édictés en matière de fichiers centraux d'incidents de paiement dans le secteur du crédit dans une recommandation du 5 juillet 1988 sur les traitements mis en œuvre par les établissements de crédit. En 1989, lors de l'instauration du fichier des incidents de paiement de crédit aux particuliers, la CNIL a émis des recommandations sur les modalités de mise en œuvre du fichier tenu par la Banque de France qui ont toutes été reprises dans le règlement du Comité de la réglementation bancaire régissant ce fichier.

Dans la très grande majorité des cas cependant, les conditions d'inscription sont laissées à l'initiative des responsables des fichiers et elles n'offrent pas toujours toutes les garanties sur la qualité de l'information. De même, le droit d'opposition prévu par l'article 26 de la loi du 6 janvier 1978 peut s'avérer difficile à exercer.

La centralisation peut avoir ainsi pour effet d'interdire l'accès à des prestations ou d'exiger des garanties complémentaires qui rendent plus difficile l'accès à certains services sans pour autant que la tenue du fichier soit entourée de garanties suffisantes. Par le passé, la CNIL a ainsi adressé un avertissement à une association gérant « *une banque de données d'opposition sur chèques pour le libre usage des particuliers et des commerçants* » [1] et demandé l'arrêt immédiat du fonctionnement du traitement qui, accessible à tous, ne comportait pas de mesures de sécurité et de confidentialité. De la même façon, elle adressait un avertissement à un groupement professionnel gérant une centrale d'incidents de paiement dans le domaine du crédit, pour défaut de sécurité du traitement [2], compte tenu de l'absence d'éléments d'identification certaine des débiteurs.

On peut également rappeler que la CNIL avait estimé qu'un traitement ayant pour finalité de centraliser les incidents de paiement consécutifs à des soins dentaires ne satisfaisait pas aux exigences de la loi. L'inscription dans le fichier aurait eu pour conséquence de priver une personne de la possibilité de se faire soigner. Or, l'article 2 de la loi du 6 janvier 1978 interdit de prendre une décision impliquant une appréciation sur un comportement humain sur le seul fondement d'un traitement automatisé.

1. Délibération n° 88-50 du 10 mai 1988.

2. Délibération n° 91-014 du 12 février 1991.

<B> Écarter les « clients à risques »

Au-delà du recensement des impayés, certains fichiers peuvent collecter des renseignements relatifs au comportement du client dans l'objectif d'évaluer le risque qu'il présente et le cas échéant l'écarter. Dans cette finalité, le défaut de paiement n'est qu'un des éléments entrant en ligne de compte dans l'évaluation du risque, l'enregistrement de présomptions ne venant qu'en complément.

De même, l'utilisation de techniques croisées aboutit à déterminer les personnes qui vont se voir écarter d'une prestation ou d'un service. Tel est le cas des outils de segmentation comportementale ou géographique et des techniques de *scoring* associées à la centralisation d'informations sur les personnes pour présumer de l'existence d'un risque de fraude.

L'existence dans les commandes successives d'une même personne, ou de celles qui lui sont directement ou indirectement rattachées, de plusieurs numéros de carte bancaire, numéros de téléphone, associés ou non à une ou plusieurs adresses de domicile ou de livraison, présentées comme suspectes, vont conduire indistinctement à écarter le client d'un service donné sans que cette personne n'ait été l'auteur d'un impayé ou d'un quelconque manquement contractuel ou acte de malveillance.

Il convient de rappeler avec force la distinction entre le traitement relatif à des impayés et le traitement d'éléments permettant de lutter contre la fraude. En effet, un organisme est tenu d'assurer le traitement des impayés en vue de permettre une gestion saine, de respecter ses obligations comptables [3] et de procéder au recouvrement de ses créances. Il peut donc légitimement conserver trace des incidents de paiement

3. En application de l'article L. 123-22 du Code de commerce (ancien article 16), les livres et documents créés à l'occasion d'activités commerciales doivent être conservés dix ans.

survenus, sans qu'un tel dispositif ne heurte les principes posés par la loi du 6 janvier 1978.

Les traitements de lutte contre la fraude sont autrement plus problématiques que les fichiers d'incidents de paiement dans la mesure où ils relèvent des fichiers d'infractions.

En effet, même si elles ne sont identifiées que comme des « anomalies » ou encore des « incohérences [4] » dans le contenu des données ou pièces justificatives fournies par les consommateurs (fausse fiche de paye, document d'identité falsifié...), les informations enregistrées par les gestionnaires de fichiers ne le sont qu'en considération de la très forte probabilité d'une tentative de fraude. Certes, ces gestionnaires ne cherchent pas à caractériser l'élément moral de l'infraction, mais il résulte de l'inscription dans de tels fichiers que sont catégorisés des segments de population « à risques » qui se voient opposer des réponses d'exclusion.

Un enregistrement de « comportement délictuel présumé » est dès lors plus dangereux pour les libertés que celui des décisions caractérisant tel ou tel délit après examen contradictoire et il convient d'affirmer clairement que de tels traitements relèvent bien des fichiers d'infractions.

Or, la mise en œuvre de tels fichiers se heurte à l'interdiction posée à l'article 30 de la loi du 6 janvier 1978 aux termes duquel : « *Sauf dispositions législatives contraires, les juridictions et autorités publiques agissant dans le cadre de leurs attributions légales ainsi que, sur avis conforme de la commission nationale, les personnes morales gérant un service public peuvent seules procéder au traitement automatisé des informations nominatives concernant les infractions, condamnations ou mesures de sûreté* ».

4. Il faut entendre par incohérence tout défaut de concordance des informations fournies par l'intéressé soit avec d'autres éléments communiqués par ce dernier auprès du même organisme (cohérence interne) soit avec des informations provenant d'autres sources publiques ou non (cohérence externe).

la diversité des fichiers centraux portant sur des « personnes à risques »

En l'état du droit positif [5], la mise en œuvre de traitements relatifs aux infractions, condamnations et mesures de sûreté est donc subordonnée à trois conditions ayant trait à la qualité du responsable du traitement (juridictions et autorités publiques, personne morale gérant un service public), au recueil de l'avis conforme de la CNIL et au strict respect de la finalité définie dans le cadre des attributions légales de ces personnes ou autorités. Toute dérogation ne peut intervenir qu'en vertu d'une disposition législative. Le casier judiciaire national, dont l'informatisation est régie par les dispositions de la loi du 4 janvier 1980, les bureaux d'ordre tenus par les greffes des juridictions répressives, le fichier de la police judiciaire STIC relèvent de ces dispositions.

Si la CNIL a, à plusieurs occasions, rappelé le caractère impératif des dispositions de l'article 30 lorsqu'il s'agissait de véritables fichiers d'infractions (par exemple dans le secteur de la grande distribution), elle s'est montrée plus souple à l'égard de la création de fichiers recensant des comportements ayant porté préjudice à leur responsable, victime de l'infraction. À cet égard, la CNIL s'est fait l'écho des travaux préparatoires à l'adoption de la loi du 6 janvier 1978. Les restrictions apportées à la constitution de fichiers d'infractions, condamnations, et mesures de sûreté étaient motivées dans le rapport Tricot [6] par le souci d'éviter la prolifération de « casiers judiciaires privés » (étaient concernés l'enregistrement d'infractions couvertes par l'amnistie, la prescription, la réhabilitation et des décisions annulées ou infirmées). Les débats parlementaires ont toutefois permis de faire apparaître [7] que le texte ne remettait pas en cause le droit des victimes de conser-

5. Le projet de loi de transposition de la directive CE 95/46 tend à soustraire du contrôle de la CNIL les fichiers dits de souveraineté, qui ne seront plus soumis à régime d'autorisation (avis tacite de la CNIL), mais dont la mise en œuvre devra être précédée de l'avis consultatif de la CNIL.

6. Rapport de la Commission « informatique et libertés » de 1975 ayant servi de base à l'adoption de la loi du 6 janvier 1978.

7. Procès-verbal de la séance du 17 novembre 1977, p. 798 : position de Monsieur Peyrefitte, Garde des sceaux, à l'examen d'un amendement.

ver trace des faits, même couverts par l'amnistie, pour réclamer réparation d'un préjudice [8].

Les entreprises mettent en avant la notion de gestion des affaires en « bon père de famille » et la nécessité d'automatiser le traitement des vérifications accomplies lors de la formation du contrat ou avant la fourniture de la prestation. Certes, la connaissance du co-contractant est un élément essentiel de la décision de contracter pour un nombre important de transactions dont les contrats de prêt. Cependant, le caractère *intuitu personae* de la transaction peut-il justifier la collecte de toute information, même relevant de l'article 30, au motif qu'elle serait de nature à porter atteinte à la nécessaire confiance devant s'établir pour permettre la conclusion du contrat ?

Le développement de la fraude organisée au détriment de plusieurs secteurs d'activité, (notamment le crédit et l'assurance) a fait apparaître l'opportunité d'une prévention collective qui se traduit par la reconnaissance de la légitimité du partage d'informations entre sociétés relevant d'un même secteur d'activité ou d'un même ensemble finalisé de partenaires.

Une spécificité a pu être reconnue au secteur bancaire en matière de lutte contre la fraude sans que ne soit toutefois envisageable, en l'état des textes en vigueur, la constitution d'un fichier commun à l'ensemble de la profession. Ainsi, saisie dans le courant de l'année 2001 de demandes visant à la mutualisation de telles informations au sein du secteur du crédit, la CNIL a alerté les pouvoirs publics en faisant valoir que la centralisation de toutes les fraudes ou tentatives de fraude – classées en différentes catégories selon le degré de gravité que les établissements leur confèrent – et la mise à disposition de telles informations à des tiers n'ayant subi aucun préjudice direct entrent manifestement dans les prévisions de l'article 30 et n'étaient pas envisageables dans le cadre juridique actuel.

8. Est ainsi opérée une distinction entre les faits et la sanction : seul le fichage de cette dernière est visé.

2
DES GRADATIONS
DANS LES GARANTIES PRÉSENTÉES

La CNIL a eu à se prononcer à plusieurs reprises sur le développement de fichiers de mauvais payeurs ou de « fraudeurs » quel que soit le secteur d'activité considéré.

Les initiatives auxquelles a été confrontée la CNIL sont apparues plus ou moins acceptables au regard de l'application des principes de protection des données. En outre, la CNIL est souvent interrogée sur le caractère public et validé par les autorités publiques de telle ou telle « liste noire ». Certains opérateurs se présentent en effet comme disposant de label ou d'agrément de la CNIL alors que cette dernière, compte tenu du cadre juridique actuel, n'en délivre pas.

La mise en œuvre de ces traitements s'effectue ainsi dans des contextes et situations juridiques très différents. Le choix du législateur, lorsqu'il est intervenu pour encadrer des fichiers mutualisés, a consisté à en confier la gestion à une personne de droit public avec des contraintes de service public. La faveur du législateur pour une gestion de service public n'a pas pour autant abouti à la formulation d'un principe d'exclusivité. Ainsi, d'autres fichiers sont le fruit de regroupements professionnels d'envergure nationale ou propre à des acteurs incontournables d'un secteur d'activité. Il convient encore de faire part de la spécificité du secteur financier et de la mise en commun de « listes noires » par des sociétés privées.

<A> Les fichiers encadrés par le législateur

Il s'agit des fichiers de la Banque de France qui s'est vue confier par la loi n° 73-7 du 3 janvier 1973 la mission de « *veiller sur la monnaie et le crédit* » et « *au bon fonctionnement du système bancaire* ».

Elle a organisé dans ce cadre la centralisation des incidents de paiement résultant de l'utilisation des moyens de paiement, dans un premier temps par la création du fichier central des chèques (FCC), puis par son extension conventionnelle à la centralisation des retraits de cartes bancaires en 1987 [9]. La Banque de France est le gestionnaire de ce fichier, alimenté par les établissements bancaires et financiers sous leur responsabilité, un rapprochement avec le FICOBA [10] résulte de la loi sur la sécurité des chèques [11].

Le fichier national des chèques irréguliers (FNCI) a été instauré par la loi du 30 décembre 1991 relative à la sécurité des chèques et recense les interdits bancaires, les interdits judiciaires, les comptes clôturés, la perte/vol de chéquiers et les faux chèques, informations rendues accessibles à tout bénéficiaire de chèque. Il ne recense que les coordonnées bancaires des personnes concernées.

Le fichier des incidents de crédit aux particuliers (FICP) a quant à lui été instauré par la loi Neiertz du 31 décembre 1989. Il recense les incidents caractérisés de remboursement ainsi que les situations de surendettement. Un règlement du Comité de la réglementation bancaire définit les conditions d'inscription sur le fichier et ses modalités de fonctionnement (interrogation, mise à jour...).

---

9. Cette extension ne résulte pas d'une modification de la loi mais de la conclusion d'une convention avec le groupement cartes bancaires. Cette extension conventionnelle a pour conséquence un traitement différencié du régime d'inscription et des durées de conservation entre les chèques et les cartes bancaires difficilement justifiable dès lors que ces moyens de paiement sont utilisés indifféremment.

10. Fichier des comptes bancaires tenus par la Direction générale des impôts.

11. Délibération n° 92-050 du 26 mai 1992.

Si ces traitements, à l'exception de la centralisation des retraits de cartes bancaires intégrée au FCC ou du fichier bancaire des entreprises (FIBEN) qui affecte notamment les dirigeants d'entreprise d'une cotation Banque de France, répondent à un encadrement législatif précis, les difficultés relatives à l'identification des personnes inscrites, les délais de radiation par les établissements de crédits, les fichages irréguliers, génèrent de nombreuses plaintes écrites et des appels téléphoniques tant auprès de la CNIL que de la Banque de France. L'action de la CNIL vise notamment à clarifier pour les personnes concernées les conditions d'inscription et de consultation de ces fichiers centraux et au-delà des réponses apportées ponctuellement aux personnes qui la saisissent, elle envisage d'élaborer des fiches pratiques mises en ligne sur le site internet et également distribuées sous forme de brochure.

<B> Les fichiers mis en œuvre par des groupements ou syndicats professionnels

Il s'agit en règle générale de fichiers tenus par les membres d'un secteur professionnel déterminé dont la consultation est réservée aux membres du secteur concerné. À côté de fichiers déclarés par des syndicats professionnels cantonnés géographiquement à des régions ou des départements donnés, les fichiers centraux tenus à l'initiative d'organismes professionnels se sont développés essentiellement dans deux secteurs : l'assurance et la téléphonie.

– ***Le secteur de l'assurance***

Le secteur des assurances a été le premier à se doter, avant l'adoption de la loi du 6 janvier 1978 et en dehors de toute réglementation particulière, de fichiers centraux destinés à prévenir le risque de fraude.

La prévention de la fraude à l'assurance a donné lieu à la création de fichiers centralisés, d'abord propres à chaque association ou fédération de sociétés d'assurances (l'Association générale des sociétés

d'assurance contre les accidents (AGSAA) et l'Assemblée plénière des sociétés d'assurance contre les incendies et les risques divers (APSAIRD)), puis cette gestion a été confiée à l'Agence de lutte contre la fraude à l'assurance (ALFA). Venant compléter une messagerie télématique qui permet aux sociétés d'assurances d'échanger ponctuellement des renseignements sur la base de questions/réponses afin de permettre la détection de manœuvres frauduleuses, l'ALFA gère un fichier commun, dénommé « échanges d'informations », recensant les informations relatives à des personnes impliquées dans des déclarations de sinistre identifiées de façon certaine comme frauduleuses.

L'Association pour la gestion des informations sur le risque automobile (AGIRA) a pour sa part mis en œuvre un traitement dont la finalité est l'échange d'informations entre sociétés afin de personnaliser les primes et cotisations d'assurance automobile. Incidemment ce recensement permet également de détecter l'omission lors de la souscription du contrat de déclarations de sinistres par l'assuré.

– ***Le secteur de la téléphonie et des télécommunications***

Dès 1996, les opérateurs de téléphonie mobile (SFR, Orange et Bouygues Télécom depuis l'année 2000) et certaines sociétés de commercialisation de services (SCS) se sont regroupées dans le seul but de pouvoir mettre en œuvre un traitement (« Préventel ») de prévention des impayés, et ce, grâce à la centralisation d'informations relatives à des impayés et à des anomalies constatées auprès de leurs abonnés au service de téléphonie mobile, survenant lors de la souscription ou de l'exécution des contrats d'abonnement, à des particuliers ou à des entreprises.

Ce traitement a fait l'objet en novembre 1996 d'une déclaration à la CNIL, conformément à l'article 16 de la loi du 6 janvier 1978.

La finalité d'un tel fichier pour les opérateurs est double. Il s'agit tout d'abord de fournir un élément d'appréciation des demandes de sous-

cription de contrats d'abonnement. À cet égard, le recensement dans le fichier ne constitue pas automatiquement un obstacle à la souscription d'un contrat mais avertit l'opérateur des risques éventuels liés au recouvrement des futures créances. Il lui appartient alors de définir la stratégie à adopter : demande d'un dépôt de garantie, refus de contracter, etc. Par ailleurs, le fichier permet la mise en œuvre d'un dispositif de vérification des informations fournies lors d'une demande d'abonnement afin de prévenir les souscriptions de contrats irrégulières et successives auprès de plusieurs membres.

<C> Les fichiers propres aux acteurs incontournables d'un secteur d'activité

Si l'on peut opposer les fichiers dits « internes », c'est-à-dire propres à une entreprise ou un organisme donné, et les fichiers dits « mutualisés » qui sont le fruit d'un regroupement ou d'un croisement de plusieurs fichiers, cette distinction n'est pas suffisante pour cerner la diversité des fichiers de « mauvais payeurs » et de « fraudeurs ». En effet, un fichier interne, du fait de la taille de l'entreprise, de son importance relative en part de marché dans un secteur d'activité donné, voire de sa situation de monopole ou d'oligopole, trouve sa place dans la présente étude : il s'agit alors d'un « fichier central » qui bien que non mutualisé ou rapproché de celui d'autres entités juridiques doit être régi par les mêmes principes.

Les phénomènes de concentration, l'élargissement du champ d'action géographique des entreprises, ont contribué au développement de fichiers centraux destinés à recenser les clients « indésirables » afin d'en diffuser la liste aux différents points de vente. Lorsque l'organisme concerné est un acteur incontournable dans un domaine d'activité, l'inscription dans le « fichier central », si son fonctionnement n'est pas encadré, pourrait conduire à priver la personne de l'accès à une prestation ou un service devenu indispensable pour la vie courante.

La CNIL a toujours été attentive à la constitution de tels fichiers centraux. Lors de l'examen du « fichier des impayés de la SNCF [12] », la CNIL avait émis un avis favorable sur un projet de mise en place d'un système destiné à lutter contre l'émission de chèques sans provision au préjudice de la SNCF et à accroître l'efficacité des procédures de recouvrement engagées par la SNCF à l'encontre de ces débiteurs en rappelant toutefois la nécessité d'informer les intéressés de leur droit d'accès et de rectification. Plusieurs principes de fonctionnement ont alors été définis afin de garantir la conformité du dispositif aux dispositions de la loi du 6 janvier 1978 : seuls certains services dépendant de la direction financière de la SNCF peuvent alimenter et consulter le fichier, seules les informations portant sur les chèques volés et les cas de récidive notoire en matière de chèque sans provision sont diffusées aux gares, une durée de conservation de quatre ans, délai nécessaire pour l'enregistrement de l'ensemble des encaissements consécutifs aux opérations de recouvrement engagées par la SNCF a été retenue, des dispositions particulières ont été prises afin d'assurer la confidentialité des données (contrôle de liaison et destruction des supports papiers dès réception des mises à jour) ; enfin, les personnes concernées par les inscriptions doivent être informées des suites que la SNCF entend réserver au traitement des chèques impayés.

<D> La spécificité du secteur financier

La CNIL a eu à examiner des déclarations de traitements qui consistent en une mise en commun d'informations en matière financière par plusieurs sociétés de crédit souhaitant procéder à une gestion centralisée de la prise de décision d'octroi de crédit.

12. Délibération n° 88-121 du 8 novembre 1988.

– ***La prévention de la fraude dans le secteur du crédit***

Dans le secteur du crédit [13], la CNIL a été saisie en 1994 de dossiers de déclaration relatifs à la constitution de fichiers de protection contre la fraude. Les deux établissements concernés souhaitaient pouvoir conserver la trace des dossiers de demandeurs pour lesquels leurs services de contrôle avaient détecté des anomalies, telles que la fourniture de documents falsifiés ou volés. Cela revenait donc pour ces services à procéder à une qualification « pénale » du comportement du demandeur.

La CNIL avait à l'époque consulté le ministère de la Justice sur ces projets et leur articulation avec les dispositions de l'article 30 de la loi du 6 janvier 1978 qui interdit le traitement des informations concernant les infractions et condamnations. Le ministère a estimé qu'*« un fichier recensant les personnes auteurs d'obtentions irrégulières de crédit ou de tentatives de telles obtentions, lorsque ces personnes se livrent à des pratiques susceptibles d'être incriminées pénalement (utilisation de documents falsifiés ou volés notamment) reviendrait d'une part à laisser au maître du fichier l'appréciation subjective d'un comportement qu'il pourrait librement qualifier de frauduleux, d'autre part à permettre au gestionnaire de procéder au traitement automatisé d'informations nominatives ayant trait à des infractions pénales »*. Mais la Chancellerie a également indiqué que ces sociétés de crédit paraissent libres de concevoir une gestion informatique leur permettant d'assurer une instruction plus efficace et centralisée des demandes de crédit visant en particulier à détecter les fraudes notamment par comparaison avec des dossiers déjà existants.

Suivant les indications de la Chancellerie, la CNIL a demandé aux sociétés concernées de modifier juridiquement et techniquement les dossiers présentés afin de parvenir à une conciliation entre leurs objectifs et les dispositions de l'article 30.

13. Ces points ont été développés dans le rapport adopté par la Commission en novembre 2000 intitulé, *Crédit à la consommation : prévention de la fraude et des impayés et loi informatique et libertés.*

Un certain nombre de préconisations ont alors été dégagées :
– les traitements relatifs à la lutte contre la fraude doivent demeurer de la seule compétence d'un service centralisé et spécialisé de l'entreprise mettant en œuvre un tel dispositif, chargé dans les cas de suspicion de fraude de procéder à des vérifications approfondies ; seuls les membres de ce service, qui doivent disposer d'un mot de passe personnel, sont habilités à traiter les informations et à procéder aux analyses nécessaires, cela en dehors de tout automatisme ;
– les services d'exploitation en relation avec la clientèle doivent soumettre les dossiers semblant présenter des irrégularités à l'appréciation du service central ;
– une anomalie avérée entraîne l'enregistrement dans le fichier centralisé de la clientèle de l'établissement d'un code, signifiant que toute nouvelle demande devra lui être transmise ; le signalement des dossiers doit disparaître dès lors que les vérifications ont levé les doutes ;
– les intéressés doivent être informés sur le formulaire de demande de crédit que toute déclaration irrégulière peut faire l'objet d'un traitement spécifique à l'égard duquel ils disposent d'un droit d'accès et de rectification.

Par la suite, les autres établissements qui souhaitaient mettre en place un système de lutte contre la fraude se sont alignés sur ces recommandations.

La CNIL a pu vérifier à l'occasion de contrôles sur place menés en 2000 auprès de plusieurs établissements de crédit à la consommation le respect de la spécialité de la finalité des traitements de lutte contre la fraude.

– Les fichiers des « risques aggravés vie » dans le secteur des assurances

Il existait avant 1990 un fichier des risques aggravés de l'assurance vie mis en œuvre par la Fédération française des sociétés d'assurance (FFSA) commun à l'ensemble des professionnels du secteur de l'assurance, mais face aux craintes suscitées par une utilisation de ce dernier

comme un fichier des exclus de l'assurance, la CNIL rappelait en 1990 les conditions de fonctionnement et tout particulièrement la nécessaire information des personnes concernées. Répondant aux préoccupations de la CNIL d'éviter tout risque de marginalisation des personnes malades ou séropositives, la FFSA avait alors fait savoir qu'elle procédait à la destruction du fichier des risques aggravés.

Toutes les sociétés d'assurance disposent toutefois en interne de fichiers recensant les personnes présentant un risque de surmortalité. En 1994, la CNIL a procédé à une mission de contrôle auprès de la Caisse nationale de prévoyance et des principales sociétés d'assurance afin de s'assurer des conditions de mise en œuvre de ces traitements.

La CNIL s'est attachée à définir les garanties devant être présentes dans la gestion de ces fichiers :
– les personnes inscrites dans un fichier de risques aggravés ne doivent pas se voir opposer de décisions automatiques ;
– l'existence d'un tel fichier doit faire l'objet d'une déclaration spécifique ;
– les personnes (et tout particulièrement les banques qui peuvent conclure directement les contrats par délégation ne doivent en aucun cas avoir accès aux codifications médicales, celles-ci ne devant être accessibles qu'aux personnes placées sous l'autorité du médecin conseil de la compagnie d'assurance) ;
– la durée de conservation des données relatives aux anciens clients des entreprises est de dix ans pour les pièces justificatives des opérations (article R. 341-2 du Code des assurances renvoyant aux textes relatifs aux obligations comptables des commerçants) ; pour les personnes ayant fait l'objet d'un refus d'assurance la CNIL a considéré que les données collectées, notamment les codes pathologiques, devaient être immédiatement effacées, à l'exception de l'identité du proposant et de la date de décision de refus, et ce, afin de permettre aux compagnies d'assurance de lutter contre la fraude ;
– enfin, toute personne doit être informée qu'elle figure dans un tel fichier et qu'elle peut s'y opposer pour des raisons légitimes.

La convention Bélorgey visant à améliorer l'accès à l'emprunt et à l'assurance des personnes présentant un risque de santé aggravé signée le 19 septembre 2001 entre l'État, la FFSA, l'Association des établissements de crédit et d'entreprises d'investissement (l'AFECEI) et des associations de malades a prévu des mécanismes de garanties des prêts spécifiques.

<E> La mise en commun de « listes noires » par des sociétés commerciales

Ressortent de cette catégorie les fichiers mis en œuvre par de petites structures, des regroupements *ad hoc* de commerçants ou de certains professionnels ou encore certaines applications de sociétés de recouvrement de créances qui ignorent le principe de sectorisation et/ou ne respectent pas l'ensemble des principes dégagés par la CNIL en matière de « listes noires » (seuil d'inscription, notification préalable, sécurité...).

Le développement de ces initiatives, le plus souvent locales, est rendu possible par le faible coût de gestion du développement d'applications permettant d'alimenter et d'accéder à la « liste noire ». Bien souvent rassemblée sur un simple tableur, la « liste noire », quand elle n'est pas diffusée par télécopie, est accessible sur un extranet réservé à des abonnés, voire à tout internaute sous réserve du paiement d'une somme forfaitaire correspondant à une consultation.

La CNIL a manifesté les plus vives inquiétudes sur ces initiatives. Elle rappelle de façon systématique aux gestionnaires de ces fichiers les impératifs posés par la loi du 6 janvier 1978, notamment en matière de sécurité et confidentialité, et attire leur attention sur la violation du principe de proportionnalité défini par les dispositions de l'article 5c de la convention du Conseil de l'Europe du 28 janvier 1981.

De plus, l'inscription dans de tels fichiers est susceptible de porter atteinte à la considération des personnes, incrimination visée par les

dispositions de l'article L. 226-22 du Code pénal réprimant « *le fait pour toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des informations nominatives dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces informations à la connaissance d'un tiers qui n'a pas qualité pour les recevoir* ».

Indépendamment des problèmes posés au regard de l'application de la loi informatique et libertés, la mise en œuvre de ces fichiers est susceptible d'entraîner l'application de sanctions découlant du droit de la consommation. La mise en œuvre de ces traitements s'accompagne souvent de la référence à une autorisation, un agrément ou un label de la CNIL, voire de l'utilisation de terminologie de nature trompeuse quant au responsable du traitement (« national », « central »...).

Or, l'article L. 711-3 du Code de la propriété intellectuelle prévoit que « *ne peut être adopté comme marque ou élément de marque un signe* […] *de nature à tromper le public, notamment sur la nature, la qualité ou la provenance géographique du produit ou du service* ». L'article L. 121-1 du Code de la consommation dispose qu'« *est interdite toute publicité comportant, sous quelque forme que ce soit, des allégations, indications ou présentations fausses ou de nature à induire en erreur, lorsque celles-ci portent sur un ou plusieurs des éléments ci-après ; existence, nature, composition, qualités substantielles, teneur en principes utiles, espèce, origine, quantité, mode et date de fabrication, propriétés, prix et conditions de vente de biens ou services qui font l'objet de la publicité, conditions de leur utilisation, motifs ou procédés de la vente ou de la prestation de services, portée des engagements pris par l'annonceur, identité, qualités ou aptitudes du fabricant, des revendeurs, des promoteurs ou des prestataires* ». D'autre part, le fait « *dans la publicité, l'étiquetage ou la présentation de tout produit ou service, ainsi que dans les documents*

commerciaux de toute nature s'y rapportant, de faire référence à une certification qui n'a pas été effectuée dans les conditions définies aux articles L. 115-27 et L 115-28 » ainsi que le fait de « *délivrer, en violation des dispositions prévues aux articles L. 115-27 et L. 115-28, un titre, un certificat ou tout autre document attestant qu'un produit ou un service présente certaines caractéristiques ayant fait l'objet d'une certification* » est prévu et réprimé par l'article L. 115-30 du Code de la consommation de deux ans de prison et/ou 37 500 euros d'amende.

L'utilisation du terme « national » serait dès lors susceptible d'entrer dans les prévisions de ces textes de même que la référence à un « label » ou « agrément » de la CNIL.

Par ailleurs, en matière de responsabilité délictuelle (article 1383 du Code civil), la jurisprudence retient comme abus de droit ouvrant droit à dédommagement le fait d'user de voies d'exécution disproportionnées avec le *quantum* de la créance [14]. La finalité affichée par les fichiers à vocation universaliste étant leur effet « accélérateur de paiement », l'absence de fixation de seuil préalable à l'inscription serait susceptible de relever de l'abus de droit, notamment lorsque le créancier n'a mis en œuvre aucune voie d'exécution « classique » et trouve dans la menace d'inscription au fichier une solution économiquement intéressante de recouvrement de créance. Le maintien de l'inscription en dépit de l'existence de contestations est un moyen de pression dont la proportionnalité devra être appréciée au cas par cas par la jurisprudence. Par ailleurs, la qualification de chantage serait également susceptible d'être retenue, en application des dispositions de l'article 312-10 du Code pénal, pour l'obtention « *d'une signature, un engage-*

14. En ce sens pour une saisie immobilière pour le recouvrement d'une somme minime civ. 2e 13 mai 1991 *Bull. civil II* n° 150 ; pour une saisie vente Paris 7 décembre 1995 D 1996 203 note Prévault ; de délivrer à un débiteur qui n'est pas en état de cessation de paiement une assignation en redressement judiciaire en vue d'exercer sur lui un moyen de pression com. 5 décembre 1989 Defrénois 1990, 1013, note Beaudrun.

ment ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'un bien quelconque », « en menaçant de révéler ou d'imputer des faits de nature à porter atteinte à l'honneur ou à la considération ».

L'ensemble de ces textes est donc de nature à conforter la position de la CNIL sur la nécessité de déterminer des exigences strictes en matière d'information des personnes concernées, de notification préalable à l'inscription dans le fichier, de la définition du seuil d'inscription, de durée de conservation des informations...

Chapitre 3

Les principes dégagés par la CNIL en matière de fichiers centraux

La CNIL a très tôt reconnu la légitimité pour les professionnels d'un secteur d'activité particulier de tenir des fichiers accessibles à l'ensemble des professionnels concernés, regroupant les personnes présentant des risques afin de leur permettre de se prémunir contre ce qui ne concernait à l'époque que les impayés, en ayant recours à des « fichiers d'alerte ».

Tel fut le cas des secteurs du crédit, des assurances et de la grande distribution.

Dès 1990 cependant, la CNIL appelait l'attention du Premier ministre sur le risque d'atteinte aux droits des personnes résultant de la prolifération de tels fichiers d'impayés et rappelait alors les limites juridiques rencontrées dans la possibilité d'en assurer la maîtrise.

Dès lors que la directive cadre du 24 octobre 1995 donne à l'autorité de contrôle la possibilité de s'opposer à la création de dispositifs privés de recensement des risques ne présentant pas les garanties indispensables au respect de la vie privée, il convient de réaffirmer avec force les grands principes dégagés par la CNIL.

1
INFORMER LES PERSONNES : « LES LISTES NOIRES NE PEUVENT ÊTRE SECRÈTES »

Afin de garantir l'application du principe de transparence décliné par les articles 27, 34 et suivants de la loi n° 78-17 du 6 janvier 1978, la CNIL préconise l'information des personnes à plusieurs stades :
– lors de la collecte des données par l'indication du destinataire chargé de mutualiser les informations ;
– lors de la réalisation de l'incident susceptible de donner lieu à une inscription avec un délai (quinze jours ou un mois) au cours duquel une régularisation est possible (notification préalable) ;
– lors de l'inscription effective (avis d'inscription).

L'information au moment de la collecte des données doit préciser la finalité du traitement, ce qui est délicat en cas de constitution de fichier d'alerte. En 1994, lors de la constitution des fichiers de fraude à l'obtention de crédit, la CNIL avait préconisé à une société de crédit de faire figurer la mention suivante : « *Toute déclaration irrégulière pourra faire l'objet d'un traitement spécifique* », mais il s'agissait à l'époque du fichier interne à la société de crédit et non d'un fichier mutualisé portant sur les clients de sociétés distinctes.

La CNIL a pu constater, dans les dossiers de déclaration récents, une certaine réticence à faire figurer dans la mention d'information destinée aux personnes concernées, l'identité du responsable du traitement opérant la mutualisation, ainsi que la finalité du traitement. Le maintien d'une telle opacité sur les traitements mis en œuvre n'est pas admissible.

L'information des personnes doit donc se faire à plusieurs niveaux :
– au moment de l'entrée en relation avec l'organisme susceptible de procéder à l'inscription ;
– au moment de l'inscription dans le fichier.
Lorsque le fichier est géré par un organisme autre que celui auprès duquel les informations ont été collectées, la CNIL préconise de désigner en clair cet organisme, la dénomination du fichier (le cas échéant) et sa finalité.

2 LA PROPORTIONNALITÉ : PRÉSERVER LA SECTORISATION POUR ÉVITER « LA MISE AU PILORI ÉLECTRONIQUE »

Afin d'éviter le risque d'exclusion sociale découlant d'une large consultation de fichiers recensant des impayés tous secteurs d'activités confondus et de respecter le principe de proportionnalité en vertu duquel les données doivent être « pertinentes, adéquates et non excessives » par rapport aux finalités pour lesquelles elles sont enregistrées, la CNIL a, de façon constante, préconisé la sectorisation de la mutualisation de l'information avec une limitation d'accès aux seuls professionnels du secteur considéré.

Sans doute, cette préconisation de sectorisation peut paraître fragile face aux développements récents de fichiers à vocation universelle. La mutualisation des incidents de paiement tous secteurs confondus constitue un créneau pour de petites structures visant les PME ou encore les particuliers : c'est le cas de fichiers qui se font fort d'en finir

avec les mauvais payeurs de toutes catégories par une inscription accessible sur internet dès la première défaillance. Il en va de même pour certains cabinets de recouvrement de créance qui ont vocation à mutualiser l'information tous secteurs confondus et qui peuvent être tentés de commercialiser les informations relatives aux débiteurs sous forme de fichiers d'alerte, à titre préventif, et non pas seulement pour provoquer le paiement en assurant le recouvrement de la créance.

Une telle centralisation stigmatise les personnes concernées et est de nature à accroître les risques d'atteinte à leurs droits et libertés ne serait-ce que du fait des erreurs d'homonymie.

Le maintien de cette exigence de sectorisation reste ainsi un rempart contre l'exclusion sociale et la CNIL estime qu'il y a lieu d'afficher clairement cette position.

Les fichiers mutualisés ou communs ne peuvent être mis en œuvre que dans un même secteur d'activité avec des garanties propres à assurer le respect de la sectorisation qu'elles soient d'ordre technique (contrôle d'accès, gestion des habilitations, journalisation des connexions ou des interrogations) ou contractuel (insertion de clauses contractuelles prévoyant des sanctions en cas de défaut).

3 VEILLER À LA PERTINENCE DES INFORMATIONS : « DES CONDITIONS D'INSCRIPTION RÉAFFIRMÉES »

<A> Les informations relatives aux impayés

L'EXIGENCE D'UN « PRINCIPE CERTAIN DE CRÉANCE »

S'agissant d'informations relatives aux impayés, la CNIL préconise de n'inscrire que des créances pour lesquelles les conditions de paiement sont supposées remplies, c'est-à-dire pour lesquelles le créancier pourrait contraindre le débiteur au paiement et le poursuivre en justice.

La réalité et l'actualité de la créance ne doivent pas être remises en cause par les contestations du débiteur. En effet, si des éléments de fait et de droit de nature à remettre en cause ce qui constituait jusqu'alors une certitude pour le créancier étaient fournis par le débiteur, il appartiendrait alors au responsable du traitement d'apporter la preuve de la réalité de la dette.

En cas de contestation sérieuse et étayée, la CNIL préconise de suspendre l'inscription ou au minimum de signaler l'existence d'une contestation par un astérisque. Ces mesures doivent être accompagnées de l'instruction effective de la contestation par le responsable du traitement selon des modalités prédéterminées et raisonnables : par exemple un échange de correspondances entre le débiteur et le responsable du traitement sur une durée limitée.

La CNIL invite les responsables de traitement et les organismes professionnels à mettre en place une instance de médiation.

La fixation d'un seuil d'inscription : vers un seuil à géométrie variable ?

À l'instar du fichier national des incidents de remboursement du crédit aux particuliers [1] (FICP), géré par la Banque de France, la fixation d'un seuil au-delà duquel l'inscription est possible est de nature à garantir le caractère non excessif de la collecte et respecte le principe de l'adéquation de la mesure d'inscription au manquement constaté. La CNIL a également préconisé que la notification du préavis d'inscription ne puisse être effectuée tant que le seuil n'est pas atteint.

Or, la détermination d'un seuil est remise en cause par plusieurs déclarants qui ont récemment saisi la CNIL sur ce point : les responsables des fichiers mutualisés estiment que la mise en place d'un seuil priverait d'efficacité le traitement effectué dans la mesure où c'est précisément la lutte contre la multiplication des petits incidents qui est combattue.

Aussi, la CNIL s'est-elle interrogée sur l'opportunité du maintien de cette préconisation en tant que telle : l'incident caractérisé ne pourrait-il pas être établi selon des mécanismes intégrant le cumul et la gravité de l'incident ? L'addition de plusieurs petits impayés dans une durée déterminée entraînerait alors l'inscription au fichier mutualisé.

De même, si cette préconisation devait être étendue aux fichiers de risques non limités au recensement des impayés, la notion d'incident caractérisé ne saurait être cernée par un seuil. Il y a donc lieu de redéfinir les éléments permettant de justifier de la gravité des faits donnant lieu à inscription.

1 Actuellement ce seuil est de 450 euros pour le FICP.

<B> La transposition de ces garanties aux fichiers centralisant des informations autres que les impayés

La CNIL s'est interrogée sur la possibilité de transposer les recommandations développées pour les fichiers mutualisant des impayés à d'autres informations tels des manquements à des obligations contractuelles.

L'inscription d'une personne dans un fichier doit reposer sur des motifs objectifs opposables à la personne concernée, faisant abstraction de tout jugement de valeur ou d'une appréciation de son comportement et représentant un certain niveau de gravité. La CNIL recommande ainsi qu'une liste des motifs d'inscription soit préétablie, que tout motif à caractère général soit exclu de même que toute inscription sans indication de motif.

L'inscription d'une personne ou l'enregistrement de données la concernant dans un fichier destiné à recenser des « mauvais payeurs » ou des « fraudeurs » doit reposer sur des motifs objectifs opposables à la personne concernée, faisant abstraction de tout jugement de valeur ou d'une appréciation de son comportement. Les motifs d'inscription doivent être préétablis et l'inscription doit être effectuée par des agents ayant compétence pour vérifier le caractère certain du manquement imputé à la personne concernée et habilités à cet effet par l'organisme procédant à la centralisation des informations.

4 DURÉE DE CONSERVATION ET MISE À JOUR DU FICHIER : « GARANTIR LE DROIT À L'OUBLI »

Afin de garantir le droit à l'oubli dont le principe est tiré des dispositions de l'article 28 de la loi n° 78-17 du 6 janvier 1978, la CNIL préconise en matière d'impayés que l'inscription soit radiée dès régularisation de l'incident et que le responsable du traitement assure la mise à jour du fichier sur la base des informations devant être transmises par les adhérents ou membres du groupement. La CNIL recommande que la mise à jour soit contractualisée sous la forme d'une obligation à la charge de l'adhérent ou du membre du groupement. Le manquement à cette obligation devrait être sanctionné par l'exclusion de l'auteur du manquement et la suppression de toutes les inscriptions portées à son initiative. La même solution devra être retenue en cas de départ, la mise à jour ne pouvant plus être assurée.

En cas de non-régularisation, le maintien de l'inscription ne peut être considéré comme proportionné que s'il est assorti d'une limite raisonnable dans le temps.

Dans les déclarations adressées à la CNIL, la durée d'inscription s'approche souvent de cinq voire dix ans. L'allongement de la durée de conservation est préoccupant dès lors qu'il remet en cause le droit à l'oubli.

On ne peut méconnaître toutefois la difficulté de fixer une durée de conservation, d'autant plus que les diverses autorités européennes de protection des données peuvent avoir des analyses différentes et que des législations spécifiques peuvent fixer des durées de conservation. Ainsi, l'article 29 de la loi espagnole relative aux services fournissant des informations commerciales sur les crédits et la solvabilité fixe à six ans la durée de conservation des informations dès lors qu'elles corres-

pondent à la situation actuelle de la personne concernée. La loi belge du 10 août 2001 relative à la Centrale des crédits aux particuliers ayant instauré un fichier positif [2] a retenu une durée de dix ans pour le maintien d'inscriptions relatives à des impayés dans le domaine du crédit. Parallèlement, l'inscription au FICP tenu par la banque de France a été ramenée de dix à cinq ans. Une harmonisation au plan européen apparaît souhaitable sur ce point.

Les durées de conservation des données enregistrées doivent être proportionnées au regard des motifs d'inscription. Des procédures de mise à jour régulière et de suppression des informations doivent être mises en œuvre. Lorsque la mise à jour ne peut être assurée toutes les informations concernées doivent être supprimées.

5 ASSURER LA SÉCURITÉ ET LA CONFIDENTIALITÉ DES DONNÉES : « DES MOYENS HUMAINS ET TECHNIQUES

<A> Des moyens humains et matériels suffisants

L'instruction des dossiers de formalités préalables ou de plaintes a mis en exergue l'insuffisance des moyens mis en œuvre par certains res-

2 Dans le langage courant, un fichier est dit « positif » dès lors que sont enregistrés les encours de crédit alors que le regroupement des défauts de paiements constitue une centrale « négative ». Une centrale enregistrant l'ensemble des crédits souscrits par une personne ainsi que les défauts de paiement associés est ainsi un fichier positif.

ponsables de traitements pour gérer les « listes noires ». Ces listes ne sont parfois constituées que d'informations inscrites dans un tableur communiqué aux bénéficiaires par messagerie, voire même par télécopie.

De tels procédés ne sauraient être considérés comme suffisants au regard de l'obligation de moyens à la charge des responsables de traitements. Des moyens en personnel et en équipements doivent en effet permettre d'assurer la réalité des engagements pris à l'occasion de la déclaration du traitement à la CNIL.

De même, il convient :
– d'assurer une gestion rigoureuse des habilitations et des contrôles d'accès ;
– de définir une politique de journalisation et de gestion des mots de passe afin de se prémunir contre les risques d'intrusion et de détournement de finalité ;
– de déterminer des algorithmes de chiffrement avancés.

<B> Le contrôle du risque d'homonymie

La prise en compte du risque d'homonymie par la collecte du lieu de naissance en sus de la date de naissance est une préconisation constante de la CNIL soucieuse d'assurer une collecte d'informations qui permette une identification certaine du débiteur. Dans un arrêt [3] du 15 février 1994 de la cour d'appel de Paris, confirmé en cassation, le président d'une centrale professionnelle d'informations sur les impayés a ainsi été condamné pour atteinte à la sécurité de l'information sur le fondement d'un manquement à l'article 29 de la loi du 6 jan-

3 CA Paris 11e chambre A 15février 1994 RG 93/03512 confirmé par cass. crim. 19 décembre 1995.

vier 1978 : il n'avait pas pris la précaution d'ajouter dans son fichier des informations complémentaires (lieu de naissance) permettant d'éviter le risque d'homonymie.

Or, dans la majorité des traitements visant à recenser les mauvais payeurs qui sont mis en œuvre par des commerçants, les date et lieu de naissance figurent rarement dans les informations transmises puisque seules les informations portées sur la facture sont connues des commerçants. Les interconnexions de fichiers rendent cette préconisation de la CNIL indispensable. Seules les personnes identifiées de façon certaine devraient pouvoir faire l'objet d'une inscription.

La CNIL appelle dès lors l'attention des responsables de traitements sur la nécessité d'adopter des mesures permettant de pallier tout risque d'homonymie, notamment dans des cas signalés d'usurpation d'identité. Ainsi, la Banque de France, dans le cadre de la gestion du fichier central des chèques (FCC), a prévu de porter la mention « *identité usurpée* » sur les dossiers pour lesquels il est établi que l'identité du tireur a bien été usurpée et que les incidents ne lui sont pas imputables ; il s'agit d'éviter que l'escroc ne puisse obtenir d'autres ouvertures de comptes au moyen de pièces d'identité dérobées.

Enfin, il n'est pas admissible que l'interrogation d'une « liste noire » conduise à rattacher à une personne des informations relatives à une autre du fait d'une gestion statistique et automatisée de phonèmes présentant un caractère de « proximité » (par exemple nom de famille commençant par les mêmes initiales, identité de prénom et de date de naissance) ou du manque de formation du personnel ayant accès au fichier. En effet, seul le personnel ayant reçu une formation spécifique à la consultation du fichier devrait y accéder et seule l'existence d'un minimum d'autonomie de décision de ces personnes en ce qui concerne l'appréciation des suites à donner à l'interrogation du fichier peut garantir le respect des dispositions de l'article 2 de la loi du 6 janvier 1978 proscrivant toute prise de décision sur le seul fondement

d'un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé.

Assurer la sécurité et la confidentialité des informations recensées dans le fichier implique de disposer des moyens humains et techniques adaptés à la taille et à l'importance du fichier. Seules les personnes identifiées de façon certaine devraient faire l'objet d'inscription dans le fichier afin d'éviter toute erreur d'homonymie.

Propositions

Chapitre 4

Il est apparu nécessaire à la CNIL d'assurer une plus grande transparence quant à l'existence et aux modalités de fonctionnement des « listes noires », de développer dès à présent les interventions de la CNIL dans ce domaine et enfin, de suggérer un encadrement législatif spécifique en matière de fichiers constitués pour lutter contre la fraude.

1 PLUS D'INFORMATION SUR LES FICHIERS CENTRAUX DE « PERSONNES À RISQUES » AU MOYEN DE L'EXPLOITATION DU « FICHIER DES FICHIERS »

Aux termes de l'article 22 de la loi du 6 janvier 1978 :

« La CNIL met à la disposition du public la liste des traitements, qui précise pour chacun d'eux :
– la loi ou l'acte réglementaire décidant de sa création ou la date de sa déclaration ;
– sa dénomination et sa finalité ;
– le service auprès duquel peut être exercé le droit d'accès ;
– les catégories d'informations nominatives enregistrées ainsi que les destinataires ou catégories de destinataires habilités à recevoir communication de ces informations.

Sont également tenus à la disposition du public, dans les conditions fixées par décret, les décisions, avis ou recommandations de la CNIL dont la connaissance est utile à l'application ou à l'interprétation de la présente loi ».

Il est symptomatique de constater que le fichier recensant l'ensemble des traitements déclarés à la CNIL, communément appelé le « *fichier des fichiers* », est utilisé majoritairement par des déclarants qui interrogent la CNIL pour mettre à jour la liste de leurs applications déclarées et non par les personnes concernées par un fichage, alors même que le but premier du recensement mis ainsi à la charge de la CNIL par le législateur est l'information du public.

Afin d'assurer une meilleure prise en compte de cette nécessaire information, la CNIL envisage de donner une publicité élargie à un sous-ensemble de ce fichier portant sur les applications relatives aux personnes à risques.

Cependant, pour assurer la transparence des traitements mis en œuvre, les informations diffusées ne sauraient se limiter à celles limitativement énumérées par l'article 22 précité. Devraient ainsi être précisées les conditions d'inscription propres à chaque fichier, les organismes habilités à consulter le fichier, la durée de conservation des informations, les conditions de radiation et enfin, le cas échéant, l'existence d'une instance de médiation spécifiquement chargée du règlement des litiges occasionnés par la tenue du fichier.

La CNIL s'attachera à assurer la publicité des fichiers centraux recensant des « mauvais payeurs » ou des « fraudeurs » par la diffusion de notices, établies contradictoirement avec les organismes gestionnaires, régulièrement mises à jour, reprenant les règles de fonctionnement de ces fichiers ainsi que les informations pratiques permettant aux personnes fichées de s'assurer de la pertinence du traitement à leur égard.

2 DÉVELOPPER LES INTERVENTIONS DE LA CNIL

<A> De nouvelles exigences

IMPOSER UNE INFORMATION CLAIRE SUR LE PÉRIMÈTRE DU FICHIER CONCERNÉ

La transparence des fichiers centraux recensant les « mauvais payeurs » et les « fraudeurs » est essentielle à l'application des principes « informatique et libertés ».

Le premier principe dégagé par la CNIL porte ainsi sur la nécessaire information des personnes sur l'éventualité, puis la réalisation d'une inscription dans un fichier central. Mais cette information doit également préciser très clairement le périmètre du traitement et les parties prenantes à l'alimentation et à la consultation des données. À l'instar de la procédure d'inscription au FICP, l'inscription sur les fichiers mutualisés et communs à plusieurs partenaires [1] devrait ainsi être formalisée par la notification d'une mise en demeure préalable informant très précisément la personne concernée de l'étendue des partenaires destinataires de l'information.

LES GARANTIES POUR LES PERSONNES DONT L'IDENTITÉ A ÉTÉ USURPÉE

Au-delà du risque d'homonymie, le développement du fichage des personnes à risques retenant un identifiant autre que l'identité d'une personne composée de ses noms, prénoms, date et lieu de naissance, tels le numéro de téléphone, l'adresse de messagerie électronique,

1 C'est le cas notamment dans le secteur du crédit à la consommation.

l'adresse de livraison... doit conduire à l'adoption de procédés propres à alerter les utilisateurs du traitement de l'existence d'une usurpation d'identité et les invitant à effectuer des vérifications complémentaires de l'identité de la personne concernée.

La création d'instances de médiation et de contrôle

Du fait de l'opacité de ces « listes noires » et de l'absence de procédure spécifique d'instruction des réclamations relatives aux inscriptions par les responsables de ces traitements, la CNIL est conduite à jouer un rôle de médiateur, les réclamations ou demandes d'exercice de leurs droits par les personnes fichées n'étant trop souvent instruites sérieusement qu'après intervention de la CNIL.

Une solution consisterait à instaurer une instance de médiation et de contrôle, dont le principe a été évoqué par l'Institut national de la consommation (INC [2]) lors de son audition par la CNIL. Il pourrait s'agir d'un système de contrôle extérieur constitué de façon paritaire en réunissant des consommateurs et des professionnels. Le médiateur de l'Association des sociétés financières (ASF) assure en particulier ce rôle.

La création d'une instance de médiation s'impose d'autant plus que le fichier est important et est par conséquent susceptible d'occasionner un nombre accru de contestations de la part des personnes inscrites. La CNIL attache du prix à ce que soit évitée une inflation des modes autoritaires de règlement des litiges liés à l'inscription dans les fichiers de « mauvais payeurs » ou de « fraudeurs » et souhaite que se développent des modes alternatifs de règlement de litiges qui devraient être prévus en même temps que la création de tels fichiers.

---

2 L'Institut national de la consommation est un établissement public à vocation d'étude et de recherche dans le domaine de la consommation et d'aide technique aux associations de consommateur. : dix-sept associations sont agrées par l'INC représentant trois familles : les associations à vocation consumériste, les associations familiales, les centrales syndicales.

DES RÈGLES RELATIVES À LA SÉCURITÉ SPÉCIFIQUES AUX FICHIERS DE RISQUES

Au regard de la sensibilité des informations contenues dans ces traitements, l'accès par des personnes non autorisées entraîne de lourds préjudices pour les personnes concernées ; aussi, un accent particulier devrait être mis sur les règles de sécurité et de confidentialité. La CNIL sera amenée à renforcer ses exigences soit par l'adoption de règles minimales, soit par l'exclusion de procédés manifestement insuffisants au regard de l'importance et la qualité des moyens devant être mis en œuvre par le responsable d'un traitement.

De même, les organismes qui déclarent des traitements opérant des interconnexions seront invités à adresser à la CNIL un organigramme fonctionnel de l'application, en vue de permettre un contrôle des différents processus d'interrogation et d'intégration des données issues de fichiers extérieurs, de vérifier le respect de la finalité de ces traitements et de prendre en compte les dispositions de l'article 2 de la loi du 6 janvier 1978, à savoir l'interdiction de fonder une décision sur la seule base d'un traitement automatisé.

<B> Des contrôles systématiques par secteur d'activité

Afin d'assurer le respect des préconisations de la CNIL et de vérifier l'exactitude des déclarations par rapport à la réalité des traitements mis en œuvre, la CNIL a décidé de systématiser une politique de contrôle par secteur d'activité ; cette politique a été largement engagée dans le courant de l'année 2002.

LES LOUEURS DE VÉHICULES

À la suite de plaintes émanant de personnes s'étant vues refuser la location d'un véhicule automobile en raison de leur inscription sur une « liste noire », la CNIL a décidé de procéder à une série de missions de

contrôle auprès des principaux loueurs de véhicules et de leur chambre syndicale, le Conseil national des professions de l'automobile (CNPA) – branche loueurs. Les missions de vérifications effectuées dans le courant de l'année 2002 ont permis de confirmer que chacune de ces sociétés gère une « liste noire » qui lui est propre et la conduit à refuser la location d'un véhicule aux personnes qui y sont inscrites. Ce procédé a pour objectif, selon les professionnels, de se prémunir contre des clients dont le comportement peut engendrer d'importants préjudices, essentiellement financiers. Les motifs d'inscription sont généralement les impayés, les vols et dégradations des véhicules loués, la survenue d'accidents graves ou multiples dans lesquels la responsabilité du client est engagée, les fraudes diverses, en particulier l'usage de faux documents d'identité. Il arrive également qu'une rubrique à caractère plus général soit créée, parfois sous le nom de « clients suspects ».

Afin d'anticiper sur le possible regroupement de ces « listes noires » internes, la CNIL a adopté, lors de la séance du 11 mars 2003, une recommandation [3] relative à la gestion des fichiers de personnes à risques par les loueurs de véhicules.

Les cabinets de recouvrement de créance

Certaines sociétés de renseignement commercial ont développé une activité de recouvrement de créance qui s'accompagne de la tenue d'un fichier de débiteurs de créances civiles dont le caractère interne n'est pas assuré. En effet, l'examen des formalités préalables laisse apparaître l'existence plus ou moins institutionnalisée d'échanges d'informations sur les débiteurs entre les cabinets de recouvrement de créance, voire entre « partenaires ».

Plusieurs missions de contrôle ont été décidées afin de vérifier la conformité des fichiers mis en œuvre dans ce secteur avec les principes posés par la loi du 6 janvier 1978.

3 Délibération n° 03-012 du 11 mars 2003, *JORF* 17 mai 2003, p. 8515.

Il convient de rappeler que le traitement des informations recueillies à l'occasion du recouvrement d'une créance est limité par un principe de finalité défini strictement : l'information utilisée en vue du recouvrement de créance ne doit pas faire l'objet d'une mutualisation destinée à une « gestion commune du risque » ou à la définition de personnes « indésirables », utilisations qui ne pourraient que conduire à une exclusion sociale au détriment de tous les principes et garanties de protection de la vie privée et des libertés individuelles.

Les applications télébillettiques

Suite à l'instruction de la demande d'avis de la RATP relative au « passe Navigo » et à plusieurs plaintes émanant de personnes estimant que la mise en œuvre d'applications billettiques par les sociétés de transports en commun portait atteinte à leur vie privée, la CNIL a décidé de procéder à une série de missions de contrôle auprès de cinq sociétés de transport en commun.

Les missions de vérifications ont permis de confirmer que chacune de ces sociétés gère une « liste noire » qui lui est propre, afin d'invalider les titres de transports correspondant à des impayés, vol ou perte du titre de transport, ou de détecter une anomalie au niveau du titre billettique laissant supposer une fraude de nature technologique ou autre.

Il est d'autant plus nécessaire que des règles claires soient définies qu'une éventualité de mutualisation de listes noires est envisagée dans le cadre de projets prévoyant de voyager sur plusieurs réseaux avec un même titre de transport. C'est notamment le cas pour la région parisienne.

Un projet de recommandation sur les applications télébillettiques mises en œuvre par les sociétés de transport en commun est actuellement en cours de formalisation et sera adopté après une phase de concertation avec les professionnels concernés.

Le secteur bancaire

Si le développement et sans doute le changement de nature de la fraude, en particulier de la fraude au crédit, rendent légitime le souhait des professionnels de s'organiser au mieux pour s'en prémunir, seule une intervention législative spécifique paraît de nature à concilier les obligations des professionnels et les droits des personnes concernées, en imposant des règles communes, notamment sur les garanties et conditions minimales d'inscription dans de tels fichiers et, le cas échéant, la durée de conservation des informations.

La CNIL s'est en effet interrogée à plusieurs reprises sur la portée de la faculté offerte au client d'autoriser le banquier à révéler certaines des informations qu'il détient à des tiers désignés. Il lui est apparu que, sous réserve de l'appréciation des tribunaux, la souscription d'une clause particulière, dite de « levée du secret bancaire » pour des conventions ayant le caractère de contrats d'adhésion, ne permet pas d'assurer que la personne a indubitablement donné son consentement, de façon libre et éclairée, compte tenu du faible pouvoir de négociation du particulier et de l'impossibilité d'exercer son droit d'opposition. En conséquence, seule une intervention législative serait de nature à permettre une dérogation aussi large au principe du secret bancaire tel que posé par les dispositions des articles L. 511-33 et L. 511-34 du Code monétaire et financier. Au minimum, les clauses relatives au partage du secret bancaire devraient être formulées de façon beaucoup plus explicite, tant au niveau de la finalité du partage que des destinataires des informations.

Téléphonie et télécommunications

Avec l'ouverture à la concurrence depuis le 1er janvier 1998 du secteur des télécommunications fixes et la fusion des différents marchés de la téléphonie, le GIE Preventel s'est ouvert à l'ensemble des opérateurs de téléphonie. Ainsi, depuis mars 2002, le fichier peut être considéré comme le fichier recensant les incidents de paiement concernant

l'ensemble des opérateurs de télécommunications, à l'exception notable de France Télécom.

Or, la CNIL reçoit un nombre croissant de plaintes relatives à l'existence ou à la tenue de ce fichier. Ces plaintes portent sur des contestations du caractère certain de la créance inscrite, sur des inscriptions consécutives à une usurpation d'identité, une falsification du contrat ou un problème d'homonymie, sur des refus ou des demandes de dépôt de garantie opposées à des personnes au motif de leur inscription dans le fichier alors qu'elles ne le sont pas, enfin, sur le non-respect du seuil d'inscription.

En novembre 2000, la CNIL avait déjà décidé des missions de vérification sur place tant auprès du groupement d'intérêt économique Préventel qu'auprès de ses membres et des principaux opérateurs en matière de téléphonie (au total, dix contrôles ont été effectués). À l'issue de ces missions, la CNIL a été amenée à rappeler la nécessité d'appliquer les principes définis en matière de fichiers de « mauvais payeurs » et de « fraudeurs » : seuil d'inscription prédéfini, réalité de la dette, examen spécifique et contradictoire des contestations, application des dispositions de l'article 30 de la loi du 6 janvier 1978 à l'utilisation d'un code « anomalie ».

L'ouverture du GIE aux opérateurs filaires s'est traduite par une modification de la déclaration effectuée auprès de la CNIL correspondant à l'extension des conditions d'inscription : abaissement du seuil de 500 FF, soit environ 70 €, à 60 €, durée de conservation des informations relatives aux personnes ayant eu au moins trois notifications distinctes d'impayés portée de trois à cinq ans. Sur ces points, la CNIL a fait savoir au GIE que ces mesures paraissaient excessives au regard du principe de proportionnalité auquel doit obéir la mise en œuvre d'un traitement de prévention d'impayés dans le domaine de la téléphonie.

La CNIL considère tout particulièrement que, s'agissant des clients contestant le montant ou le fondement juridique de la somme dont le

paiement leur est réclamé, c'est à l'opérateur d'établir le bien-fondé de sa demande de paiement, par une instruction contradictoire de la contestation, conduite dans un délai raisonnable, de façon non-automatisée, et assortie de la suspension du processus d'inscription dans le fichier ou tout au moins d'un signalement spécifique.

Des bilans réguliers sont établis afin de vérifier l'application des principes dégagés par la CNIL.

3

LA DÉFINITION DE DÉROGATIONS LÉGALES À L'INTERDICTION POSÉE À L'ARTICLE 30

L'article 30 de la loi du 6 janvier 1978 réserve, sauf dispositions législatives contraires, aux juridictions et autorités publiques agissant dans le cadre de leurs attributions légales ainsi que, sur avis conforme de la CNIL, aux personnes morales gérant un service public, la mise en œuvre du traitement automatisé des informations nominatives concernant les infractions, condamnations ou mesures de sûreté.

Cette disposition, bien que pénalement sanctionnée par l'article 226-19 du Code pénal, n'a malheureusement pas empêché la multiplication de fichiers destinés à prévenir la fraude. S'il peut paraître paradoxal, au regard de la protection des droits et libertés, de proposer une dérogation de nature à rendre licite, dans certains cas, la centralisation d'informations relatives à des infractions, la distorsion constatée entre l'interdiction légale et la pratique se traduisant par un développement anarchique d'initiatives non sanctionnées, conduit la CNIL, après une réflexion approfondie, à considérer que seul un aménagement législatif du régime d'interdiction permettrait d'offrir une garantie effective des droits des personnes.

<A> La reconnaissance d'une légitimité à la prévention de la fraude dans certains secteurs d'activité

La CNIL a ainsi clairement indiqué qu'elle était sensible à la légitimité de l'objectif de prévention de la fraude dans le secteur du crédit mais qu'elle considérait qu'un fichier commun destiné à la prévention de la fraude devait faire l'objet d'un encadrement législatif précis sur les conditions d'inscription, la durée de conservation et les droits des personnes. De plus, un tel fichier, s'il s'avérait indispensable à la profession et socialement admis, devrait être régi par des contraintes de service public, même s'il était exploité par une société privée. La directive du 24 octobre 1995 relative à la protection des données personnelles y invite en précisant dans son article 8 (5) [4] qu'un fichier « d'infractions » peut être mis en œuvre dans le secteur privé, uniquement à la condition que des garanties appropriées soient réunies ou sous le contrôle de l'autorité publique.

Le projet de loi [5] portant transposition de la directive du 24 octobre 1995 tel qu'adopté en première lecture par l'Assemblée nationale ne prévoit cependant aucune disposition permettant de sortir de l'impasse représentée par l'interdiction posée à l'article 30 de la loi du 6 janvier 1978 au regard de la légitimité pour certains secteurs d'acti-

4 *« Le traitement de données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté ne peut être effectué que sous le contrôle de l'autorité publique ou si des garanties appropriées et spécifiques sont prévues par le droit national, sous réserve des dérogations qui peuvent être accordées par l'État membre sur la base de dispositions nationales prévoyant des garanties appropriées et spécifiques. Toutefois, un recueil exhaustif des condamnations pénales ne peut être tenu que sous le contrôle de l'autorité publique. Les États membres peuvent prévoir que les données relatives aux sanctions administratives ou aux jugements civils sont également traitées sous le contrôle de l'autorité publique. ».*

5 Le présent rapport a été adopté avant l'examen du projet de loi par le sénat qui a eu lieu le 1er avril 2003. Le projet de loi prévoit la possibilité pour *« les personnes morales victimes d'infractions, pour les stricts besoins de la lutte contre la fraude et dans les conditions prévues par la loi »* de mettre en œuvre de traitements portant sur les infractions (nouvel article 9 de la loi du 6 janvier 1978).

vité de se prémunir contre la fraude et la mise en œuvre effective de traitements ayant cette finalité. Le projet de loi reprend en effet les dispositions de l'article 30 de la loi du 6 janvier 1978 en ajoutant les seuls auxiliaires de justice alors que l'article 8 (5) de la directive européenne, qui porte sur les fichiers d'infractions, est plus large et permettrait d'envisager l'extension du champ des dérogations possibles.

La CNIL a également admis la possibilité pour les établissements de crédit de constituer des applications informatiques de lutte contre la fraude, après concertation avec la Chancellerie, compte tenu de la légitimité de tels fichiers pour les victimes des fraudes [6]. Cependant, le problème posé par le partage du savoir-faire en matière de lutte contre la fraude au crédit reste entier [7], ainsi que la nécessité de rendre le système moins opaque pour les personnes fichées qui n'ont pas conscience que le même établissement assure la gestion des crédits de plusieurs sociétés et regroupe ainsi des informations collectées dans le cadre de ses différents crédits.

L'évolution de la doctrine de la CNIL démontre qu'elle a recherché des solutions pragmatiques lui paraissant répondre à un équilibre délicat à atteindre entre la légitimité des professionnels et la protection des droits des personnes. Une prise de position est attendue de la part du législateur afin d'assurer une protection efficace des citoyens et de reconnaître aux professionnels la possibilité de tenir de tels fichiers, dans des conditions de transparence qui n'existent pas aujourd'hui.

<B> L'appréciation de la situation en Europe

Il résulte d'un examen comparatif des lois nationales transposant la directive du 24 octobre 1995 que l'article 8 (5) relatif aux fichiers

6 Rapport annuel 1994, p. 134.

7 Rapport annuel 2000, p. 168.

d'infractions donne lieu à deux grandes prises de position, s'agissant de la tenue de fichiers privés d'infractions :

– Une tendance pragmatique admet l'existence de fichiers privés d'infractions. C'est le cas de cinq États membres : l'Autriche (intérêt légitime du responsable), le Danemark (pour la poursuite d'un intérêt public prédominant), l'Italie (nécessité d'une autorisation de l'autorité de protection des données et poursuite d'un intérêt public). Le Portugal prévoit également une autorisation de la Commission qui veille au respect des droits et garanties offerts aux personnes tout en s'assurant que le responsable du traitement justifie bien d'un intérêt légitime. Les Pays-Bas sont les plus permissifs en prévoyant la tenue de tels fichiers par des opérateurs privés pour assurer la protection de leurs intérêts.

– Une tendance plus rigoureuse prohibe la tenue de fichiers privés d'infractions. Ainsi, un principe d'exclusion pure et simple est adopté par l'Espagne, la Grèce, la Suède, et la Finlande en les subordonnant à l'accomplissement d'une obligation découlant de la loi, tandis que la Belgique les admet exclusivement pour la gestion du contentieux.

<C> Les conditions d'une dérogation à l'interdiction

La prolifération récente de fichiers mutualisant au niveau d'un secteur d'activité les personnes présentant un risque de fraude [8] pose avec encore plus d'acuité la problématique liée à l'interdiction posée à l'article 30 de la loi. L'intervention du législateur aurait pour objectif de concilier les obligations des professionnels et les droits des personnes concernées en imposant des règles communes notamment sur les garanties et conditions minimales d'inscription dans de tels fichiers (définition de critères objectifs d'inscription, limitation de la durée de conservation, information des personnes afin de permettre la rectifica-

8 Voir le rapport annuel de la CNIL 2001 p. 150.

tion d'informations erronées...), et il serait souhaitable qu'un débat ait lieu sur ce point au Parlement à l'occasion de la transposition de la directive.

La possibilité de tenir des fichiers privés, et *a fortiori* mutualisés, relatifs à des infractions pourrait résulter soit d'une autorisation légale spécifique propre à chaque secteur d'activité, soit d'une autorisation de portée plus générale dans le cadre de la transposition de la directive du 24 octobre 1995 avec l'instauration d'un régime d'autorisation par la CNIL.

La définition d'autorisations légales sectorielles

L'encadrement de fichiers destinés au fichage des « fraudeurs » peut résulter de la définition d'autorisations légales sectorisées, c'est-à-dire portant sur un secteur d'activité donné, et pour un objectif prédéfini et strictement délimité : la prévention de la fraude.

Ainsi, en Espagne, une loi sectorielle prise dans le secteur du crédit prévoit, à certaines conditions, la tenue de fichiers mutualisés à l'ensemble des professionnels concernés.

Tout fichier mutualisé constitué en dehors d'un encadrement légal spécifique à un secteur d'activité défini devra être considéré comme violant les dispositions de l'article 30 de la loi du 6 janvier 1978 et dénoncé au Parquet à ce titre.

La mise en œuvre d'un régime général d'autorisation

L'instauration d'un régime général d'autorisation des traitements destinés à prévenir la fraude pourrait assurer une garantie satisfaisante de protection des droits des personnes. En effet, cela rendrait possible la tenue de tels fichiers dans un secteur d'activité précis pour des personnes justifiant de la poursuite d'un intérêt général, à savoir la lutte contre la fraude, mais dans le respect de garanties appropriées et spécifiques définies par la CNIL.

La mise en œuvre de ces traitements devrait s'accompagner de contraintes de service public, incluant notamment un devoir de neutralité, ainsi que la vérification de la qualité et de l'exhaustivité des informations traitées.

La CNIL serait, dans le cadre de la nouvelle loi, à même de vérifier les droits et garanties offerts aux personnes concernées dans la mesure où elle devra autoriser ces fichiers. Conformément à l'article 25-I. 3° du projet de loi modifiée, ces traitements seront soumis à l'autorisation de la CNIL qui pourra ainsi s'assurer de la justification de la poursuite d'un intérêt général dûment établi (la lutte contre la fraude pour un secteur d'activité donné) et imposer des conditions de fonctionnement pour ces traitements, notamment s'agissant des garanties et conditions minimales d'inscription dans de tels fichiers (définition de critères objectifs d'inscription, limitation de la durée de conservation, information des personnes afin de permettre la rectification d'informations erronées...).