Université de Montpellier I

Faculté de droit

Année :

2003

N° attribué par la bibliothèque

□□□□□□□□

MEMOIRE DE DEA INFORMATIQUE ET DROIT

Sous la direction

du professeur Jean Frayssinet

LE SYSTEME DE TRAITEMENT DES INFRACTIONS CONSTATEES (STIC) ET LA PROTECTION DES DONNEES PERSONNELLES

Présenté par :

Baffard William

Formation doctorale : Informatique et Droit

Equipe de Recherche Informatique et Droit (E.A. 2997)

Section CNU : Droit privé et sciences criminelles. 71 Sciences de l'information et de la communication.

E.R.I.D.

Remerciements

Nous tenons à remercier Messieurs les professeurs Jean Frayssinet et Michel Bibent pour le temps qu'ils consacreront à la lecture de ce mémoire, ainsi que pour la richesse de leurs enseignements respectifs.

Résumé

Le 18 mars 2003, la loi pour la sécurité intérieure, adoptée suite aux élections présidentielles de 2002 placées sous le signe de la sécurité, a reconnu l'existence du principal fichier informatique de police judiciaire, le Système de Traitement des Infractions Constatées (STIC). Ce traitement, issu du regroupement de l'ensemble des traitements automatisés et manuels utilisés par la police depuis des décennies, fonctionnait en réalité depuis une dizaine d'années, « *à titre expérimental* ».

Ce mémoire vise à retracer l'histoire complexe du STIC, en parallèle avec les difficultés qu'a connues la CNIL depuis le début des années 1990 en matière d'encadrement des traitements de données à caractère personnel du secteur public. Il aborde également les modalités dans lesquelles le STIC est censé fonctionner maintenant que la loi est venue enfin l'encadrer, et décrit les nombreux risques d'erreurs que le fichier présente.

Abstract

Français

Informatique et libertés

Protection des données personnelles

Vie privée

Fichiers de police judiciaire

Loi pour la sécurité intérieure

English

Information technology and individual liberties

Personal data protection

Privacy

Police files

Domestic security act

Plan général

Résumé 3

Plan général 4

Introduction 5

PARTIE 1 – LA MISE EN PLACE DU STIC 10

Titre 1 – La déclaration des traitements automatisés d'informations nominatives *12*

Chapitre 1 – Définitions 12

Chapitre 2 – L'exigence de déclaration de tous les traitements automatisés d'informations nominatives 19

Titre 2 – L'apparition et l'exploitation progressive du STIC *28*

Chapitre 1 – Les premières traces du projet STIC 28

Chapitre 2 – Premier dépôt du dossier à la CNIL, 1994 30

Chapitre 3 – Loi d'orientation et de programmation relative à la sécurité, 1995 31

Chapitre 4 – L' « incompréhensible » reconnaissance de l'existence du STIC par la CNIL, 1998 31

Chapitre 5 – Délibération de la CNIL "relative à un projet de décret en Conseil d'Etat portant création du STIC et application des dispositions du troisième alinéa de l'article 31 de la loi de 1978", 2000 33

Chapitre 6 – Décret portant légalisation du STIC, 2001 34

Chapitre 7 – Loi sur la sécurité quotidienne, 2001 35

Chapitre 8 – Projet de loi pour la sécurité intérieure, 2002 35

Chapitre 9 – Loi pour la sécurité intérieure, 2003 36

Conclusion de la première partie 38

PARTIE 2 – LES ENJEUX DE LA RECONNAISSANCE LEGALE DE L'EXISTENCE DU STIC 39

Titre 1 – Une légalisation longtemps réclamée par la CNIL *41*

Chapitre 1 – Le rôle de la CNIL dans cette évolution 41

Chapitre 2 – La place de la CNIL pour l'avenir 49

Titre 2 – Le fonctionnement du STIC : un traitement difficilement contrôlable *53*

Chapitre 1 – La nature des données collectées 53

Chapitre 2 – Les personnes concernées par la collecte 60

Chapitre 3 – La mise à jour des données 69

Chapitre 4 – L'accès aux données 73

Conclusion 79

Bibliographie 80

Table des matières 90

Introduction

1. - « Vous avez déjà vu un stick aussi large ? ». Ce slogan publicitaire, vantant les dimensions d'un déodorant plutôt que son efficacité, aurait pu être repris par le ministère de l'Intérieur pour décrire le Système de Traitement des Infractions Constatées (STIC) après l'adoption en mars 2003 de la loi pour la sécurité intérieure.

En effet, ce texte vient, parmi d'autres dispositions augmentant les pouvoirs de la police, étendre le domaine d'application du principal fichier informatisé de la police judiciaire, sur lequel portera cette étude.

2. - Le STIC représente un des exemples les plus réussis de traitement automatisé d'informations nominatives, du moins pour le volume d'information qu'il peut contenir, s'inscrivant dans la longue histoire des fichiers recensant des informations sur des individus.

En effet, depuis maintenant une cinquantaine d'années, les moyens informatiques ont progressivement permis, d'abord aux administrations publiques, puis aux entreprises du secteur privé, d'organiser et rationaliser leurs activités, que cela soit par le biais de logiciels de traitement de texte, de tableurs ou autres applications automatisées facilitant des tâches qui existaient déjà avant sous une forme manuelle plus fastidieuse.

3. - Toutefois, il est un domaine administratif dans lequel l'informatique a permis une réelle révolution, celui des fichiers d'informations nominatives. En effet, les administrations disposaient déjà, par nécessité, d'informations d'ordre fiscal, social ou autres, sur de nombreux individus, informations longtemps stockées sur des classiques fiches en papier, rangées dans d'envahissants classeurs et dossiers. L'informatisation a progressivement permis de stocker des quantités presque infinies d'informations dans un espace de plus en plus réduit, grâce aux progrès de la miniaturisation des supports de mémoire de masse.

Cette modernisation n'a pas seulement intéressé les services fiscaux et sociaux des diverses administrations. En effet, les services de police et de gendarmerie ont rapidement vu dans l'informatique un moyen de faciliter leurs enquêtes en conservant des informations sur les biens volés, les infractions et les suspects des affaires classées ou en cours, ainsi qu'un instrument statistique permettant de mesurer l'efficacité de leur action. Les services de police,

de même que tous les services visant à assurer la sécurité publique, disposaient déjà de fichiers manuels contenant ce genre d'informations, mais l'informatisation allait leur permettre de mieux regrouper et communiquer leurs renseignements.

4. - Ce sont précisément les modalités de ces regroupements et communications d'informations recueillies au cours des enquêtes qui sont l'objet de notre étude. En France, les traitements automatisés d'informations nominatives sont en théorie encadrés par la loi du 6 janvier 1978, souvent désignée comme la loi « Informatique et libertés »[1].

5. - Cette loi est issue d'une polémique soulevée au milieu des années 1970, quand le gouvernement avait décidé d'étendre l'utilisation du Numéro d'Identification au Répertoire National d'Identification des Personnes Physiques (NIR, le « R » résumant l'acronyme RNIPP), couramment appelé « numéro de sécurité sociale », à toutes les administrations de l'Etat, afin de faciliter la communication des dossiers, par exemple entre les services fiscaux et sociaux. Ce projet, baptisé « SAFARI » (Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus), du nom du fichier d'attribution du NIR, était préparé confidentiellement par le gouvernement, jusqu'à ce qu'un article, intelligemment intitulé « Safari ou la chasse aux Français », publié dans Le Monde[2], rende l'affaire publique.

En effet, les Français s'étaient jusqu'alors assez peu intéressés au traitement qui pouvait être fait de leurs données personnelles, oubliant presque qu'à l'origine, le NIR, qui permettait notamment de distinguer les juifs des non-juifs de la même façon qu'il indiquait le sexe de la personne, avait été utilisé par le régime de Vichy pour commettre les exactions que l'on sait.

6. - C'est suite à ce débat, facilité par la publication en 1976 du rapport réalisé, sur demande du gouvernement Chirac par la Commission dirigée par le Conseiller d'Etat Monsieur Bernard Tricot[3], que la loi put être adoptée en janvier 1978.

---

[1] Loi n° 78-17 du 6 janvier 1978, *relative à l'informatique, aux fichiers et aux libertés*, Journal officiel du 7 janvier 1978.
[2] Ph. Boucher, *Safari ou la chasse aux Français*, Le Monde, 21 mars 1974.
[3] Rapport de la Commission informatique et libertés, La Documentation française, 1975.

7. - Cette loi avait pour objet de définir un certain nombre de principes auxquels devaient se soumettre toutes les personnes exploitant un traitement de données personnelles, les « maîtres de fichiers » comme on les appelait alors.

8. - Le gouvernement avait toutefois commencé à s'interroger sur l'encadrement des ces fichiers informatisés dès le début des années 1970, notamment après que le Land de Hesse en Allemagne ait adopté en 1970 la première loi « *relative au traitement automatisé des informations nominatives* », qui servit par la suite de base à la loi fédérale de 1977. La Suède fit de même en 1973, et les Etats-Unis en 1974[4].

9. - La France avait donc un peu de retard dans ce domaine, mais il faut dire ici qu'elle l'a largement compensé en créant dans la loi de 1978, suite à un amendement du Sénat, la Commission Nationale Informatique et Libertés (CNIL), première autorité administrative indépendante, chargée de veiller au respect des dispositions de la loi.

10. - La CNIL a joué un rôle particulier tout au long de l'évolution du STIC. En effet, elle a rapidement détecté le potentiel sécuritaire et liberticide du projet, et nous verrons dans cette étude qu'elle aura toujours tenté, avec plus ou moins de succès, d'encadrer ce « mégafichier »[5].

11. - L'influence de la CNIL est un aspect d'autant plus important de cette étude que la loi de 1978 va connaître prochainement quelques modifications, avec la future loi de transposition de la directive communautaire de 1995 sur la protection des personnes physiques à l'égard des traitements de données à caractère personnel[6].

12. - La protection des données personnelles n'était en principe pas une matière dans laquelle le droit communautaire avait vocation à intervenir. Toutefois, cela a été rendu possible grâce au développement des activités économiques gravitant autour de ces données, en vertu du principe de libre circulation des marchandises, les données personnelles faisant

---

[4] A. Lucas, J. Devèze, J. Frayssinet, *Droit de l'informatique et de l'Internet*, PUF, Collection Thémis, Paris, 2001, p. 41.

[5] M. Linglet, *La CNIL légalise le mégafichier policier STIC – Information criminelle ou infractions constatées ?*, Expertises des Système d'Information, janvier 1999, p.403.

[6] 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 des Communautés européennes n° L 281 du 23 novembre 1995, p. 0031 – 0050.

désormais l'objet d'un véritable marché entre les Etats membres, au même titre que les tomates ou les automobiles.

13. - A ce propos, il peut paraître inopportun d'envisager les dispositions de la directive dans ce mémoire consacré à un fichier de police, puisque ce type de traitement représente l'exemple de domaine dans lequel le droit communautaire n'est pas compétent.

Ainsi, dans l'article définissant le champ d'application de la directive de 1995, les « *traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'Etat (…) et les activités de l'Etat relatives à des domaines du droit pénal* »[7] sont exclus.

Toutefois, le gouvernement français a unilatéralement choisi, dans un souci de cohérence de ses institutions, de soumettre le STIC aux règles prévues par la directive, de la même façon qu'il avait choisi de ne pas profiter des dérogations prévues par la loi de 1978 pour ce genre de fichier, comme nous l'expliquerons plus tard. De plus, la directive venant modifier les définitions des notions clefs de la loi de 1978, nous devons dans tous les cas aborder ces changements.

14. - La particularité du STIC a plusieurs causes. D'une part, comme tout fichier de police, il bénéficie d'une relative opacité. D'autre part, l'histoire de son apparition est particulièrement instructive pour illustrer la réticence des gouvernements, aussi bien de droite que de gauche, à accepter de le soumettre au contrôle, pourtant bien légitime puisque prévu par la loi de 1978, de la CNIL.

15. - De plus, nous verrons dans cette étude que le STIC est un traitement particulièrement dangereux, puisque les lacunes dans son contrôle, dans les conditions de son « alimentation » et de sa mise à jour, en font un « fourre-tout » à la mémoire infaillible, allant parfois contrarier les principes fondamentaux de la procédure pénale.

16. - Dans ce mémoire, nous nous intéresserons donc à la façon dont un fichier de police aussi intrusif que le STIC peut concilier son efficacité répressive et statistique avec le respect des libertés individuelles et de la vie privée des personnes figurant dans sa mémoire.

---

[7] Article 3, Directive 95/46/CE.

17. - Pour cette étude, largement basée sur une comparaison des règles gouvernant le fonctionnement du STIC avec la législation, nous commencerons par étudier comment il est apparu. En effet, cette partie historique est assez représentative de l'esprit dans lequel il a été élaboré. Pour cela, nous commencerons par décrire les formalités auxquelles sa création était soumise, avant de voir comment elles ont été respectées en pratique.

18. - Dans une seconde partie, nous étudierons plus spécifiquement le fonctionnement du STIC, toujours en comparaison avec les différentes règles et barrières mises en place pour le contrôler. Nous retrouverons régulièrement la présence, plus ou moins influente selon les époques, de la CNIL sur ce parcours.

PARTIE 1 – LA MISE EN PLACE DU STIC

19. - L'histoire de l'apparition du STIC est en elle-même symptomatique de la nature controversée de ce fichier. Elle est de plus indéniablement liée à l'évolution de la CNIL. En effet, ce fichier représente précisément ce pour quoi la loi du 6 janvier 1978[8] a été adoptée : la protection des individus contre les atteintes que les fichiers, manuels ou automatisés, pourraient porter à leur vie privée et à leurs libertés, par la compilation d'informations dites « nominatives » (ou « données à caractère personnel » selon la future appellation qui suivra la transposition de la directive de 1995[9]) dans des fichiers au contenu et a l'accès incontrôlable, à la manière du roman de George Orwell, 1984[10], décrivant un monde totalitaire dans lequel un ordinateur tout puissant, « Big Brother », surveillerait tous les individus en permanence et connaîtrait tout de leur vie privée.

20. - Bien que le STIC soit encore loin d'être un traitement permettant une telle dérive, la Commission Nationale Informatique et Libertés s'est très tôt intéressée à ce dossier, d'une part parce que ses modalités de fonctionnement lui paraissaient difficilement compatibles avec les dispositions de la loi de 1978, et d'autre part parce que les différents ministres de l'Intérieur qui ont essayé de le mettre en œuvre ont allègrement négligé les formalités prévues par la loi et les délibérations de la CNIL à ce propos.

C'est pourquoi nous commencerons cette étude en examinant dans un premier temps les règles applicables à ce genre de traitement, puis nous retracerons l'histoire de l'apparition et de la mise en exploitation confidentielle, pour ne pas dire clandestine, du STIC.

[8] Loi n° 78-17.
[9] Directive 95/46/CE.
[10] G. Orwell, *1984*, Gallimard, Paris, 1950 – Réédition Gallimard, collection Folio, Paris, 1976.

Titre 1 – La déclaration des traitements automatisés d'informations nominatives

21. - Une des principales nouveautés de la loi de 1978 a été de soumettre la création de tous les traitements d'informations nominatives à une déclaration à la CNIL[11], afin de lui permettre de s'assurer de la légitimité de l'exploitation de chaque fichier. Le STIC, en tant que fichier public, est donc soumis à une telle déclaration, dans des conditions propres aux fichiers publics, et plus particulièrement aux fichiers dits de sécurité publique.

22. - Avant de décrire les modalités de cette déclaration en fonction du type de fichier, nous définirons d'abord les notions essentielles de la loi de 1978, en prenant en compte les précisions apportées par la directive de 1995[12] et par le projet de loi de transposition de celle-ci[13].

Chapitre 1 – Définitions

23. - La loi de 1978 est axée autour de deux notions fondamentales : l'information nominative, et le traitement automatisé de ce type de données. Avant de montrer les formalités auxquelles était soumis le STIC, il importe donc de bien définir ces deux concepts, essentiels dans notre problématique. Nous commencerons donc logiquement par la définition de l'information nominative, avant de nous intéresser aux différents aspects des traitements.

Section 1 – Informations nominatives

24. - Les informations nominatives sont le réel objet de la protection apportée par la loi de 1978. C'est en effet par leur biais qu'on peut porter atteinte à la vie privée et aux libertés individuelles des personnes physiques.

---

[11] Articles 15 et s., Loi n° 78-17.
[12] Directive 95/46/CE.
[13] Projet de loi *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,* modifié et adopté par le Sénat le 1er avril 2003.

La loi de 1978 fournissant une définition de la notion d'information nominative, ce qui est assez rare dans la technique française, nous commencerons par présenter celle-ci, avant de mentionner celle, plus moderne, de donnée à caractère personnel, prévue dans la directive de 1995.

25. - A quelques mois, espérons-le, de l'adoption définitive de la loi transposant la directive de 1995 dans le droit interne, il peut paraître inopportun de revenir sur les dispositions de la loi de 1978 pour les définitions des termes, puisque celles auxquelles on se réfère aujourd'hui la plupart du temps sont celles de la directive de 1995 ou de leur adaptation, quasi-identique, dans le projet de loi en question.

Toutefois, les premières bases du Système de Traitement de l'Information Criminelle, comme il s'appelait alors, ayant été posées à la fin des années 1980[14], le début de son utilisation officielle n'ayant été annoncé en 1994, et la directive n'étant pas invocable dans l'ordre juridique français avant l'expiration du délai de transposition qui était de trois ans, soit en 1998, le droit applicable était encore celui de la loi de 1978. De plus, nous estimons intéressant de montrer comment la loi de 1978 avait déjà été conçue pour pouvoir être appliquée aux considérables progrès technologiques qui marquèrent les années 1980 et 1990.

§1 – La définition de la loi de 1978 : les informations nominatives

26. - La loi du 6 janvier 1978 définit comme nominatives toutes les informations « *qui permettent, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou une personne morale* »[15].

Dès la première lecture de cette définition, on est frappé par son imprécision. Mais c'est précisément ce qui a fait la force de la CNIL comme autorité chargée de veiller au respect de la loi de 1978, cette souplesse lui permettant de s'adapter à toutes les formes d'identification des personnes physiques possibles, que le législateur ne pouvait pas anticiper alors. C'est d'ailleurs ce qui fait la spécificité de la loi française, et de la pratique juridique continentale en

[14] Auteur inconnu, *Un rassemblement de données éparses*, Le Monde, 5 décembre 1988.
[15] Article 4, Loi n° 78-17 du 6 janvier 1978.

général : là où les systèmes juridiques de tradition anglo-saxonne prévoiront une longue liste de ce qui entre dans le champ de la définition, les juristes de tradition continentale, qu'il s'agisse par ailleurs d'une loi ou d'un contrat, prévoiront seulement une description générale et volontairement vague de ce qu'il faudra y inclure, afin de permettre des interprétations téléologiques plus difficiles à imposer dans les systèmes fournissant une liste exhaustive.

27. - C'est aussi grâce à cette qualité que la loi de 1978 ne nécessite que quelques légères modifications, dont beaucoup ne sont que des questions de terminologie, pour entrer en conformité avec la directive. La complexité de la transposition ne peut donc certainement pas être utilisée comme argument pour expliquer les cinq ans de retard de la France dans ce processus.

28. - La définition précise que l'identification permise par l'information nominative peut aussi bien être indirecte que directe. La distinction entre l'identification directe et l'identification indirecte n'est pas très claire. Monsieur le professeur J. Frayssinet propose de « *retenir l'idée que des données en apparence anonymes ou ayant de très faibles éléments d'identification peuvent, en étant rapprochées entre elles, avec une probabilité suffisante, être rapportées à une personne qui devient identifiable. Les données deviennent alors des données personnelles* »[16]. Cette distinction n'a dans tous les cas pas beaucoup d'intérêt dans le cas qui nous intéresse, puisque les informations collectées par les services de police pour alimenter le STIC sont toutes on ne peut plus directement nominatives.
Intéressons nous maintenant à la définition fournie par la directive de 1995.

§2 – La définition de la directive de 1995 : les données à caractère personnel

29. - La directive de 1995 contient un article donnant les définitions des notions clefs contenues dans ses dispositions. La notion centrale de ce texte est devenue la « donnée à caractère personnel », définie ainsi : « *toute information concernant une personne physique identifiée ou identifiable (personne concernée); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro*

[16] A. Lucas, J. Devèze, J. Frayssinet, op. cit., n°114. M. le professeur J. Frayssinet y fait un renvoi aux « *analyses ambiguës et contestables* » de l'ouvrage réalisé sous la direction de MM. les professeurs M. Vivant et Ch. Le Stanc, *Droit de l'informatique et des réseaux*, Lamy, Paris, 2002, n°508 et s.

d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale »[17].

30. - L'expression « données à caractère personnel » ne peut pas réellement être considérée comme une appellation plus moderne de ce que la loi de 1978 appelait « informations nominatives », puisqu'elle était déjà utilisée en 1981 dans la Convention *pour la protection des personnes à l'égard du traitement des données à caractère personnel* du Conseil de l'Europe[18], qui inspira largement les rédacteurs de la Directive de 1995, à l'instar de la loi française de 1978. L'expression « donnée à caractère personnel » étant souvent remplacée, dans la doctrine, par la formule, plus légère et toute aussi claire, de « donnée personnelle », nous utiliserons cette dernière pour la suite de nos développements.

31. - La définition de 1995 n'est pas beaucoup plus précise que celle donnée en France par la loi de 1978, mais on peut remarquer la référence à des « *éléments spécifiques* », ce qui permet d'inclure, en plus des informations au sens strict, des données que l'on pouvait plus difficilement faire entrer dans la catégorie des « informations », comme par exemple l'empreinte palmaire d'un individu, ou le son de sa voix, qui sont pourtant des identifiants uniques beaucoup plus fiables que l'adresse d'un domicile. Monsieur le professeur J. Frayssinet considère que la référence au nom induite par le qualificatif « *nominative* » a sans doute provoqué des interprétations étroites des catégories de données soumises à la protection de la loi[19]. Cette définition très extensive a été élaboré afin de permettre la même souplesse que celle qu'a connue la loi française grâce à la doctrine développée par la CNIL dans ce sens.

Après avoir noté le peu de changements apportés par la directive concernant les données à protéger, nous pouvons maintenant vérifier s'il en est de même pour la définition des traitements.

---

[17] Article 2 a) Directive 95/46/CE.
[18] Convention *pour la protection des personnes à l'égard du traitement des données à caractère personnel* du 28 janvier 1981 du Conseil de l'Europe (Convention 108).
[19] A. Lucas, J. Devèze, J. Frayssinet, op. cit., n° 111.

Section 2 – Traitement automatisé

32. - Les traitements sont précisément ce que la loi vise à encadrer en s'assurant de la légitimité de leur exploitation, afin de protéger les libertés des individus. L'inquiétude à l'égard des traitements de données personnelles s'est surtout développée dans les années 1970 avec le développement de l'informatique, mais cela faisait déjà plusieurs décennies que les citoyens étaient en droit de se soucier de la protection de leurs données personnelles.

En effet, les fichiers manuels, c'est à dire de simples fiches de papier stockées dans des dossiers, compilant déjà de nombreux renseignements, étaient couramment utilisés par diverses administrations, ainsi que par les services de police, notamment le vieux fichier des renseignements généraux qui avait été créé au début du XX^{ème} siècle, ou le fichier Canonge, devant son nom au policier marseillais qui créa le premier fichier mécanographique de signalements, qui contenait déjà, dans les années 1950, la photographie des personnes mises en cause dans des affaires judiciaires.

33. - On retrouve ici une sorte de malentendu qui existe toujours à propos du champ d'application de la loi : on l'appelle couramment « Loi Informatique et Libertés », mais la mise de côté de l'aspect « fichier » a eu pour conséquence de faire penser à beaucoup que la loi ne concernait que les fichiers informatisés. Or, même si la plupart des articles mentionnent effectivement les « traitements automatisés d'informations nominatives », l'article 45 de la loi prévoit que la plupart de ces dispositions sont également applicables aux fichiers manuels[20].

La notion de traitement est donc très large, comme vont nous le montrer les deux définitions que nous présenterons successivement, celle de la loi de 1978, puis celle de la directive de 1995.

§1 – La définition de la loi de 1978 : le traitement automatisé d'informations nominatives

34. - La loi de 1978 définit le traitement automatisé d'informations nominatives comme « *tout ensemble d'opérations réalisées par les moyens automatiques, relatif à la collecte,*

[20] Article 45, Loi n° 78-17.

l'enregistrement l'élaboration, la modification, la conservation et la destruction d'informations nominatives ainsi que tout ensemble l'opérations de même nature se rapportant à l'exploitation de fichiers ou bases de données et notamment les interconnexions ou rapprochements, consultations ou communications d'informations nominatives. »[21].

35. - Contrariant la tradition évoquée plus haut, selon laquelle les juristes français préfèreraient les définitions très générales plutôt que les listes exhaustives pour décrire les notions importantes des textes à valeur juridique[22], nous trouvons ici une liste des plus détaillées des opérations pouvant constituer un traitement automatisé d'informations nominatives. En réalité, cette liste est tellement large qu'elle a parfois été considérée comme « abusivement extensive »[23] par certains, puisque la CNIL a développé une doctrine autour de cette conception assez large, et que les juges se sont alignés sur cette position. Il suffit ainsi qu'une seule des opérations mentionnées soit effectuée pour que soit constitué le traitement d'informations nominatives, l'aspect préparatoire ou expérimental de l'acte étant sans effet sur la qualification[24].

36. - Comme nous le verrons dans la seconde partie, les opérations effectuées sur les données par les services de police dans le cadre du STIC correspondant, pour leur part, à toutes celles décrites par la loi, bien que la destruction des données collectées soit relativement rare dans ce domaine, il ne fait aucun doute que le STIC soit bien un traitement automatisé d'informations nominatives.

Etudions maintenant la définition fournie par la directive.

§2 – La définition de la directive 1995 : le traitement de données à caractère personnel

37. - Comme nous l'avons déjà dit, les modifications apportées par la directive de 1995 à la loi du 6 janvier 1978 portent essentiellement sur des questions de terminologie ou de forme, mais les principes restent les mêmes. Ainsi, les « traitements automatisés d'informations

---

[21] Article 5, Loi n° 78-17.
[22] cf. supra n° 26.
[23] A. Lucas, J. Devèze, J. Frayssinet, op. cit., n°125.
[24] TGI Paris, 17ème ch., 5 décembre 1991, note J. Frayssinet, Expertises des Systèmes d'Information, n°148, mars 1992, p.107 ; CNIL, 12ème rapport d'activité 1991, La Documentation française, 1992, p.30.

nominatives » sont ils devenus des « traitements de données à caractère personnel », définis comme « *toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction* »[25].

38. - Cette définition est encore plus large que celle adoptée en France en 1978. Cela est dû d'une part, à l'ajout d'opérations, dont la plupart aurait aussi bien pu entrer dans les catégories de la loi de 1978, et d'autre part à l'abandon du critère d'automatisation qui faisait l'ambiguïté de la définition française : les règles de la directive s'appliquent indifféremment à tous les fichiers de données personnelles.

39. - Face à des textes permettant des interprétations aussi extensives, certains auteurs, comme Monsieur le professeur J. Frayssinet, regrettent l'absence d'exceptions au champ d'application de la loi, qui permettraient l'exploitation de traitements de données personnelles quand ils ne représenteraient pas de danger manifeste pour les droits et libertés des personnes[26]. Il suggèrerait plutôt de raisonner en termes téléologiques, en s'interrogeant davantage sur le sens de la loi au regard de son article premier, selon lequel « *L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.* »[27]. C'est peut être dans ce sens que la directive prévoit que ses dispositions ne s'appliquent pas au traitement « *effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques* »[28].

Maintenant que nous avons vu que le STIC était un des exemples les plus représentatifs de ce qu'est un traitement de données personnelles, nous allons aborder les formalités auxquelles est soumis un tel traitement, celle-ci dépendant de son genre.

---

[25] Article 2 b) Directive 95/46/CE.
[26] A. Lucas, J. Devèze, J. Frayssinet, op. cit., n°127.
[27] Article 1, Loi n° 78-17.
[28] Article 3 2., Directive 95/46/CE.

Chapitre 2 – L'exigence de déclaration de tous les traitements automatisés d'informations nominatives

40. - La commission Tricot, formée en 1975 par le gouvernement pour étudier les problèmes liés aux traitements de données personnelles, a présenté un rapport qui a largement été repris dans le projet qui devint la loi du 6 janvier 1978[29]. Le rapport proposait un système de déclaration préalable des traitements, selon des modalités qui varieraient en fonction du type de fichier.

Nous présenterons donc d'abord les justifications de ce principe, avant d'en étudier les modalités.

Section 1 – Le principe

41. - Nous décrirons ici encore les deux régimes qu'il faut prendre en compte pour l'étude des formalités auxquelles est soumise la création du STIC : celui prévu par la loi de 1978, puis celui de la directive de 1995.

§1 – La demande d'avis ou la déclaration exigée par la loi de 1978

42. - La CNIL est l'autorité administrative indépendante qui a été créée afin de veiller au respect des dispositions de la loi[30]. Un des moyens prévus par la loi pour permettre ce contrôle est la formalité selon laquelle tout traitement automatisé d'informations nominatives doit, au moins comme nous le verrons dans la section 2, faire l'objet d'une déclaration à la CNIL, déclaration comportant l'engagement du responsable du traitement sur le respect des obligations légales dans son exploitation[31]. Cela permet, non pas de s'assurer que tous les traitements utilisés respectent scrupuleusement la loi, puisque la plupart des traitements ne sont pas déclarés, mais de pouvoir engager la responsabilité du « maître du traitement » en cas de plainte faisant suite à un manquement à ses obligations.

---

[29] Rapport de la Commission informatique et libertés, op. cit.
[30] Article 6, Loi n° 78-17.
[31] Article 15, Loi n° 78-17.

43. - En effet, une des caractéristiques de la loi de 1978 est de créer des sanctions pénales pour les cas de violation de certaines dispositions de la loi. Ces normes pénales ont même été ajoutées au nouveau Code pénal en 1994, faisant l'objet d'une section dans le titre consacré aux atteintes à la personne humaine, la section V intitulée « *Des atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques* »[32], au même niveau donc que les atteintes à la vie privée ou les dénonciations calomnieuses.

Ainsi, la personne exploitant un fichier sans avoir respecté, « *y compris par négligence* », les formalités prescrites par la loi s'expose à trois ans d'emprisonnement et à 45.000€ d'amende[33]. La loi prévoit d'autre part des peines beaucoup plus sévères pouvant aller jusqu'à 300.000€ d'amende et cinq ans d'emprisonnement, notamment pour les cas de collecte déloyale[34] ou de manquement aux exigences relatives à la sécurité des données faisant l'objet du traitement[35].

44. - L'intérêt principal de la déclaration est donc de pouvoir identifier un responsable du traitement, qui s'engagera à respecter les prescriptions légales et décrira la caractéristiques du fichier dans la déclaration.

La déclaration doit préciser l'identité du responsable du traitement, les caractéristiques, la finalité et la dénomination de celui-ci, les services chargés de le mettre en œuvre, donner les coordonnées du service auprès duquel les personnes concernées pourront exercer leur droit d'accès du traitement, les catégories de personnes ayant un accès direct aux informations enregistrées, le type d'informations recueillies, leur origine et la durée pendant laquelle elles seront conservées, les opérations effectuées sur celles-ci, signaler les rapprochements, interconnexions et mises en relation pouvant être opérés sur les informations, décrire les mesures prises pour assurer la sécurité des données, et enfin signaler si le traitement est destiné à l'expédition d'informations nominatives vers l'étranger[36]. Par la suite, toute opération ne correspondant pas à ce qui a été décrit dans la déclaration pourra être sanctionné comme détournement de finalité.

---

[32] Articles 226-16 et s., Code pénal, Dalloz, Paris, 2002.
[33] Articles 226-16, Code pénal.
[34] Article 226-18, Code pénal.
[35] Article 226-17, Code pénal.
[36] Article 19, Loi n° 78-17.

La directive de 1995 ne vient pas, ici non plus, apporter de changements considérables à cette formalité, mais apporte une nouveauté en permettant aux Etats membres de l'aménager par des simplifications et dérogations.

§2. La notification exigée par la directive de 1995

45. - Cette formalité a pris le nom de « notification » dans la directive de 1995[37].

La directive propose une liste des mentions que doit contenir au minimum la notification. Ces mentions sont le nom et l'adresse du responsable du traitement, la finalité de celui-ci, une description des catégories de personnes concernées et des données traitées, les destinataires des données recueillies, les transferts envisagés à destination des pays tiers, et une description générale des mesures de sécurité prises pour protéger les données traitées[38].

46. - La directive autorise toutefois les Etats à permettre une simplification, voire une dérogation à cette obligation, dans certains cas.

Ainsi, quand les traitements ne risquent pas de causer d'atteinte manifeste aux droits et libertés de personnes concernées, la notification peut ne mentionner que « *les finalités des traitements, les données ou catégories de données traitées, la ou les catégories de personnes concernées, les destinataires ou catégories de destinataires auxquels les données sont communiquées et la durée de conservation des données* »[39].

La deuxième dérogation possible dispense de notification le responsable du traitement qui aura désigné « *un détaché à la protection des données à caractère personnel chargé notamment: d'assurer, d'une manière indépendante, l'application interne des dispositions nationales prises en application de la présente directive,* [et] *de tenir un registre des traitements effectués par le responsable du traitement, contenant les informations visées à*

[37] Article 18., Directive 95/46/CE.
[38] Article 19., Directive 95/46/CE.
[39] Article 18. 2., Directive 95/46/CE.

l'article 21 paragraphe 2, et garantissant de la sorte que les traitements ne sont pas susceptibles de porter atteinte faux droits et libertés des personnes concernées.»[40]

47. - Le projet de loi de transposition de la directive dans le droit français prévoit déjà la création de cette fonction de « *correspondant à la protection des données à caractère personnel chargé d'assurer le respect des obligations prévues dans la présente loi et de tenir un registre des traitements effectués immédiatement accessible à toute personne en faisant la demande* »[41].

48. - Le projet de loi permet aussi l'exploitation d'un traitement de données personnelles sans déclaration préalable pour les traitements de données relatives aux membres et correspondants d'association et des partis politiques et les traitements ayant pour objet la tenue d'un registre public destiné à l'information du public.

Concernant un fichier comme le STIC, qui est placé sous la responsabilité de la police nationale, personne publique, les formalités préalables sont un peu différentes, comme nous allons le voir dans la prochaine section.

Section 2 – Les différents régimes applicables en fonction de la nature du traitement

49. - Dans les années 1970, quand l'opinion publique a pris conscience des dangers du fichage informatique, seules les administrations disposaient des moyens techniques suffisants pour exploiter de gros volumes d'informations. C'est pour cela que la loi a prévu des régimes différents pour les traitement effectués par des personnes publiques et par des personnes privées. Il était également justifié de prévoir un régime dérogatoire pour la catégorie très spécifique des traitements relatifs à la sécurité publique, dont le STIC fait partie.

§1 – La distinction entre fichiers privés et publics

[40] Article 18. 2., Directive 95/46/CE.
[41] Article 4, Projet de loi *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*, modifié et adopté par le Sénat le 1er avril 2003.

50. - Dans les années 1970, l'inquiétude de l'opinion publique n'était, à raison, suscitée que par les traitements exploités par l'administration. La loi de 1978 elle-même a été rédigée dans cette optique, selon laquelle seules les personnes publiques disposeraient des moyens techniques, donc financiers, permettant de collecter et stocker assez de données pour représenter un danger pour les libertés individuelles.

51. - C'était sans compter sur les considérables progrès qui ont marqué l'informatique dans les années qui suivirent, progrès qui permettent aujourd'hui de traiter des informations sur des milliers de personnes avec un micro-ordinateur pour un prix très modique, de les stocker sur une disquette (capacité 1,44 Mb, soit plus d'un million de caractères), un cd-rom (capacité 700 Mb), un dvd-rom (capacité pouvant aller de 4 à 17Gb), et de les transmettre en une fraction de seconde à l'autre bout de la planète grâce au réseau Internet.

52. - Ces données pouvant avoir une grande valeur commerciale après quelques simples analyses, de nombreuses sociétés ont basé leur activité sur la collecte et la revente de fichiers de consommateurs, permettant des offres commerciales ciblées. Sans faire de développement sur le « droit à être laissé tranquille » de ces personnes, on ne peut s'empêcher d'imaginer que les mêmes techniques pourraient aussi bien être utilisées à des fins politiques.

Ainsi en 1998, la chambre criminelle de la Cour de Cassation rejetait un pourvoi visant à l'annulation d'une décision dans laquelle le Front National et le Comité national des Français juifs avaient été condamnés, après dénonciation par la CNIL, pour avoir utilisé, sans déclaration à la CNIL, un « *traitement automatisé de données faisant apparaître les origines raciales ou religieuses* », en l'occurrence l'origine juive, de personnes pour leur envoyer des documents de propagande électorale appelant à voter pour le candidat du FN aux élections législatives[42]. Les dangers sont donc bien les mêmes pour les traitements exploités par des personnes privées.

53. - Il semble donc qu'aujourd'hui, la différence de régime entre les traitements publics et privés n'ait plus réellement de raison d'être. C'est d'ailleurs la raison pour laquelle, dans le projet de loi visant à transposer la directive de 1995, elle a été remplacée par une distinction plus pertinente, basée sur la nature de l'information, selon un critère matériel plutôt

[42] Cass. Crim., 3 février 1998, n° de pourvoi 96-82665.

qu'organique. Toutefois, pour les mêmes raisons qui nous ont fait étudier les définitions en vigueur à l'époque de l'apparition du STIC, nous allons ici brièvement décrire les deux régimes de déclaration prévus par la loi de 1978.

I. La simple déclaration des fichiers du secteur privé

54. - Pour les traitements ordinaires de données personnelles, ce qui revient à désigner les fichiers qui ne sont pas créés pour le compte de l'Etat, la seule formalité à remplir est une déclaration auprès de la CNIL, contenant les informations présentées plus haut[43], notamment le type d'informations recueillies, la finalité du traitement et la durée de conservation. Cette formalité suffit, et le demandeur doit ensuite attendre que le récépissé attestant de l'enregistrement de son traitement par la CNIL pour pouvoir commencer à l'exploiter.

55. - Pour les catégories de traitements les plus courants, qu'ils soient publics ou privés, la CNIL a même créé des formulaires, appelés « *normes simplifiées* » facilitant la procédure pour ces fichiers ne menaçant manifestement pas la vie privée et les libertés[44].

II – La demande d'avis pour les fichiers du secteur public

56. - Intéressons nous maintenant à ce qui fait la différence entre les fichiers privés et ceux tenus par des personnes publiques. Il existe plusieurs régimes pour les fichiers créés par des personnes publiques.

Les plus simples, mentionnés au paragraphe précédent, pour lesquels existe une norme simplifiée, ne méritent pas plus de développement.

57. - La deuxième catégorie est celle des « *traitements automatisés d'informations nominatives opérés pour le compte de l'Etat, d'un établissement public ou d'une collectivité territoriale, ou d'une personne morale de droit privé gérant un service public* »[45]. Ceux-ci sont créés par un acte réglementaire, après consultation de la CNIL qui rend un avis motivé. Il

[43] cf. supra n° 44
[44] Article 17, Loi n° 78-17.
[45] Article 15, Loi n° 78-17.

n'est possible de passer outre un avis défavorable qu'avec un décret pris sur avis conforme du Conseil d'Etat. Quand on sait qu'en pratique, le gouvernement n'est jamais passé outre un avis défavorable de la CNIL, on constate qu'il existe un réel système d'autorisation préalable dépendant de la CNIL.

Au niveau supérieur du formalisme préalable à la création du fichier, on trouve ceux intéressant la sûreté de l'Etat, la défense et la sécurité publique.

§2 – Les fichiers intéressant la sûreté de l'Etat, la défense et la sécurité publique

58. - Ce sont des fichiers qui, par leur nature même, nécessitent une certaine opacité sur les données qu'ils contiennent : on imagine en effet assez mal une personne soupçonnée de terrorisme, se sachant surveillée, exercer son droit d'accès aux données la concernant dans un fichier de police pour savoir ce que la police sait réellement d'elle. Pour permettre la création d'un tel fichier, la loi ne requiert en théorie pas de formalité particulière en plus de celles prévues pour les traitements du secteur public. Il existe même deux dispositions spécifiques prévues par la loi pour les fichiers intéressant notamment la sécurité publique.

I – L'allègement de la demande d'avis

59. - Ainsi, la demande d'avis peut être allégé par rapport à celle des autres traitements du secteur public[46]. Le décret du 28 novembre 1979[47], fixant les conditions d'application de la loi aux traitements concernant la sécurité publique, prévoit les mentions que doit comporter au minimum la demande d'avis. Ces mentions obligatoires sont : « *l'autorité qui présente la demande, la finalité et la dénomination du traitement, ainsi que le service chargé de la mise en œuvre, le service auprès duquel s'exerce le droit d'accès, les catégories de personnes qui ont accès aux informations enregistrées, les destinataires des informations, les rapprochements et interconnexions* »[48].

---

[46] Article 19 alinéa 3, Loi n° 78-17.
[47] Décret 79-1160 du 28 décembre 1979, *fixant les conditions d'application aux traitements d'informations nominatives intéressant la sûreté de l'Etat, la défense et la sécurité publique de la loi n° 78-17 relative à l'informatique, aux fichiers et aux libertés*, Journal officiel du 31 décembre 1979.
[48] D. Martin, *Les fichiers de police*, éd. PUF, coll. Que sais-je ?, n°3461, Paris, 1999, p. 14.

60. - Les mentions qui manquent par rapport au régime de droit commun sont toutefois essentielles : « *les informations nominatives traitées, leur origine et la durée de leur conservation;* […] *les dispositions prises pour assurer la sécurité des traitements et des informations et la garantie des secrets protégés par la loi ; si le traitement est destiné à l'expédition d'informations nominatives entre le territoire français et l'étranger, sous quelque forme que ce soit, y compris lorsqu'il est l'objet d'opérations partiellement effectuées sur le territoire français à partir d'opérations antérieurement réalisées hors de France* »[49].

61. - Cet allègement de la demande d'avis confère une opacité considérable au fonctionnement du traitement, en particulier si aucun contrôle n'est effectué sur le type d'informations recueillies, puisque cela ouvre la porte à la collecte d'informations dites sensibles, très encadrée pour tous les autres traitements[50].

62. - On peut également s'inquiéter du silence laissé sur la possibilité de transmettre des informations à l'étranger, notamment lorsque l'on sait que les fichiers de police destinés à la collaboration internationale, EUROPOL et le système informatique national du Système d'Information Schengen (N-SIS) sont déjà interconnectés et s'échangent en permanence des informations, parfois erronées, comme le prouvent tous les ans les chiffres publiés par la CNIL sur les rectifications apportées par suite de l'exercice du droit d'accès de certaines personnes.

Ainsi, en 2000, sur 514 personnes signalées au N-SIS ayant exercé leur droit d'accès, 183, soit 35, 6% ont obtenu la suppression de leur fiche, grâce aux investigations de la CNIL, par les services allemand (152), français (20), italien (6), néerlandais (2), espagnol (1) et belge (1)[51]. Quand on sait que certaines des données contenues dans ces traitements sont parfois transmises aux services de police et des douanes des Etats-Unis, et que des accords portant sur la collaboration entre Europol et les Etats-Unis sont en discussion[52], on peut s'inquiéter des problèmes liés à ces erreurs.

II – La dispense de publication de l'acte réglementaire portant création du fichier

[49] Article 19 alinéa 1, Loi n° 78-17.
[50] Article 31, Loi n° 78-17.
[51] CNIL, 21ème Rapport d'activité 2000, La Documentation Française, 2001, p. 13.
[52] CNIL, 23ème Rapport d'activité 2002, La Documentation Française, 2003, p. 10.

63. - L'opacité des fichiers est encore plus importante quand on applique en plus la seconde disposition spécifique aux fichiers de sécurité publique, puisque la loi permet de ne pas publier l'acte réglementaire portant création du fichier[53]. Toutefois, cette possibilité n' été utilisée qu'une fois, avec le décret du 7 mars 1986 *portant application à certains actes réglementaires relatifs à des traitements automatisés d'informations nominatives intéressant la sûreté de l'Etat, la défense et la sécurité publique des dispositions du deuxième alinéa de l'article 20 de la loi du 6 janvier 1978*, prévoyant que « *ne seront pas publiés les actes réglementaires relatifs aux fichiers gérés par la direction de la surveillance du territoire, la direction de la sécurité extérieure, et par la direction de la protection et de la sécurité de la défense* » [54], autrement dit, ce que l'on appelle communément les « services secrets ». Cela signifie que le droit commun des traitements du secteur public est appliqué aux fichiers de police en ce qui concerne la publication de l'acte réglementaire en portant création, alors qu'ils entraient a priori parfaitement dans les catégories prévues à l'article 20 de la loi du 6 janvier 1978, en tant que « fichiers intéressant la sécurité publique ».

64. - Profitant de ce renoncement à la possibilité de garder secrète la mise en place d'un fichier intéressant la sécurité publique, la CNIL est même allée jusqu'à exiger que la création du STIC se fasse par la voie législative, plutôt que réglementaire, afin de donner toute la publicité nécessaire à l'exploitation d'un tel fichier. C'est en tout cas ce qu'elle a exigé assez tôt, et que les différents ministres de l'Intérieur ont successivement refusé, tout en exploitant clandestinement le fichier, qui n'avait par ailleurs pas non plus d'existence réglementaire jusqu'en 2001 comme nous le verrons dans le titre 2 de ce premier chapitre.

[53] Article 20 alinéa 3, Loi n° 78-17.
[54] Décret n° 86-326 du 7 mars 1986 *portant application à certains actes réglementaires relatifs à des traitements automatisés d'informations nominatives intéressant la sûreté de l'Etat, la défense et la sécurité publique des dispositions du deuxième alinéa de l'article 20 de la loi du 6 janvier 1978*, Journal Officiel du 8 mars 1986.

Titre 2 – L'apparition et l'exploitation progressive du STIC

65. - Nous allons voir ici que le STIC, dont l'existence vient enfin d'être reconnue par la loi du 18 mars 2003 sur la sécurité intérieure, a connu, selon les termes de la CNIL « *de nombreuses vicissitudes* »[55] au cours de sa création. Nous retracerons donc son « histoire », des premiers projets jusqu'à sa légalisation tardive, en montrant les difficultés qu'a connues la CNIL tout au long de ce long processus, pour obtenir un certain nombre de garanties sur le fonctionnement de ce fichier, qui représente un danger potentiel considérable pour les libertés individuelles comme nous le montrerons dans le deuxième titre.

Chapitre 1 – Les premières traces du projet STIC

66. - La première communication officielle sur le STIC remonte à 1985, quand le projet de sa création fut annoncé dans un rapport annexe à la loi du 7 août 1985, *relative à la modernisation de la police nationale*[56].

67. - C'est toutefois en décembre 1990, aux « Journées internationales police et haute technologie » qui se tinrent à Nice que fut davantage décrit ce qui s'appelait alors le « Système de Traitement de l'Information Criminelle »[57]. Le projet visait alors à mettre en place, à partir de 1990, un système informatisé centralisant l'ensemble des fichiers criminels en France.

68. - Le principal de ces fichiers était alors le fichier de recherches criminelles, devenu mécanographique entre 1964 et 1970, puis électronique. Il recensait déjà des informations sur « *1,3 million d'infractions concernant 450 000 personnes (250 000 personnes connues et 200 000 signalements)* », ainsi que sur 3,5 millions d'objets volés. Il permettait alors d'identifier l'auteur d'un crime à partir d'un signalement ou de rapprochements.

69. - La nouveauté qu'apporterait le STIC serait de faciliter l'accès à ce fichier, ainsi qu'à tous les autres fichiers qui seraient regroupés pour l'occasion. En effet, le nouveau système

---

[55] CNIL, 21ème Rapport d'activité 2000, p. 73.
[56] Loi n° 85-835 du 7 août 1985, *relative à la modernisation de la police nationale*, Journal officiel du 8 août 1985.
[57] J.-Y. Nau, *L'informatisation des fichiers de la police criminelle. L'ordinateur mène l'enquête*. Le Monde, 9 décembre 1988

serait fondé sur deux principes : la décentralisation et l'unicité de la saisie. Il est en effet alors prévu que des postes de travail locaux alimenteraient des bases de données régionales, elles-mêmes liées à la base nationale. Cela permettrait une plus grande communication des informations entre les services, puisque les policiers pourraient alors interroger directement la base nationale.

Le projet prévoyait déjà également plusieurs niveaux d'accès, en fonction du grade et de la spécialité du policier, afin d'éviter que tout gardien de la paix ait accès à des informations exigeant une certaine discrétion.

Ce système d'accès à plusieurs niveaux se ferait par le biais d'une carte magnétique propre à chaque agent, ce qui permettrait en plus de tenir une sorte de journal des consultations, afin de contrôler que celles-ci sont bien effectuées en conformité avec les attributions et enquêtes de l'agent.

70. - Il était de plus déjà prévu que les fichiers régionaux et national seraient en liaison avec les fichiers des personnes recherchées, des véhicules volés, des renseignements généraux, des visas et des cartes grises. Dès le début, le STIC était donc destiné à recouper une masse considérable d'informations contenues dans des fichiers à finalités différentes.

71. - Les principales justifications fournies pour l'exécution de ce projet étaient alors la modernisation des moyens de lutter contre le crime mis à la disposition des services de police, afin de rattraper le retard qui caractérisait alors la France vis à vis des autres pays.

72. - On peut noter que le projet ne mentionnait alors aucune utilisation à des fins administratives, ni aucun moyen pour les personnes concernées d'exercer leur droit d'accès. Rien n'est non plus prévu concernant le contrôle des données ou leur mise à jour.

73. - Au cours de cette annonce aux « Journées internationales police et haute technologie », M. Jacques Genthial, responsable de la sous-direction de la police technique et scientifique au ministère de l'intérieur, prévoyait le début de l'exploitation « expérimentale »

en grandeur réelle du STIC au début de l'année 1990 dans la région de Reims, avec une extension à l'ensemble du territoire effective cinq ou six années plus tard[58]. Le dossier ressortit toutefois avant cette échéance, en 1994.

Chapitre 2 – Premier dépôt du dossier à la CNIL, 1994

74. - En effet, en 1994, M. Charles Pasqua, alors ministre de l'intérieur, demande officiellement à la CNIL son avis sur le Système de Traitement de l'Information Criminelle.

Cela fait alors plusieurs années que le STIC fonctionne, toujours à titre expérimental, mais il ne correspond déjà plus exactement à ce qui avait été décrit en 1988. En effet, selon la CNIL, le dossier présenté était alors « *beaucoup plus qu'un fichier de police judiciaire : l'intégralité des procès-verbaux de la police judiciaire devait y figurer et être accessible non seulement aux officiers de police judiciaire mais aussi aux autorités administratives. En outre, les témoins d'une infraction devaient être fichés au même titre que les auteurs.* »[59].

Face à l'ampleur du projet, la Commission a eu besoin de « *plusieurs réunions de travail et de visites sur place* »[60], interventions qui dérangeaient apparemment le ministre de l'intérieur puisqu'il retira plusieurs fois le dossier à la CNIL, à tel point que le 11 décembre 1997, celle-ci dut envoyer un courrier au Premier ministre, pour attirer son attention sur les obstacles qui venaient perturber l'avancement de son étude.

75. - Le 23 février 1998, le Premier ministre répondit à la CNIL qu'il avait demandé au ministère de l'Intérieur, « *en liaison avec le garde des sceaux, ministre de la Justice et le ministre de la Défense » de préparer un nouveau dossier de demande d'avis* »[61].

[58] J.-Y. Nau, op. cit.
[59] CNIL, *Communiqué de presse relatif au Système de Traitement des Infractions Constatées (STIC)*, 3 décembre 1998
[60] CNIL, 21ème Rapport d'activité 2000, p.73.
[61] CNIL, 21ème Rapport d'activité 2000, p.73.

Chapitre 3 – Loi d'orientation et de programmation relative à la sécurité, 1995

76. - Entre temps, en 1995, le ministère de l'Intérieur avait évoqué le STIC comme une de ses priorités, dans une document annexé à la loi d'orientation et de programmation *relative à la sécurité*[62].

77. - La justification de cette mise en priorité de la création du STIC était un argument que le ministère avait souvent utilisé et utilisera souvent par la suite, le besoin de modernisation des méthodes d'investigation de la police, afin de rattraper le retard sur ses homologues européens. Les raisons de rattraper ce retard sont doubles : d'une part améliorer les recherches de délinquants en permettant d'interconnecter les différents fichiers existants, et d'autre part disposer d'un meilleur outil statistique sur l'étude de la criminalité. C'est d'ailleurs pour cela que le mégafichier s'appelait encore « Système de Traitement de l'Information Criminelle ».

Chapitre 4 – L' « incompréhensible »[63] reconnaissance de l'existence du STIC par la CNIL, 1998

78. - Finalement, en 1998, après trois examens du dossier, la CNIL a rendu un avis favorable à la création du STIC[64], émettant toutefois un certain nombre de réserves. C'est après cette délibération que le dossier STIC commença à attirer l'attention.

79. - En effet, la presse ne s'était jusqu'alors pas vraiment intéressée à la situation, qu'il s'agisse de la presse généraliste ou de la presse juridique spécialisée. De même, aucune contestation professionnelle ne s'est élevée contre le projet, alors que les avocats et parquets auraient eu intérêt à se manifester, respectivement pour leurs plaidoiries quotidiennes et mission de contrôle du dossier[65]. Au moment même où fut adoptée cette délibération, l'attention des journalistes était davantage concentrée sur le projet d'extension du NIR par les services fiscaux.

---

[62] Loi 95-73 du 21 janvier 1995, Loi d'orientation et de programmation *relative à la sécurité*, Journal officiel du 23 janvier 1995.
[63] M. Linglet, *Le fichier informatisé STIC, Réflexions et témoignages. Un « pré-jugement » policier*, Expertises des Système d'Information, Juin 2000, n°238, p.166.
[64] Délibération de la CNIL n° 98-097 du 24 novembre 1998, *portant avis sur le projet d'arrêté interministériel relatif à la création du système de traitement de l'information criminelle (STIC) et sur le projet de décret présenté par le Premier ministre en application de l'article 31 - alinéa 3 de la loi du 6 janvier 1978.*
[65] M. Linglet, *Le fichier informatisé STIC, Réflexions et témoignages.* op. cit.

80. - La finalité déclarée du STIC était alors « *la rationalisation du recueil et de l'exploitation des informations contenues dans les procédures judiciaires aux fins de recherches criminelles, de statistiques et de gestion des archives* ».

81. - Face à ces multiples finalités, la CNIL a donc exigé « *de très sérieuses garanties* ».

La première réserve formulée par la CNIL dans son avis portait sur la dénomination du traitement. En effet, l'enregistrement des données devant concerner les « *personnes mises en cause* » dans des affaires portant sur des crimes, délits et six contraventions de cinquième classe (les violences volontaires avec incapacité totale de travail inférieure ou égale à 8 jours ; le racolage ; la destruction ou dégradation volontaire d'un bien appartenant à autrui avec dommage léger ; le port ou l'exhibition d'uniformes, d'insignes ou d'emblèmes rappelant ceux d'organisations ou de personnes responsables de crimes contre l'humanité ; l'intrusion dans les établissements scolaires ; la provocation non publique à la discrimination, à la haine ou à la violence raciale), la mention du terme « *criminelle* » dans le nom du fichier apparaissait alors inappropriée, et aurait pu constituer une atteinte à la présomption d'innocence. C'est pourquoi la CNIL a préféré proposer la dénomination de « *Système de Traitement des Infractions Constatées* », plus neutre, et ayant l'avantage de conserver l'acronyme STIC, facile à utiliser, même si peu ont pensé que cela pouvait rappeler l'anglais « *stick* », pouvant désigner aussi bien un simple bâton que la matraque du policier[66].

82. - Les autres réserves ayant été suivies par le ministère de l'Intérieur, nous les aborderons dans la partie consacrée aux apports de la CNIL sur la création du STIC. Il nous paraît en effet plus approprié de ne mentionner le contenu de la recommandation dans une autre partie que celle-ci, davantage consacrée à l' « histoire » du STIC. Nous pouvons toutefois déjà signaler ici une réserve importante : l'interdiction d'utiliser le STIC à des fins administratives.

[66] *Sommes-nous tous fichés ?*, www.transfert.net, 14 mars 2002.

Chapitre 5 – Délibération de la CNIL "*relative à un projet de décret en Conseil d'Etat portant création du STIC et application des dispositions du troisième alinéa de l'article 31 de la loi de 1978*", 2000

83. - Cette délibération[67] a été prise en application des dispositions de l'article 31 de la loi du 6 janvier 1978, encadrant strictement les traitements manipulant des données dites « sensibles », c'est à dire faisant apparaître « *les origines raciales ou les opinions politiques, philosophiques ou religieuses ou les appartenances syndicales ou les mœurs* [cette expression sera remplacée par « *la vie sexuelle* » dans la loi modifiée par la directive[68]] des *personnes* »[69].

84. - Ainsi, un tel traitement peut être permis dans quatre cas : s'il est réalisé avec l'accord exprès des personnes concernées, s'il est réalisé par les Eglises, groupements à caractère religieux, philosophique, politique ou syndical à propos de leurs membres ou correspondants, ou pour des motifs d'intérêt public, sur avis conforme de la CNIL par décret en Conseil d'Etat, ou enfin si le traitement est réalisé par des organismes de la presse écrite ou audiovisuelle quand une application stricte de l'article 31 aurait pour effet de limiter l'exercice de leur liberté d'expression. C'est donc la troisième exception qui a motivé cette délibération : les motifs d'intérêt public que constitue la sécurité publique.

En effet, comme nous le verrons dans la seconde partie, le STIC manipule, par nécessité, de ces données parfois qualifiées de « sensibles ».

85. - Cette délibération est intervenue après consultation, « notamment d'un certain nombre d'associations de sauvegarde des droits de l'homme et de syndicats de police »[70].

Cette délibération reprenant essentiellement les réserves formulées en 1998, nous n'en parlerons pas plus ici. On peut toutefois noter que la proposition de la CNIL de changer la signification de l'acronyme « STIC » a bien été retenue depuis cette délibération. Un des

---

[67] Délibération de la CNIL n° 00-064, *relative à un projet de décret en Conseil d'Etat portant création du « Système de Traitement des Infractions Constatées (STIC) » et application du troisième alinéa de l'article 31 de la loi du 6 janvier 1978,* 19 décembre 2000.

[68] Article 2, Projet de loi *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*, modifié et adopté par le Sénat le 1er avril 2003.

[69] Article 20 alinéa 3, Loi n° 78-17.

[70] C. Charbonneau, F. Pansier, *Le Système de Traitement des Infractions Constatées ou les faits infractionnels à l'épreuve de la « memory S.T.I.C. »*, Les Petites Affiches, 24 août 2001, n°169, p. 4.

principaux apports de cette version du projet fut aussi la distinction entre mise à jour et effacement des données conservées dans le STIC.

Chapitre 6 – Décret portant légalisation du STIC, 2001

86. - Faisant suite à aux avis conformes de la CNIL et du Conseil d'Etat, le gouvernement publia le 5 juillet 2001, un décret venant enfin, pour la première fois, donner un statut légal au STIC[71].

87. - Ce décret fut fortement critiqué pour avoir été adopté discrètement au début du mois de juillet, époque de l'année où l'activité réglementaire est généralement assez calme, et où les journalistes sont moins attentifs, ce qui contribua à confirmer l'idée, que nous vérifierons par la suite, selon laquelle le ministère de l'Intérieur, quel qu'en soit le bord politique, le gouvernement en 2001 étant de « gauche plurielle », ne tient pas particulièrement à ce que l'existence du STIC et son fonctionnement soient connus de tous.

88. - Une circulaire destinée à expliquer concrètement le fonctionnement du STIC fut également publiée peu de temps après le décret[72]. Elle donnait notamment une définition de cette notion très controversée de « personne mise en cause », et décrivait comment les procédures de mise à jour et d'accès aux dossiers, ce qui tendait à prouver l'infaillibilité du STIC en matière à la fois statistique, répressive et de respect des libertés individuelles et de la vie privée.

89. - C'est sur la base des principes prévus dans ce décret que la loi sur la sécurité intérieure de mars 2003 autorise la police et la gendarmerie à mettre en place des applications automatisées d'informations nominatives.

---

[71] Décret n° 2001-583 du 5 juillet 2001 *pris pour l'application des dispositions du troisième alinéa de l'article 31 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et portant création du système de traitement des infractions constatées*, Journal officiel du 6 juillet 2001.

[72] Circulaire de la direction des affaires criminelles et des grâces, *présentation des dispositions du décret n° 2001-583 du 5 juillet 2001 pris pour l'application des dispositions du 3e alinéa de l'article 31 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et portant création du système de traitement des infractions constatées (STIC)*, Bulletin officiel du ministère de la Justice n°83, du 1er juillet au 30 septembre 2001.

Chapitre 7 – Loi sur la sécurité quotidienne, 2001

90. - Suite aux événements du 11 septembre 2001 à New York, les autorités françaises ont décidé de mettre en place des mesures exceptionnelles pour lutter contre la menace terroriste. C'est ainsi que fut adoptée la loi sur la sécurité quotidienne le 15 novembre 2001[73], prévoyant des mesures plus rigoureuses devant être appliquées jusqu'au 31 décembre 2005[74].

91. - Certaines de ces mesures entraient dans le champ de la loi de 1978, mais la loi sur la sécurité quotidienne ayant été modifiée par la loi sur la sécurité intérieure, nous aborderons leurs apports dans une autre section.

Chapitre 8 – Projet de loi pour la sécurité intérieure, 2002

92. - Suite aux élections d'avril 2002, placées sous le signe de la sécurité et de la répression, le ministre de l'Intérieur a présenté son projet de loi pour la sécurité intérieure[75], annonçant le contenu de la loi pour la sécurité intérieure adoptée en mars 2003.

93. - Ce projet s'articule autour de trois objectifs : « *faciliter les enquêtes en rendant certaines règles de la procédure plus efficaces ; mieux réprimer des comportements qui affectent particulièrement la vie quotidienne de nos concitoyens et se sont multipliés impunément au cours des dernières années ; renforcer l'autorité et la capacité des agents publics de la sécurité, tout en leur assurant une meilleure protection juridique ainsi qu'aux membres de leur famille* »[76].

94. - Avec un tel programme, il est évident qu'une attention toute particulière doit être portée à l'application de cette loi. D'ailleurs, qu'il s'agisse de la protection des données personnelles ou du principe de présomption d'innocence, de nombreuses voix se sont élevés contre ce projet, parfois qualifié de « liberticide ».

95. - C'est dans l'objectif d' « *améliorer l'efficacité du travail des forces de sécurité intérieure* » que la loi aborde la question des données personnelles. Ainsi, la principale

---

[73] Loi n° 2001-1061 du 15 novembre 2001 *sur la sécurité quotidienne*, Journal officiel du 16 novembre 2001.
[74] Article 22, loi n° 2001-1061.
[75] Projet de loi *pour la sécurité intérieure*, 23 octobre 2002.
[76] *La sécurité, première des libertés*, texte décrivant le projet de loi *pour la sécurité intérieure*, 23 octobre 2002.

mesure prise dans ce domaine a été la mise en commun des fichiers de la police (STIC) et de la gendarmerie (JUDEX), afin de faciliter les enquêtes. Il faut tout de même signaler ici qu'avant cette loi, le fichier JUDEX de la gendarmerie nationale, fonctionnant sur le même modèle que le STIC, n'avait absolument aucune existence légale.

96. - Pour un projet d'une telle ampleur, il aurait fallu, comme le prévoit la loi de 1978[77], consulter la CNIL pour avis. Mais le ministre de l'Intérieur s'en est abstenu, pensant peut être que le recours à la voie législative pour faire passer ces importantes interconnexions de fichiers n'ayant pas nécessairement les mêmes finalités suffirait à faire oublier ce mépris de la loi.

97. - Face à cette irrégularité, la CNIL, en la personne de son président Monsieur Michel Gentot, prit la décision de s'autosaisir, dès le lendemain de la présentation du projet par Monsieur Nicolas Sarkozy, pour la première fois de son histoire, pour donner son avis sur le projet de loi[78].

Le contenu du projet de loi étant le même que celui de la loi, nous les aborderons ensemble dans le prochain chapitre.

Chapitre 9 – Loi pour la sécurité intérieure, 2003

98. - Entre l'annonce du projet en octobre 2002 et le vote définitif de la loi pour la sécurité intérieure en mars 2003, l'opinion publique s'est enfin réveillée face aux risques auxquels elle se trouverait exposée en cas d'application rigoureuse de la loi. Cela n'a toutefois pas empêché son adoption.

Section 1 – La décision du Conseil Constitutionnel

99. - Le Conseil Constitutionnel a été saisi par les députés afin de vérifier la constitutionnalité de la loi. Dans une décision du 13 mars 2003, le Conseil a considéré que « *l'ensemble des garanties que ce texte offre en matière de création et d'utilisation des*

[77] Article 15, loi n° 78-17.
[78] CNIL, *Position de la CNIL sur les dispositions du projet de loi pour la sécurité intérieure relatives aux fichiers de police judiciaire et au fichier national automatisé des empreintes génétiques* - Séance du 24 octobre 2002

fichiers de police « est de nature à assurer, entre le respect de la vie privée et la sauvegarde de l'ordre public, une conciliation qui n'est pas manifestement déséquilibrée »[79].

100. -En plus des garanties déjà exigées par la CNIL, le Conseil a relevé que les destinataires des informations contenues dans le STIC étaient limitativement énumérées et habilitées, et que l'article 39 de la loi de 1978, relatif à l'exercice du droit d'accès, avait été modifié, comme le nécessitaient les mesures proposées dans la loi. Le Conseil émit toutefois une réserve, exigeant que toutes les personnes fichées puissent exercer ce droit d'accès.

101. -Dans une réserve expresse, le Conseil rappelle que ces traitements restent soumis aux dispositions de la loi du 6 janvier 1978.

Pour le reste, les dispositions de la loi ont été admises par le Conseil Constitutionnel. Nous allons donc les décrire maintenant.

Section 2 – Le contenu de la loi pour la sécurité intérieure

102. -La loi n'a pratiquement pas connu de changement entre le projet présenté en octobre 2002 et le vote en mars 2003. Nous n'aborderons ici que les dispositions relatives aux fichiers de police judiciaire, la loi contenant d'autres dispositions relatives aux données personnelles dans le cadre du Fichier National Automatisé des Empreintes Génétiques, qui nous concerne moins.

103. -C'est le chapitre V de la loi, intitulé « *Dispositions relatives aux traitements informatisés d'informations* » qui nous intéresse ici.

Il prévoit enfin de donner un statut légal aux fichiers de police judiciaire[80], en en définissant les contours, les caractéristiques et les destinataires.

Il décrit d'autre part les organismes étrangers ou internationaux pouvant être destinataires des informations recueillies, précisant que seuls les pays présentant les mêmes garanties que

---

[79] Conseil Constitutionnel, décision du 13 mars 2003, citée dans le 23ème rapport d'activité de la CNIL pour 2002, La Documentation Française, 2003.
[80] Article 21, loi n° 2003-239 du 18 mars 2003, *pour la sécurité intérieure*, Journal Officiel du 19 mars 2003, p. 4761.

celles valables dans le droit interne en matière de sécurité pourraient se voir communiquer ces données[81].

104. -Une disposition contre laquelle la CNIL avait lutté depuis les débuts de la vie officielle du STIC a toutefois été adoptée : celle permettant d'utiliser les fichiers de police judiciaire non plus à des fins de police administrative mais à des fins de simple administration[82].

Conclusion de la première partie

105. -Dans cette partie, nous avons vu qu'entre les premiers projets (1985) et la reconnaissance légale de l'existence du STIC (2003), les différents ministères de l'Intérieur, une fois encore quel qu'en soit la couleur politique, ont toujours été un peu embarrassés par ce dossier, ce qui les a longtemps poussés à reculer la date de l'examen officiel du dossier STIC par la CNIL, le Conseil d'Etat et le Conseil Constitutionnel, et à violer allègrement les règles les plus fondamentales concernant un traitement de données personnelles de ce type.

106. -Dans la prochaine partie, nous essaierons de montrer ce qui, dans le fonctionnement de son Système de Traitement des Infractions Constatées, a pu l'inciter à négliger l'examen pour avis du projet de loi sur la sécurité intérieure à la CNIL.

[81] Article 24, loi n° 2003-239.
[82] Article 25, loi n° 2003-239.

PARTIE 2 – LES ENJEUX DE LA RECONNAISSANCE LEGALE DE L'EXISTENCE DU STIC

107. -Après avoir étudié l'histoire du STIC, nous allons tenter dans cette partie d'expliquer, à travers son fonctionnement, pourquoi, depuis le début, ce fichier de police judiciaire provoque autant de commentaires et controverses, certains allant jusqu'à qualifier la loi le légalisant de « liberticide ».

108. -Nous montrerons comment le reconnaissance de l'existence du STIC par la voie législative a été un long combat de la CNIL, avant d'expliquer pourquoi cette autorité administrative indépendante est toujours restée attentive à l'évolution du projet.

Titre 1 – Une légalisation longtemps réclamée par la CNIL

109. -En tant qu'autorité administrative indépendante, créée par la loi du 6 janvier 1978 afin de « *veiller au respect des dispositions de* [la] *présente loi* »[83], il a donc toujours été de la compétence de la CNIL de s'assurer que les traitements mis en œuvre, aussi bien par les personnes privées que publiques, seraient en conformité avec le cadre défini par la loi.

110. -Dans cette partie, nous allons donc montrer la place qu'a tenue la CNIL dans ce domaine dans la création du STIC, avant d'envisager l'avenir qui se profile pour cette précieuse institution, le projet de loi de transposition de la directive de 1995 prévoyant déjà des changements dans ses prérogatives[84].

Chapitre 1 – Le rôle de la CNIL dans cette évolution

111. -Nous verrons ici comment la CNIL a pu accomplir efficacement sa mission depuis l'entrée en vigueur de la loi en 1980, malgré des problèmes qu'elle a constamment connus.

Section 1 – Une protectrice de la première heure de la vie privée et des libertés individuelles

112. -La CNIL a donc depuis sa création toujours eu à s'occuper de projets de traitements délicats. L'idée selon laquelle les fichiers publics sont le principal danger en matière de protection des données personnelles est certes un peu obsolète, face à l'évolution des techniques aujourd'hui accessibles à tous, mais les traitements du secteur public ont tout de même toujours eu, et ont encore aujourd'hui comme en atteste le STIC, un potentiel important d'atteinte à la vie privée.

En effet, les affaires les plus retentissantes dont elle a eu à traiter sont les fichiers de la gendarmerie en 1981, la carte d'identité informatisée en 1980 et 1986, les décrets sur les fichiers des renseignements généraux en 1990 et 1991, la vidéosurveillance en 1994, le fichier

---

[83] Article 6, loi n° 78-17.
[84] Projet de loi *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,* modifié et adopté par le Sénat le 1er avril 2003.

électoral de la mairie du IIIème arrondissement, l'utilisation du NIR dans les fichiers fiscaux[85], et bien sûr, le STIC depuis 1994.

Nous n'aborderons ici que les apports de la CNIL concernant le STIC.

§1 – L'élaboration d'un « corps de règles » applicables aux fichiers de police

113. -En 1990, la CNIL fut consultée dans le cadre d'un projet de décret visant à réglementer, après des années d'utilisations clandestines, le fichier des renseignements généraux. Elle définit alors un « corps de règles », fixant des principes fondamentaux pour le respect desquels elle serait intraitable.
Les règles définies pour les renseignements généraux étant transposables aux fichiers de police judiciaire, la CNIL les réaffirma dans la communiqué de presse[86] qui suivit sa délibération du 24 novembre 1998[87].

114. -La première de ces règles est l'interdiction de collecter des informations sur les témoins des affaires concernées par le traitement. Cette règle n'apparaît pas expressément dans la délibération de 1998, mais elle fut soulignée dans le communiqué, avant d'être consacrée dans la délibération de 2000 sur le projet de décret en Conseil d'Etat[88].

Ce principe était essentiel car il permettait de préciser le cadre des personnes sur lesquelles pouvaient être collectées les informations au cours des enquêtes. En effet, le ministère de l'Intérieur voulait pouvoir recueillir des données sur les victimes et les « personnes mises en cause ». Comme nous le verrons plus tard, cette notion de « personne mise en cause » est assez vague, et le ministère aurait voulu y inclure les témoins. Grâce à la CNIL, cela a pu être évité.

115. -La CNIL a également tenu à interdire les consultations du STIC à des fins de simple enquêtes administratives de moralité, du type de celles effectuées à l'occasion de recrutement pour des emplois dans la fonction publique. Selon la CNIL, seul le bulletin n° 2 du casier

---

[85] F. Paoletti, *Informatique et libertés : principes et concepts*, extrait du colloque « *Que ne peut l'informatique ?* » organisé les 27, 28 et 29 octobre 1999 au Conservatoire National des Arts et Métiers de Paris.
[86] CNIL, *Communiqué de presse relatif au STIC*, op. cit.
[87] Délibération de la CNIL n° 98-097.
[88] Délibération de la CNIL n° 00-064.

judiciaire, au contenu strictement encadré, comme nous le verrons également plus tard, et accessible par l'administration, devrait être consulté à cet effet.

Toutefois, sur ce terrain, la CNIL a perdu, puisque la loi sur la sécurité intérieure permet désormais ce genre de consultation [89].

La CNIL souligne tout de même, probablement pour minimiser cet échec, que cela n'a été permis que par le biais d'un amendement gouvernemental adopté lors des débats sur le projet de loi sur la sécurité quotidienne, qui intervinrent juste après les événements du 11 septembre 2001, ce qui justifia une telle mesure.

116. -La troisième règle fondamentale « imposée » par la CNIL fut la proportionnalité des durées de conservation à la gravité des infractions commises et à l'âge des personnes mises en cause. En effet, le projet du ministère de l'Intérieur prévoyait des durées de conservation uniformes pour toutes les infractions susceptibles de faire l'objet d'un fichage, et le statut des données collectées sur les mineurs mis en cause n'était pas des plus clairs.

Ici, la CNIL a obtenu que les informations collectées sur des mineurs soient effacées au bout de cinq ans, de même que pour les infractions commises par des majeurs, ne portant pas d'atteinte à l'ordre public, telles que l'abandon de famille, la non-présentation d'enfant ou encore les infractions d'usage de stupéfiant.

117. -La CNIL a tenu à ce que les personnes puissent avoir un accès direct aux informations les concernant dans le STIC. Les modalités d'accès à ce fichier méritent des précisions.

En effet, la loi de 1978 a prévu des dispositions spéciales concernant les « *traitements intéressant la sûreté de l'Etat, la défense et la sécurité publique* ». C'est ce que certains ont appelé, abusivement, le droit d'accès « indirect », qui consiste pour le requérant à demander à la CNIL de vérifier si les traitements de ce type contiennent des informations les concernant. Le membre de la CNIL effectuant cette mission peut alors vérifier la présence d'informations, leur authenticité, et éventuellement les modifier, voire les effacer, notifiant par la suite au

[89] Article 25, loi n° 2003-239.

requérant « *qu'il a été procédé aux vérifications* »[90]. Le requérant ne se voyant jamais communiquer l'information détenue par le gestionnaire du fichier, il n'y a simplement pas d'accès à celle-ci, ni direct ni indirect.

118. -Toutefois, en 1991, le décret encadrant le fichier des renseignements généraux a créé un autre régime, entre l'accès direct aux données existant déjà pour les autres fichiers, et l'accès défini ci-dessus, selon lequel le requérant pourra se voir transmettre les informations le concernant, avec l'accord du ministre de l'Intérieur, si la communication de celles-ci ne met pas en cause la sûreté de l'Etat, la défense et la sécurité publique.

La loi sur la sécurité intérieure vient d'étendre ce régime hybride institué en 1991 pour le fichier des renseignements généraux à l'ensemble des fichiers de sécurité publique, modifiant pour cela l'article 39 de la loi de 1978[91].

119. -La cinquième règle définie par la CNIL au cours de l'instruction du dossier STIC, concerne la mise à jour des informations. En effet, la saisie des informations devant « *s'effectuer directement à partir d'un logiciel de rédaction des procédures mis à la disposition des fonctionnaires de la police nationale afin d'alléger leur tâche de saisie répétitive des informations* », sans autre contrôle judiciaire immédiat, il importe que les personnes apparaissant dans le STIC et « *ayant bénéficié d'une décision de non-lieu, de relaxe ou d'acquittement devenue définitive ou, à l'expiration du délai de prescription de l'action publique, d'une décision de classement sans suite, puisse*[nt] *demander directement au procureur de la République ou, par l'intermédiaire de la CNIL à l'occasion de l'exercice du droit d'accès, que les informations qui la concernent soient, en application de l'article 37 de la loi du 6 janvier 1978, mises à jour et qu'il en soit de même pour toutes les personnes ayant bénéficié de l'amnistie ou d'une mesure de réhabilitation légale ou judiciaire.* »[92].

120. -Ce contrôle peut s'exercer, de plusieurs façons.

---

[90] Article 39, loi n° 78-17.
[91] Article 5, projet de loi *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*, modifié et adopté par le Sénat le 1er avril 2003.
[92] Délibération de la CNIL n° 98-097.

D'une part, ce contrôle est assuré par le procureur de la République, tenu par le décret de 2001, et en particulier par la circulaire qui en découle, de transmettre aux gestionnaires de fichiers toutes les décisions d'acquittement, de relaxe ou de non-lieu.

D'autre part, la personne concernée peut désormais faire effectuer elle-même les modifications nécessaires, puisque les informations pourront lui être transmises dans les conditions décrites plus haut. Ainsi, les personnes concernées pourront exiger, auprès du procureur compétent ou de la CNIL, que la qualification des faits retenue par l'autorité judiciaire soit substituée à la qualification initialement enregistrée dans le fichier lors de la saisie effectuée par le policier.

121. -La CNIL s'est enfin opposée à ce que le STIC puisse être consulté à l'occasion d'enquêtes ordonnées par l'autorité administrative, sauf en cas de mise en danger de la sécurité des personnes. Elle a toutefois tenu à préciser qu'une telle utilisation ne devait se faire que dans des circonstances exceptionnelles, « *telles un événement attirant un public nombreux, un internement d'office, etc.* »[93]. De plus, afin d'assurer un contrôle adéquat de ce type d'utilisation, la CNIL a réussi à obtenir que les personnels habilités à consulter le fichier à de telles fins soient individuellement désignés, et que soit mis en place un système de journalisation permettant de conserver des traces de chacune des consultations, avec le numéro de l'agent effectuant la recherche.

122. -Ce corps de règles a constitué le principal apport de la CNIL dont on trouve des traces concrètes dans le processus d'apparition du STIC.

123. -La CNIL a également servi d'intermédiaire entre les associations de défense des droits de l'homme et de la vie privée et le ministère d'Intérieur, en se faisant le porte-parole de leurs revendications, certaines ne figurant pas dans le « corps de règles » édicté par la CNIL.

124. -Une de ces revendications concernait les multiples finalités du traitement. En effet, le fichier est présenté comme un outil statistique, ce qui justifie l'exhaustivité des données devant y apparaître, mais pas nécessairement une longue durée de conservation de celle-ci.

---

[93] CNIL, *Communiqué de presse relatif au STIC.*

D'autre part, le fichier est un outil de recherche criminelle, permettant de recouper les caractéristiques d'une infraction avec les précédents, ce qui justifie alors la conservation des informations pendant de longues durées, mais pas nécessairement concernant l'ensemble des infractions concernées par le traitement.

Ces finalités multiples et contradictoire combinées constitueraient, selon les associations auditionnées par la CNIL pendant l'instruction du dossier, une dérogation au principe de « spécialité » des fichiers de police, selon lequel un fichier général ne devrait être que de portée locale, et les fichiers nationaux devraient être limités à un domaine en particulier, comme le terrorisme, les empreintes digitales ou autres secteurs bien délimités[94].

125. -La deuxième revendication évoquée par la CNIL concernait d'une façon assez large les critères d'inscription au fichier et à l'absence de contrôle judiciaire sur la réalité des faits. Celle-ci a toutefois été dégagée par la CNIL dans la formulation du corps de règles cité plus haut.

126. -Le troisième point sur lequel les associations ont attiré l'attention de la CNIL était les risques d'utilisation du STIC comme un « casier judiciaire bis », mais nous évoquerons également ce problème davantage plus loin.

127. -La plupart de ces revendications se sont retrouvées dans la délibération de 2000, à côté de l'exigence que le STIC soit strictement encadré par la loi. Ainsi, la CNIL a pu se féliciter que la loi sur la sécurité intérieure vienne enfin consacrer l'existence de ce fichier qui n'avait jusqu'alors été reconnue que par le décret du 5 juillet 2001. Cela constitue une réelle victoire de la CNIL, puisque la loi de 1978 impose seulement que les fichiers de police judiciaire soient créés par la voie réglementaire.

128. -Ainsi a été consacré par la récente loi un certain nombre de garanties auxquelles tenait la CNIL, telles que le contrôle du traitement placé sous la responsabilité du procureur de la République territorialement compétent, la définition des personnes mises en cause, le principe de limitation de la durée des informations traitées et enregistrées, et le renforcement

[94] CNIL, 21ème Rapport d'activité 2000, p. 77.

de la mise à jour, voire de l'effacement, des données concernant les victimes comme les personnes mises en cause[95].

On voit donc que la CNIL a joué un rôle déterminant dans la mise en place du STIC comme dans tous les traitements de données personnelles un peu délicats, s'imposant comme la gardienne des libertés individuelles et de la vie privée face aux risques que présentent les traitements automatisés de données personnelles. Cela a même été reconnu par le Conseil Constitutionnel.

§2 La reconnaissance par le Conseil Constitutionnel

129. -Avant le vote de la loi sur la sécurité intérieure, le projet a été soumis au Conseil Constitutionnel. Dans la décision qu'il délivra, il émit une réserve qui était comme un clin d'œil à la CNIL. En effet, au lendemain de la présentation du projet de loi, en octobre 2002, la Commission regrettait d'une part de ne pas avoir été consultée, et d'autre part qu'aucune référence à la loi du 6 janvier 1978 ne soit faite dans cette loi comportant un chapitre entier de « *dispositions relatives aux traitements informatisés d'informations* »[96].

En effet, le Conseil constitutionnel rappela alors dans une réserve expresse (§ 26) de sa décision du 13 mars 2003 que les dispositions de la loi du 6 janvier 1978, qu'il considère comme « protectrices de la liberté individuelle » depuis sa décision no 97-389 du 22 avril 1997[97], s'appliqueront aux traitements dont la création est envisagée, même si aucune référence explicite à la loi n'était présente dans le texte.

130. -Malgré ce genre de soutien et de reconnaissance de l'importance qu'elle tient dans la protection des libertés individuelles et de la vie privée, nous avons vu que l'opinion de la CNIL a très souvent été négligée.

---

[95] CNIL, 23ème Rapport d'activité 2002, p. 21.
[96] Articles 21 et s., loi n° 2003-239.
[97] Conseil Constitutionnel, décision 97-389 du 22 avril 1997.

Section 2 – Une autorité administrative un peu trop indépendante

131. -La Commission Nationale Informatique et Libertés a été créée suite à un amendement du Sénat au projet de loi présenté par le gouvernement Chirac. C'est ainsi qu'elle est devenue la première autorité administrative indépendante, sur le modèle duquel ont par la suite été créés le Conseil Supérieur de l'Audiovisuel ou le médiateur de la République.

132. -Toutefois, nous avons vu dans la première partie comme dans le début de celle-ci, que la CNIL avait très souvent eu du mal à imposer ses recommandations, particulièrement depuis le début des années 1990. Ce manque d'efficacité s'explique par plusieurs facteurs.

133. -D'une part, la CNIL ne dispose pas réellement d'appuis politiques : étant une autorité indépendante, elle ne sera pas, par définition, systématiquement soutenue par le gouvernement au pouvoir, comme nous en atteste aujourd'hui le mépris avec lequel le ministre de l'Intérieur considère les prises de position de la CNIL concernant le STIC.

Pourtant, parmi ses membres, on trouve deux députés et deux sénateurs élus dans leurs assemblées respectives[98], mais cela ne suffit apparemment pas pour que la CNIL attire réellement l'intérêt des politiques, qui pourraient pourtant y trouver parfois des arguments allant dans leur sens. Par exemple, peu de politiciens ont évoqué l'inquiétude de la CNIL à propos du STIC au cours des discussions du projet de loi pour la sécurité intérieure.

134. -Un des handicaps de la CNIL est aussi le manque de publicité sur son activité. Cet argument était en réalité surtout valable les années précédentes. En effet, depuis trois ans, la CNIL enregistre des records de saisine de la part de personnes souhaitant exercer leur droit d'accès aux données les concernant dans les fichiers de sécurité publique.

Ainsi, en 2002, les demandes d'accès « *indirect* » aux fichiers de police et de sécurité publique ont augmenté de 51%, après avoir déjà connu une croissance de 67% en 1999 et de 21% en 2000[99].

[98] Article 8, loi n° 78-17.
[99] CNIL, 23ème Rapport d'activité 2002, p. 12.

Bien sûr, la CNIL se félicite de ces augmentations, mais il faut sans doute signaler ici le rôle qu'ont pu jouer les associations de protection des libertés individuelles et de la vie privée dans cette évolution, et plus précisément l'ouverture sur Internet en mars 2002 du site www.renseignementsgeneraux.net. Ce site est en fait une initiative du site Bug Brother, webzine spécialisé dans les informations sur la surveillance, soutenu par des nombreuses associations militant pour la liberté sous toutes ses formes. On y trouve des informations sur les formalités permettant d'exercer son droit d'accès aux informations conservées dans les fichiers de sécurité publique, en particulier celui des renseignements généraux et le STIC[100].

135. -La CNIL souffre également d'un problème de moyens. Elle dispose en effet d'un budget annuel de 40 millions de francs (un peu plus de 6 millions d'euro), pour soixante-douze salariés[101], les commissaires étant des volontaires non rémunérés.

Face à ces problèmes limitant considérablement son action, la loi transposant la directive de 1995 est venue donner de nouveaux pouvoirs à la CNIL, mais aussi en retirer certains.

Chapitre 2 – La place de la CNIL pour l'avenir

136. -Le projet de loi de transposition de la directive de 1995, de retour à l'Assemblée Nationale en deuxième lecture, n'est en réalité pas seulement destiné à permettre à l'ordre juridique national d'entrer en conformité avec le droit communautaire. Il comporte en plus d'importantes modifications touchant directement la CNIL, et sans rapport avec les recommandations de Bruxelles. Nous décrirons d'abord les apports du projet de loi augmentant les pouvoirs de la CNIL, avant de montrer qu'elle a en fait perdu d'importantes prérogatives.

Section 1 – Les nouveaux pouvoirs conférés par la future loi de transposition de la directive

137. -Si l'on met à part la création de la fonction de « *correspondant à la protection des données à caractère personnel* » qui n'est pas réellement un nouveau pouvoir de la CNIL, la

[100] *Sommes-nous tous fichés ?* , www.transfert.net, 14 mars 2002.
[101] C. Ducourtieux, *Des garde-fous contre la surveillance. La CNIL a réussi à s'imposer*, Le Monde, 3 octobre 2001.

plupart des nouveaux pouvoirs de la CNIL sont en réalité issus des débats qui eurent lieu au Sénat au cours de la première lecture du projet de loi.

138. -Les sénateurs ont en effet renforcé le rôle de la CNIL dans la coordinations avec d'autres autorités administratives indépendantes. Il lui sera également permis de participer aux négociations internationales à la demande du Premier ministre dans le domaine de la protection des données personnelles. Le Sénat lui a de plus confié la mission « *d'éclaire*[r] *le chemin* », de se tenir « *informée de l'évolution des technologies de l'information* [et de rendre] *public le cas échéant son appréciation des conséquences qui en résultent pour l'exercice des droits et libertés* » [102].

139. -Le Sénat a également conféré à la CNIL de nouvelles prérogatives permettant réellement une lutte plus efficace contre les violations des dispositions de la loi de 1978. Les pouvoirs de la CNIL concernant le contrôle de la mise en œuvre des traitements sont ainsi précisés et renforcés. Les membres de la Commission pouvaient déjà se rendre sur place pour contrôler la régularité des fichiers, mais désormais, si le responsable du traitement s'oppose à l'exercice de cette mission, non seulement il encourra des sanctions pénales, mais les commissaires pourront effectuer les vérifications malgré cette opposition avec l'autorisation du président du Tribunal de Grande Instance territorialement compétent[103].

La CNIL pourra également prononcer de réelles sanctions contre les contrevenants à la loi de 1978. Il peut s'agir de sanctions pécuniaires, d'une injonction de faire cesser le traitement, pouvant devenir un retrait de l'autorisation accordée en vertu de l'article 25 de la loi[104].

Il a toutefois été demandé à la CNIL de tenir compte de la situation économique des entreprises pour les sanctions financières, et on lui a retiré le pouvoir qu'elle avait jusqu'alors d'ordonner la destruction des fichiers tenus en violation de la loi.

---

[102] S.G., *Modernisation de la loi Informatique et Libertés : Le Sénat brouille les pistes*, www.legalbiznext.com , 4 avril 2003 ; E.C., *Le Sénat renforce la protection des données personnelles*, Le Monde Informatique, www.weblmi.com , 2 avril 2003 ; L. Nachury, *Le Parlement veut tempérer les pouvoirs de la CNIL*, www.01net.com , 2 avril 2003.

[103] Article 6, projet de loi *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*, modifié et adopté par le Sénat le 1er avril 2003.

[104] Article 7, projet de loi *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*, modifié et adopté par le Sénat le 1er avril 2003.

On le voit ici, bien qu'il mette en place de nouvelles prérogatives, le projet de loi de transposition en modère considérablement les effets. Cela n'est toutefois rien au regard de la compétence que ledit projet est venu retirer à la CNIL.

Section 2 – La contrepartie : un retrait de toutes les prérogatives de contrôle des fichiers de police

140. -Monsieur Michel Gentot, président de la CNIL, a souvent dit que le contrôle des fichiers de police était la « *pierre de touche* » de l'indépendance de la CNIL[105]. Il semblerait que pour l'avenir, la CNIL doive apprendre à se passer de cette pierre de touche, puisque le projet de loi vient lui retirer ce pouvoir, qui était en effet un des plus importants dont elle disposait.

141. -Comme l'annonçait déjà en juillet 2001 un article vu sur Internet, « *L'ombre du fichier STIC plane sur la réforme de la CNIL* »[106]. En effet, désormais, les fichiers « *intéressant la sûreté de l'Etat, la défense ou la sécurité publique* » pourront être créés après avis motivé et publié de la CNIL, alors que la loi exigeait avant un avis conforme qui ne pouvait être contourné que par un décret en Conseil d'Etat, ce qui ne fut jamais utilisé[107].

Ce nouveau régime a déjà été qualifié d'« *autorisation par soi-même* » [108], renvoyant la CNIL à un simple rôle consultatif, et limitant ses moyens d'action à l'appel au débat qui devrait suivre la publication d'un avis négatif de sa part.

142. -La loi n'a toutefois pas encore été définitivement été adoptée, à la différence de celle pour la sécurité intérieure. Nous pouvons donc encore espérer qu'à l'issue du débat

---

[105] CNIL, 23ème Rapport d'activité 2002, p. 21 ; M. Gentot, *La CNIL et les fichiers de sécurité publique*, discours prononcé au cours de la Conférence de Printemps des Commissaires à la protection des données, organisée à Séville les 3 et 4 avril 2003.
[106] Ph. Astor, J. Thorel, *L'ombre du fichier STIC plane sur la réforme de la CNIL*, www.zdnet.fr, 18 juillet 2001.
[107] Article 4, projet de loi *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*, modifié et adopté par le Sénat le 1er avril 2003.
[108] E. Drouard, Cabinet Gide Loyrette Nouel, *La refonte du régime de déclaration à la* CNIL, Séminaire *« Informatique et libertés demain : quelles protections face à quelles menaces ? »*, organisé par la Chambre de Commerce et d'Industrie de Paris, le 9 avril 2002. Compte rendu par J. Le Clainche, www.droit-ntic.com.

parlementaire, la CNIL conservera ses prérogatives de contrôle des fichiers de police. Autrement, nous devrons nous poser la question formulée par ce vers de Juvénal dans les Satires, reprise par de nombreuses associations veillant au respect des données personnelles, *Sed quis custodiet ipsos custodes ? (Qui surveillera les surveillants ?)*[109].

[109] Juvénal, *Satires*, VI, 347.

Titre 2 – Le fonctionnement du STIC : un traitement difficilement contrôlable

143. -Après avoir décrit la mise en place du STIC, et le rôle qu'a joué la CNIL dans la mise en place des limites qu'il fallait y apporter, nous allons maintenant en décrire le fonctionnement de façon plus précise.

Nous étudierons d'abord la nature des données qui y figurent, puis les catégories de personnes pouvant être concernées, avant de nous intéresser aux modalités de mise à jour et d'accès à celles-ci.

Chapitre 1 – La nature des données collectées

144. -Nous commencerons par évoquer l'origine des informations, puis leur nature précise.

Section 1 – L'origine des informations

145. -Le STIC a souvent été qualifié de « mégafichier ». En effet, depuis le début, l'objectif des services de police et des différents ministres de l'Intérieur ayant soutenu sa création était de créer un fichier informatique regroupant les informations de police judiciaire jusqu'alors dispersées dans des fichiers manuels ou dans des traitements automatisés déjà soumis au contrôle de la CNIL.

146. -Il existe actuellement de nombreux fichiers nationaux informatisés de police : le fichier central, le fichier des personnes recherchées, le fichier des recherches criminelles, le fichier des véhicules volés, la partie française du système d'information de Schengen, le fichier des chèques volés ou perdus, le fichier de contrôle pénal, le fichier des empreintes digitales, le fichier national transfrontière et le fichier des brigades spécialisées. A ces fichiers viennent s'ajouter des fichiers régionaux et le fichier mécanographique Canonge, comportant les photographies et le signalement des personnes mises en cause dans une procédure judiciaire[110].

[110] C. Richard, *Le STIC (Système de Traitement des Informations Constatées)*, extrait du colloque « *Que ne peut l'informatique ?* » organisé les 27, 28 et 29 octobre 1999 au Conservatoire National des Arts et Métiers de Paris.

147. -On voit donc que dès sa création, le STIC contenait de nombreuses informations. Toutefois, par la suite, le STIC est alimenté à l'issue de la phase policière de l'enquête à partir de comptes rendus d'enquêtes, se présentant sous la forme normalisée de procès-verbal de synthèse joint au dossier de la procédure.

148. -Selon les termes de la loi pour la sécurité intérieure, les informations nominatives destinées à alimenter le STIC sont « *recueillies au cours des enquêtes préliminaires ou de flagrance ou des investigations exécutées sur commission rogatoire* »[111].

Ainsi, grâce aux principes de décentralisation et d'unicité de la saisie mentionnés plus haut[112], le STIC a très rapidement contenu un volume gigantesque d'informations, puisque la moindre plainte ou infraction était rapportée dans sa mémoire.

Nous allons maintenant nous intéresser à la nature même des ces informations.

Section 2 – Le type d'informations

149. -Nous commencerons par décrire les deux catégories d'informations susceptibles d'être collectées, avant de montrer les risques liés à la saisie d'informations effectuée par des policiers.

§1 – Les informations ordinaires

150. -La CNIL a affirmé que les données collectées pour le STIC sont les « *catégories classiques d'informations qui figurent généralement dans les fichiers de police* »[113]. Selon le décret de 2001, les informations enregistrées ne sont pas les mêmes si la personne concernée est une victime ou une personne « mise en cause » dans l'infraction, comme nous le montrerons plus loin.

151. -Les informations enregistrées sur les personnes mises en cause sont donc les suivantes :

- identité (nom, nom marital, nom d'emprunt officiel, prénoms, sexe) ;

---

[111] Article 21, loi n° 2003-239.
[112] cf. supra n° 69.
[113] CNIL, 21ème Rapport d'activité 2000, p. 81

- surnom, alias ;
- date et lieu de naissance ;
- situation familiale ;
- filiation ;
- nationalité ;
- adresse(s) ;
- profession(s) ;
- état de la personne ;
- signalement ;
- photographie.

152. -Les informations collectées sur les victimes sont heureusement moins précises :

- identité (nom, nom marital, nom d'emprunt officiel, prénoms, sexe) ;
- date et lieu de naissance ;
- situation familiale ;
- nationalité ;
- adresse ;
- profession ;
- état de la personne ;
- signalement (personnes disparues et corps non identifiés) ;
- photographie (personnes disparues et corps non identifiés).

« *Sont également enregistrées les informations non nominatives qui concernent les faits objet de l'enquête, les lieux, dates de l'infraction et modes opératoires ainsi que les informations relatives aux objets, y compris celles qui sont indirectement nominatives*. »[114].

§2 – Les données dites « sensibles »

153. -Le décret de 2001 prévoyait que le STIC pouvait « *traiter des données nominatives de la nature de celles mentionnées à l'article 31 de la loi du 6 janvier 1978 susvisée, dans les seuls cas où ces informations résultent de la nature ou des circonstances de l'infraction ou se rapportent à des signes physiques particuliers, objectifs et permanents, en tant qu'éléments de*

[114] Décret n° 2001-583.

signalement des personnes, dès lors que ces éléments sont nécessaires à la recherche et à l'identification des auteurs d'infractions définies à l'article 2. »[115]

154. -En revanche, la loi pour la sécurité intérieure ne prévoit aucune disposition permettant de collecter des données relevant des catégories d'informations visées à l'article 31 de la loi de 1978, comme « *les origines raciales ou les opinions politiques* »[116].

155. -Toutefois, la CNIL avait déjà fait remarquer, dans son rapport d'activité pour l'année 2000, qu'il était possible de déduire ce genre d'informations « sensibles » des données « classiques » ne faisant pas l'objet de contrôle particulier. Par exemple, dans une affaire d'injures raciales ou d'agression sexuelle, il sera parfois aisé de déduire des informations sur l'origine, la vie sexuelle ou la religion d'une des personnes, mise en cause ou victime, qui représentent par ailleurs de précieuses aides si elles font partie du signalement d'une personne mise en cause[117], mais pourraient alors rappeler que pendant la dernière guerre, des fichiers publics utilisant le NIR avaient été utilisés pour localiser les Français de confession juive.

Il serait en effet des plus faciles d'effectuer une recherche sur l'ensemble des fiches du STIC pour en extraire tous les noms des personnes impliquées dans des affaires d'agressions racistes, antisémites ou homophobes. C'est précisément pour éviter ce genre de dérive, qui n'est pas inenvisageable si un jour un Président d'extrême droite était élu, que la CNIL a été constituée et a toujours tâché d'utiliser son influence toute relative pour faire encadrer le STIC.

Nous allons maintenant montrer qu'il existe, en plus de ce risque propre au traitement ordinaire de données personnelles, des possibilités importantes d'erreurs toutes aussi graves.

§3 – Les risques d'erreurs

156. -Les erreurs peuvent trouver leur origine aussi bien avant la création du STIC que dans la suite de son « alimentation ».

I/ Les risques de répétition des erreurs antérieures à la légalisation

[115] Article 1, décret n° 2001-583.
[116] Article 31, loi n° 78-17.
[117] CNIL, 21ème Rapport d'activité 2000, p. 81.

157. -Nous l'avons vu, le STIC est avant tout un fichier regroupant l'ensemble des fichiers de police utilisés depuis des années, et qui étaient déjà soumis au contrôle de la CNIL. Leur mise en commun au niveau national va sans doute amplifier l'effet des erreurs qu'ils pouvaient contenir, erreurs qui peuvent parfois être dues à de simples erreurs de saisie, ou à des manquements dans leur mise à jour.

158. -Afin de montrer les risques réels liés à ce type d'erreurs, la CNIL a présenté, lors de la conférence qui suivit la présentation du projet de loi pour la sécurité intérieure en octobre 2002, une liste d'exemples marquants relevés dans le STIC au cours d'enquêtes effectuées à la demande de personnes voulant exercer leur droit d'accès, souvent parce qu'elles ne comprenaient pas pourquoi elles se voyaient refuser des autorisations en théorie délivrées sans difficulté particulière par l'administration.

Ainsi en 2002, la CNIL a dû faire procéder dans 64 cas, parmi les 175 personnes fichées ayant fait la demande, à des « *mises à jour, voire à la suppression de signalements erronés ou manifestement injustifiés* »[118]. Cela représente tout de même 34% d'erreurs.

Parmi les exemples les plus significatifs, dont la liste a ici encore été rendue accessible grâce à une association, la Fédération Informatique et Libertés[119], au travers de son site Internet, on peut relever cette personne signalée comme auteur de viols alors qu'elle n'était que témoin, ou encore le cas d'une mineure qui avait été signalée à sept ans dans le fichier des personnes recherchées pour une fugue, et qui s'est retrouvée inscrite dans le STIC.

Un exemple particulièrement représentatif, parce qu'il rejoint en plus le problème des consultations effectuées à des fins strictement administratives, celui d'un gendarme qui s'était vu refuser un logement en caserne parce que quinze ans auparavant, sa concubine, qui ne vivait pas encore avec lui, s'était livrée à la prostitution pendant huit mois, alors qu'aucune procédure n'avait été relevée à son encontre.

Un autre exemple, touchant à la fois la problématique des consultations administratives et celle des communications d'informations à l'étranger, concerne une personne qui s'est vue

---

[118] M. Gentot, *La CNIL et les fichiers de sécurité publique*, op. cit.
[119] Fédération Informatique et libertés, *Liste des erreurs recensées par la CNIL dans le fichier STIC*, www.vie-privee.org , le 11 janvier 2003.

refuser une autorisation d'immigration au Canada parce qu'elle avait été signalée en qualité de mis en cause dans une affaire de fausse monnaie dans laquelle elle n'était que témoin.

159. -Les exemples de ce type sont nombreux, et sont la plupart du temps immédiatement rectifiés après l'intervention de la CNIL, mais si on imagine que parmi les personnes saisissant la CNIL, et étant réellement fichées, on peut trouver jusqu'à 34% d'erreurs, cela laisse imaginer les erreurs qui subsistent dans les milliers de fiches qui ne feront jamais l'objet d'un exercice du droit d'accès.

160. -On pourrait être tenté de se rassurer en espérant que ces erreurs font partie du passé de la CNIL, et que maintenant que le fichier est légalisé, il ne peut plus y avoir d'erreurs. Pourtant, l'alimentation même du fichier pose encore problème.

II/ Les qualifications inappropriées effectuées sans contrôle et avant toute procédure

161. -Nous avons vu que le STIC était alimenté par des documents synthétisant les informations recueillies « *au cours des enquêtes préliminaires ou de flagrance ou des investigations exécutées sur commission rogatoire* »[120].

Ces étapes constituent le début de l'enquête, avant toute poursuite. Il suffit de déposer une plainte pour une des infractions concernées pour apparaître dans le STIC en qualité de victime, en espérant que l'agent ne fera pas l'erreur de substituer à cette qualité celle de mis en cause. A ce stade de l'enquête, toutes les qualifications sont effectuées par l'agent, toujours sans contrôle du procureur de la République. Il peut ainsi inscrire un individu comme auteur de meurtre, alors que l'instruction retiendra par la suite la qualification de coups et blessures volontaires ayant causé la mort sans intention de la donner, ou révèlera que l'auteur des coups et blessures était une autre personne et que l'individu précité n'était que témoin.

Idéalement, la fiche concernant cette personne devrait être rectifiée dans le premier cas, détruite dans le second, l'interdiction du fichage des témoins étant une des victoires de la CNIL. Toutefois, même sur ce terrain, qui semble pourtant clairement réglé, on peut citer un des exemples retenus par la CNIL dans sa fameuse liste. Ainsi, une personne avait été

[120] Article 21, loi n° 2003-239.

signalée dans une affaire d'usage de stupéfiant, après avoir été entendue dans le cadre de la mise en examen de son colocataire pour usage et cession de produits stupéfiants. La personne n'était même pas nécessairement témoin de quoi que ce soit, et elle s'est retrouvée inscrite dans le STIC.

162. -Nous devons également aborder ici le problème que pose ce fichage sans contrôle face au principe général du droit qu'est la présomption d'innocence, dans le cadre du respect des droits de la défense. En effet, ce documents sont remplis sans aucun contrôle, ni aucun débat contradictoire, par des agents de police. La qualification qui y est portée mériterait, maintenant que l'on sait les conséquences que cela peut avoir, de pouvoir être discutée dès le début, mais la plupart du temps, la personne ne saura même pas sous quelle qualification elle a été inscrite au fichier tant qu'elle ne sera pas mise en examen. Selon Me Henri Leclerc, président de la Ligue des Droits de l'homme, le STIC est le symbole et l'outil de « *l'ère du soupçon* », puisque « *tout individu qui y a figuré, même peu, même par erreur, restera marqué de l'estampille : douteux* »[121].

163. -Nous devons souligner ici que lors des auditions organisées par la CNIL, des représentants de syndicats de police ont affirmé que les rubriques d'alimentation du STIC n'étaient pas toujours les même que celles du compte-rendu d'enquête joint au dossier de la procédure, et que le contrôle hiérarchique n'était pas systématique. Certaines associations et syndicats ont même admis que la qualification des faits devrait relever des magistrats.

164. -Ces problèmes étant largement liés à la question de la mise à jour des informations recueillies, nous y reviendrons dans la section consacrée à ce problème. On peut toutefois s'interroger sur l'efficacité de la mise à jour des renseignements concernant un témoin éventuel qui n'aura rien d'intéressant à apporter à l'instruction, et dont la seule trace sera l'ensemble des informations énumérées plus haut, avec la mention « mis en cause » dans une affaire dont la qualification ne sera pas nécessairement appropriée.

Nous allons maintenant aborder plus précisément la question des personnes concernées par la collecte.

---

[121] M. Linglet, *Le STIC toujours dans l'illégalité*, Expertises des Système d'Information, mai 1999, p.131.

Chapitre 2 – Les personnes concernées par la collecte

165. -Grâce à l'opposition ferme de la CNIL, seuls deux types de personnes peuvent apparaître dans le STIC : les personnes mises en cause, et les victimes.

Section 1 – Les personnes mises en cause

166. -Nous tenterons d'abord de décrire ce que recouvre cette formule, avant de montrer les difficultés liées à son ambiguïté et de décrire les conditions dans lesquelles ces informations sont conservées.

§1 – Le champ d'application

167. -La qualité de personne mise en cause dépend de deux facteurs : d'une part l'infraction commise, et d'autre part la personne elle-même.

I/ Les infractions

168. -Le décret de 2001, régularisant pour la première fois le STIC, énumérait précisément les infractions devant faire l'objet d'une inscription dans le fichier. Ces infractions étaient alors l'ensemble des crimes et des délits, et certaines contraventions de cinquième classe, prévues aux articles suivants du code pénal :

- R. 625-1 : violences volontaires avec incapacité totale de travail d'une durée inférieure ou égale à huit jours ;
- R. 625-7 : provocation non publique à la discrimination, à la haine ou à la violence raciale ;
- R. 625-8 : racolage ;
- R. 635-1 : destruction ou dégradation volontaire d'un bien appartenant à autrui avec dommage léger » ;
- R. 645-1 : port ou exhibition d'uniformes, d'insignes ou d'emblèmes rappelant ceux d'organisations ou de personnes responsables de crimes contre l'humanité ;
- R. 645-12 : intrusion dans les établissements scolaires[122].

[122] Article 2, décret n° 2001-583.

169. -Dans la loi pour la sécurité intérieure, les contraventions de cinquième classe devant faire l'objet d'une inscription au STIC ont seulement été décrites comme celles « *sanctionnant un trouble à la sécurité ou à la tranquillité publique ou une atteinte aux personnes, aux biens ou à l'autorité de l'Etat* »[123]. Ce changement n'est pas innocent. En effet, face à une description aussi vague, il est beaucoup plus facile d'interpréter de manière extensive le contenu de cette description. Ainsi, toutes les atteintes à la personne relevant de la cinquième catégorie sont désormais concernées, notamment les blessures par imprudence causant une ITT inférieure ou égale à trois mois qui étaient pourtant exclues du champ d'application défini par le décret[124].

170. -On peut donc noter ici encore que le gouvernement a voulu élargir, autant que possible, les hypothèses de fichage, grâce à une formule floue et facile à interpréter dans le sens voulu.

II/ Les personnes

171. -La définition de la qualité de personne mise en cause est également un problème d'interprétation, particulièrement important quand on sait que la loi pour la sécurité intérieure permet le fichage des personnes, « *sans limitation d'âge* »[125]

A/ Une définition large des personnes concernées

172. -La définition de la qualité de « personne mise en cause » a également évolué entre le décret de 2001 et la loi de mars 2003. En effet, le décret de 2001 permettait de recueillir des informations sur les personnes à l'encontre desquelles sont réunis « *des indices ou des éléments graves et concordants attestant leur participation à la commission* »[126] d'une des infractions citées plus haut.

173. -En revanche, la loi pour la sécurité intérieure adoptée en mars 2003 permet le traitement « *des informations sur les personnes, sans limitation d'âge, à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles aient pu participer, comme auteurs ou complices, à la commission des infractions mentionnées au premier alinéa du I* »[127].

[123] Article 21 I., loi n° 2003-239.
[124] Article R. 625-2, Code pénal.
[125] Article 21 II., loi n° 2003-239.
[126] Article 2, décret n° 2001-583.
[127] Article 21 II., loi n° 2003-239.

174. -Même si la différence entre les deux définitions est très légère, l'introduction dans le projet présenté en 2002 de la notion de « *vraisemblance* » de la participation de la personne permet d'étendre considérablement le champ d'application. La vraisemblance est définie par le « Petit Larousse » comme ce qui a « *l'aspect de la vérité, qu'on est en droit d'estimer vrai* »[128]. Cela est donc beaucoup plus vague que les éléments « *attestant la participation* » exigés par le décret. On peut donc penser qu'ici encore, le gouvernement a tenu à se préserver une certaine marge d'appréciation de la « vraisemblance » de l'implication d'une personne dans la commission d'une infraction.

B/ Le statut des mineurs

175. -Le décret de 2001 permettait déjà la collecte des informations concernant les mineurs mis en cause dans une des infractions concernées[129]. La loi pour la sécurité intérieure prévoit quant à elle que le STIC et les autres traitements utilisés par les services de police judiciaire « *peuvent contenir des informations sur les personnes, sans limitation d'âge* »[130].

176. -La loi n'apportant pas davantage de précision sur le statut des mineurs, on peut supposer qu'il reste le même que celui défini dans le décret. La particularité du régime applicable aux mineurs concernant essentiellement la durée de conservation des informations, nous l'étudierons dans les troisième paragraphe de cette section, qui y est consacré.

177. -Nous devons toutefois évoquer ici une remarque faite par le Conseil Constitutionnel : *« l'atténuation de la responsabilité pénale des mineurs en fonction de l'âge, comme la nécessité de rechercher leur relèvement éducatif et moral par des mesures adaptées à leur âge et à leur personnalité, prononcées par une juridiction spécialisée ou selon des procédures appropriées, ont été constamment reconnus par les lois de la République depuis le début du vingtième siècle ; que ces principes trouvent notamment leur expression dans la loi du 12 avril 1906 sur la majorité pénale des mineurs, la loi du 22 juillet 1921 sur les tribunaux pour enfants et l'ordonnance du 2 février 1945* [et que] *ce principe n'est pas méconnu du seul fait que les dispositions contestées ne comportent pas de limitation quant à l'âge des personnes*

[128] *Petit Larousse illustré 1990*, Larousse, Paris, 1989
[129] Article 7, décret n° 2001-583.
[130] Article 21 II., loi n° 2003-239.

sur lesquelles sont recueillies des informations dans les conditions prévues à l'article 21 de la loi déférée »[131].

Cette précision empêchera donc des interprétations visant à traiter les mineurs de la même façon que les majeurs dans le traitement des informations les concernant, préservant le principe selon lequel la répression n'est pas la priorité en matière de responsabilité pénale des mineurs.

§2 – Le problème posé par cette notion

178. -La définition qui a été finalement été choisie dans la loi peut très facilement permettre de ficher des personnes qui auront été dénoncées, même sans raison.

179. -D'autre part, on peut noter qu'elle correspond à celle donnée dans le Code de procédure pénale[132] pour la qualité de témoin, seulement renforcée par la qualification des faits qui doivent être graves et concordants.

L'avantage de cette pratique est de donner un encadrement précis, la jurisprudence ayant déjà interprété la définition du Code de procédure pénale. Toutefois, si la définition reste la même, les deux contextes dans lesquels elle est utilisée présentent d'importantes différences dans leurs finalités[133].

En effet, l'article 105 du Code de procédure pénale vise à donner à la personne concernée une plus grande protection, le statut de témoin lui interdisant de bénéficier d'un certain nombre de droits de la défense, comme en a attesté par la suite la création de la qualité de témoin assisté par la loi du 15 juin 2000[134].

En revanche, dans le cadre de la loi pour la sécurité intérieure, il est dans l'intérêt de l'individu de ne pas correspondre à la définition, afin de ne pas être fiché. Les deux définitions ne correspondent donc pas exactement, et l'argument selon lequel il est plus pratique de faire référence à une définition déjà interprétée par la jurisprudence doit donc être

---

[131] Conseil Constitutionnel, décision du 13 mars 2003.
[132] Article 105, Code de procédure pénale, Dalloz, Paris, 2003.
[133] C. Charbonneau, F. Pansier, op. cit., p. 4.
[134] Article 131-II de la loi n° 2000-516 du 15 juin 2000, *renforçant la protection de la présomption d'innocence et les droits des victimes*, Journal officiel du 15 juin 2000.

nuancé, l'interprétation dans le cadre de la procédure pénale se faisant généralement dans un sens favorable à la personne.

180. -La définition retenue dans la loi de mars 2003 présente toutefois l'avantage d'être proche de celle utilisée « *pour caractériser les personnes dont l'inscription des empreintes digitales dans le fichier automatisé autorisé par la CNIL est possible (décret n° 87-249 du 8 avril 1987). L'intérêt est que la police a déjà connaissance de cette définition et sera donc à même de l'appliquer avec plus de constance* »[135].

181. -Cette qualité de mis en cause rejoint également le problème de la présomption d'innocence évoqué pour les infractions.

Nous allons maintenant expliquer dans quelles conditions sont conservées les données recueillies dans le STIC.

§3 – Les modalités de conservation des données sur les personnes mises en cause

182. -Nous étudierons d'abord ce qui est prévu par la loi pour la sécurité intérieure, avant de comparer ces règles avec les principes formulés dans le Code de procédure pénale.

I/ Les dispositions de la loi

183. -La loi pour la sécurité intérieure ne dit pas pour combien de temps sont conservées les données recueillies dans le STIC. Ici encore, c'est un renvoi implicite aux dispositions du décret de 2001.

184. -Le décret prévoit différentes durées, d'après une double distinction : d'une part entre mineurs et majeurs, et d'autre part entre les infractions graves et moins graves. Ainsi le principe est de conserver les informations concernant les majeurs pendant vingt ans. Pour les infractions les plus graves, énumérées dans une annexe du décret, la durée de conservation est étendue à quarante ans.

Concernant les infractions contre les personnes, cette liste comprend l'empoisonnement, les crimes contre l'humanité, l'homicide volontaire, la torture, le viol et le proxénétisme. Les infractions contre les biens incluent le chantage, le vol à main armée ou en bande organisée, et

[135] C. Charbonneau, F. Pansier, *op. cit.*

les atteintes à la paix publique auxquelles est appliqué ce régime sont les actes de terrorisme et les infractions au régime des armes et munitions[136].

185. - La durée de conservation est réduite à cinq ans pour les mineurs et les personnes mises en cause pour un délit prévu par le code de la route, ou aux à un certain nombre d'articles du code pénal :

- Article 227-3 à 227-11 avec l'article L. 3421-1 du Code de la Santé publique : délits relatifs à l'abandon de famille, la non-présentation d'enfants ;
- Article 221-6 : homicide involontaire ;
- Article 222-19 : coups et blessures involontaires ayant provoqué une ITT supérieure à trois mois ;
- Article 311-3 : vol simple;
- Articles 314-5 et 314-6 : détournement de gage ou d'objet saisi ;
- Article 431-1 : entrave aux libertés constitutionnellement protégées ;
- Article 431-4 : participation sans arme à un attroupement interdit[137].

Cette liste des infractions pour lesquelles les informations ne sont conservées que cinq ans comprend également l'ensemble des contraventions concernées énumérées plus haut[138].

186. -Concernant les mineurs, la durée de conservation passe de cinq à dix ans pour les infractions visées à l'annexe II du décret et vingt ans pour les plus graves énumérées en annexe III. Les infractions de l'annexe III sont toutes celles de l'annexe I destinée aux majeurs qui n'apparaissent pas dans l'annexe II[139].

187. -En cas de commission de nouveaux faits susceptibles de faire l'objet d'un fichage au STIC, le délai applicable à l'ensemble des infractions à l'origine de la mise en cause est celui de la plus récente.

Ces durées semblent clairement établies et faciles à mettre en œuvre. Toutefois, nous devons maintenant les envisager sous l'angle des principes fondamentaux de la procédure pénale.

II/ Le cadre ordinaire du Code de procédure pénale

---

[136] Annexe I au décret n °2001-583.
[137] Code pénal.
[138] cf. supra n° 168.
[139] Annexes II et III au décret n° 2001-583.

188. -Le Code de procédure pénale regroupe l'ensemble des règles « définissant la manière de procéder pour la constatation des infractions, l'instruction préparatoire et le jugement »[140]. Le STIC contenant des informations utilisées au cours de l'instruction, il est légitime de comparer les règles générales de la procédure pénale à celles définies pour le STIC, tout en n'omettant pas que celui-ci a également une finalité statistique qui pourrait justifier des dispositions dérogatoires.

189. -En matière pénale, la durée de conservation des données dépendra de la prescription de l'action publique, dont l'existence est justifiée, selon certains auteurs, parce que « *comme la prescription de la peine, la prescription de l'action publique repose sur l'idée qu'au bout d'un certain temps, dans un intérêt de paix et de tranquillité sociale, mieux vaut oublier l'infraction qu'en raviver le souvenir* »[141]. Ainsi, en ce qui nous concerne, « *prévoir une disparition des informations au bout d'un certain temps rejoint cette idée d'amnésie définitive par effet du temps, sauf qu'en matière de fichier informatique, une procédure de destruction est obligatoire pour que l'oubli puisse avoir lieu* »[142].Messieurs les professeurs G. Stefani, G. Montagnier et B. Bouloc justifient d'autre part l'idée de l'oubli par le risque de « *dépérissement des preuves* », « *une action exercée trop longtemps après la commission de l'infraction risquerait de provoquer une erreur judiciaire. Pour l'éviter, dans l'intérêt même de la justice répressive et par suite de la société, le mieux est de renoncer à exercer l'action publique* »[143].

190. -Le Code de procédure pénale prévoit des délais beaucoup plus courts pour toutes les infractions concernées. En effet, la prescription de l'action publique est de un an pour les contraventions, trois ans pour les délits et dix ans pour les crimes[144] (à l'exception des crimes contre l'humanité qui sont imprescriptibles). Cela signifie qu'une personne mise en examen dans un affaire criminelle sera certaine, en l'absence de poursuite, qu'après dix ans, il ne restera aucune trace de son fichage et qu'elle ne sera plus jamais inquiétée à propos de cette affaire. Or nous avons vu qu'avec le STIC, une personne mise en cause ne pourra pratiquement jamais être certaine de ne pas voir resurgir une de ces affaires.

---

[140] S. Guinchard, G. Montagnier (sous la direction de), *Lexique – Termes juridiques*, Dalloz, Paris, 1995.
[141] G. Stefani, G. Levasseur, B. Bouloc, *Précis de procédure pénale*, Dalloz, Paris, 2000, n° 141.
[142] C. Charbonneau, F. Pansier, op. cit.
[143] G. Stefani, G. Levasseur, B. Bouloc, op. cit., n° 142.
[144] Articles 7 à 9, Code de procédure pénale.

191. -Les principaux arguments invoqués par les différents ministres de l'Intérieur s'étant occupés du dossier (Monsieur Daniel Vaillant à l'époque du décret) sont d'une part, la nécessité de disposer d'un outil statistique fiable, et d'autre part la possibilité d'effectuer des recoupements. Or ces finalités sont difficilement conciliables, comme nous l'avons déjà expliqué au cours de la description des revendications associatives au STIC reçues par la CNIL[145]. Face à ce problème, il a en effet été plus simple pour le ministère de choisir la solution la plus pratique pour lui : l'adoption de durées de conservation très longues.

192. -Il n'y a pourtant pas de raison particulière à ce que les principes appliqués au STIC diffèrent considérablement de ceux définis pour la procédure pénale en général, les finalités étant au fond les mêmes : la connaissance des circonstances de l'infraction, la détermination de l'auteur et son jugement.

Nous allons maintenant voir si les règles concernant les victimes sont aussi généreuses que celles sur les personnes mises en cause.

Section 2 – Les victimes

193. -A défaut de pouvoir recueillir des informations sur les témoins, le STIC en collecte sur les victimes. Nous expliquerons d'abord la raison de cette collecte, avant d'en décrire les modalités.

§1 – Les raisons de la collecte de données sur les victimes

194. -Le ministère de l'Intérieur a évoqué deux raisons principales à la collecte d'informations sur les victimes. Nous les étudierons donc successivement.

I/ La confrontation avec les auteurs

195. -Une des raisons pour lesquelles les victimes font également l'objet d'un fichage est la possibilité d'entrer en contact avec elles une fois l'auteur de l'infraction arrêté. Cela peut notamment être utile si une reconnaissance de l'auteur est requise, ou pour la restitution d'objets volés, ou pour informer les compagnies d'assurance, par exemple[146].

II/ Le rapprochement entre affaires, par le profil des victimes

---

[145] cf. supra n° 124.
[146] CNIL, 21ème rapport d'activité 2000, p. 80.

196. -La seconde raison est plus liée aux recherches de l'auteur de l'infraction. En effet, dans certains cas, et plus particulièrement les cas d'infractions sexuelles ou de crimes en série, le « profil » de la victime (âge, catégorie socioprofessionnelle, lieu de résidence, caractéristiques physiques) peut permettre aux agents d'identifier de manière inverse le profil criminel de l'auteur de l'infraction[147].

§2 – Les modalités de conservation des données sur les victimes

I/ Les dispositions de la loi

197. -Ici encore, la loi mentionne la possibilité de recueillir des informations sur les victimes sans plus de détail, ce qui renvoie aux dispositions du décret. Il prévoit dans le même article dans quelles conditions seront recueillies les informations relatives aux personnes mises en cause et les victimes[148]. Ainsi, toutes les infractions citées plus haut feront l'objet d'une collecte d'informations sur les victimes.

198. -Les seules dispositions que l'on trouve sur la durée de la conservation de ces informations, aussi bien dans le décret que dans la circulaire, est la durée maximale de conservation de celles-ci : quinze ans[149]. Ce délai ne courra qu'à partir de la découverte des objets pour les infractions portant sur des œuvres d'art, des bijoux ou des armes[150].

199. -Il existe toutefois un droit reconnu à la victime, celui de s'opposer à la conservation des données la conservant une fois l'auteur définitivement condamné.

200. -Certains craignent que cette collecte d'informations sur les victimes créent des risques de suspicion lors des enquêtes, notamment en considération des classements de fait des affaires par les policiers en dehors de toute saisine des autorités judiciaires.

II/ Le cadre ordinaire du Code de procédure pénale

201. -Les règles consacrées aux victimes dans le Code de procédure pénale ne concernent que la réparation du dommage ou l'action civile, mais jamais l'instruction du dossier. Les données recueillies sur les victimes dans le cadre de la procédure pénale sont donc

---

[147] CNIL, 21ème rapport d'activité 2000, p. 80.
[148] Article 2, décret n° 2001-583.
[149] Article 7 IV, décret n° 2001-583, et Circulaire présentant le décret n° 2001-583.
[150] Circulaire présentant le décret n° 2001-583 et Délibération de la CNIL n° 00-064.

vraisemblablement limitées à de simples renseignements administratifs qui ne seront jamais utilisés pour les mêmes finalités que celles du STIC.

Nous allons maintenant aborder un autre problème central du dossier STIC : la délicate question de la mise à jour des données.

Chapitre 3 – La mise à jour des données

202. -Nous avons vu qu'un des principaux problèmes que présentait le STIC était le risque d'erreurs dans les données conservées. Ces erreurs peuvent avoir plusieurs causes, une des plus importantes étant une mauvais gestion de leur mise à jour.

Nous expliquerons donc d'abord comment cette mise à jour est censée fonctionner, avant de montrer comment des erreurs peuvent facilement intervenir dans ce suivi de l'alimentation du STIC.

Section 1 – Les dispositions de la loi : la responsabilité du procureur de la République

203. -Le suivi du STIC relève de la responsabilité de son gestionnaire. Toutefois, la loi pour la sécurité intérieure prévoit que le traitement des informations contenues dans le STIC est placé sous le contrôle du procureur de la République compétent. C'est donc à celui-ci d'ordonner aux services de police judiciaire de le mettre à jour.

Il peut ainsi demander que les données soient « *effacées, complétées ou rectifiées, notamment en cas de requalification judiciaire* ». De plus, « *en cas de décision de relaxe ou d'acquittement devenue définitive, les données personnelles concernant les personnes mises en cause sont effacées sauf si le procureur de la République en prescrit le maintien pour des raisons liées à la finalité du fichier, auquel cas elle fait l'objet d'une mention. Les décisions de non-lieu et, lorsqu'elles sont motivées par une insuffisance de charges, de classement sans suite font l'objet d'une mention sauf si le procureur de la République ordonne l'effacement des données personnelles.* » [151].

[151] Article 21, loi n° 2003-239.

204. -Dans le projet initial de décret du gouvernement, aucune mise à jour n'était envisagée. Le garde des Sceaux s'était seulement engagé à diffuser une circulaire demandant aux procureurs de transmettre systématiquement aux gestionnaires de STIC, c'est à dire les services de police judiciaire, les décisions de relaxe ou d'acquittement.

C'est seulement suite à la délibération de la CNIL du 24 novembre 1998[152] et à l'avis défavorable du Conseil d'Etat de janvier 1999 que le gouvernement a mentionné l'obligation faite au procureur de transmettre les décisions de relaxe ou d'acquittement devenues définitives ainsi que celles de non-lieu et de classement sans suite pour insuffisance de charges[153].

205. -C'est ainsi qu'après la délibération de la CNIL de décembre 2000[154], le texte finalement publié est devenu plus complexe, distinguant mise à jour et effacement.

La suppression définitive des informations est prévue dans cinq hypothèses :

- pour les faits qui ont fait l'objet d'une décision de relaxe ou d'acquittement ;
- lorsque le procureur décide de prescrire l'effacement d'informations concernant une décision de relaxe ;
- pour tous les faits tombant dans le champ d'une amnistie ;
- lorsque les personnes mises en cause atteignent l'âge de 75 ans ;
- si la victime le demande, après la condamnation définitive de l'auteur.[155]

Une simple mise à jour est prévue dans les cas suivants :

- pour les décisions de non-lieu (sauf si le procureur en ordonne la suppression) ;
- pour les décisions de classement sans suite pour insuffisance de charges ;
- si la personne concernée demande une correction des mentions initiales, notamment en cas de requalification des faits.

Le régime a donc assez peu changé entre le décret de 2001 et la loi de 2003.

---

[152] Délibération de la CNIL n° 98-097.
[153] C. Charbonneau, F. Pansier, op. cit..
[154] Délibération de la CNIL n° 00-064.
[155] Articles 3, 7 et 9, décret n° 2001-583.

206. -Afin de permettre au procureur de vérifier toutes les informations enregistrées par les agents de police judiciaire, le décret prévoyait « *que les informations nominatives relatives aux personnes mises en cause et aux victimes ainsi que la qualification des faits, telles qu'elles sont enregistrées dans le STIC, sont transmises au procureur de la République territorialement compétent en même temps que la procédure*. »[156]

Pour cela, la circulaire prévoyait un système complexe de comptes rendus d'enquête ou d'infraction (si l'auteur présumé était identifié ou non) contenant les informations recueillies, accompagnées de fiches navettes intitulées « suites judiciaires », concernant chacune des personnes mises en cause[157].

Nous allons maintenant nous intéresser aux problèmes que peut connaître la mise en œuvre de cette lourde procédure.

Section 2 – Les difficultés probables de mise en œuvre

207. -Nous devons tout d'abord souligner la constitutionnalité discutable des mesures proposées pour la mise à jour du STIC. En effet, depuis l'entrée en vigueur de la loi du 6 janvier 1978, on considère parfois qu'il existe un « principe républicain » selon lequel le contrôle d'un fichier ne peut être abandonné à son utilisateur (qui serait alors juge et partie), mais est confié à une autorité administrative indépendante, la CNIL[158]. Or, le texte confie le contrôle des fichiers du STIC au procureur de la République, son principal utilisateur avec les agents de police. « *C'est comme si l'on confiait le contrôle des fichiers des renseignements généraux au ministère de l'Intérieur* »[159]. Ce recul dans la protection des données à caractère personnel est par conséquent inconstitutionnel en vertu du principe de l'effet « cliquet » de la loi de 1978.

208. -Concernant la mise en pratique, et sans rentrer trop profondément dans les détails techniques de ce système de « fiches navettes » censées circuler entre le parquet et les services de police au cours de la procédure, l'efficacité de la mise à jour du STIC semble des

---

[156] Article 2, décret n° 2001-583.
[157] Circulaire présentant le décret n° 2001-583.
[158] *Extension des fichiers de police : l'article 9 du projet de loi « sécurité intérieure »*, www.temps-reels.net , 20 décembre 2002.
[159] *Extension des fichiers de police : l'article 9 du projet de loi « sécurité intérieure »*, op. cit.

plus fragiles. En effet, il faut prendre en considération le fait que des millions de personnes sont fichées, et que la mise à jour des informations les concernant devra être effectuée à l'initiative des cent-quatre-vingt procureurs de la République, qui sont par ailleurs surchargés. Cela semble irréalisable de façon fiable, d'autant plus que les procureurs n'auront jamais de temps à consacrer à l'effacement de données dont l'inscription ne leur a été d'aucune utilité pour l'action publique.

209. - Nous devons à ce propos mentionner un exemple jurisprudentiel dans lequel c'est la CNIL qui a manqué à ses obligations en matière de mise à jour et d'exercice du droit d'accès. En effet, dans l'affaire « Ferrari », qui a fait l'objet d'une décision du Conseil d'Etat[160], le requérant s'est vu refuser par la CNIL le droit de mettre à jour les données le concernant dans un fichier de police.

Il avait appris que des données datant de 1963 le concernant apparaissaient dans un procès verbal établi en 1992. La CNIL avait alors refusé de prendre en considération sa demande de dénonciation au parquet de cette irrégularité, alors qu'elle y était tenue en vertu de la loi de 1978[161] et du code de procédure pénale[162]. Le Conseil d'Etat reprocha alors à la CNIL de ne pas avoir mené les recherches nécessaires pour vérifier si elle devait, en l'espèce, saisir le parquet pour cette irrégularité, pourtant flagrante.

Un tel exemple de faute de la CNIL est heureusement assez rare, mais il ne peut empêcher de nous faire douter de l'efficacité des moyens dont disposent les individus fichés pour faire rectifier ou mettre à jour les informations les concernant.

210. -Selon une déclaration faite par Raymond Forni, alors vice-président de la CNIL et un des « pères spirituels » de la loi du 6 janvier 1978, « *Le STIC, c'est la rumeur et le soupçon généralisés. Les défenseurs du projet objecteront que les parquets surveilleront les fichiers, leur contenu et leur mise à jour. Pas plus qu'aujourd'hui, la justice ne mettra les pieds demain dans un commissariat* »[163]. Ces réflexions ont été recueillies en 1999, avant même

---

[160] Conseil d'Etat, section du contentieux, *Jean Ferrari/CNIL*, 28 juillet 2000.
[161] Article 21, loi n° 78-17.
[162] Article 40, Code de procédure pénale.
[163] R. Forni, dans un entretien accordé à M. Linglet, *La CNIL légalise le mégafichier STIC. Information criminelle ou infractions constatées ?*, op. cit.

l'adoption du décret qui a servi de base à la loi pour la sécurité intérieure. Aujourd'hui, la CNIL se félicite d'avoir pu renforcer les modalités de mise à jour.

211. -Nous restons donc sceptique et pessimiste sur ce point, et même dans le cas où le STIC serait parfaitement tenu depuis mars 2003, il est certain que pendant des années encore, des personnes découvriront qu'elles étaient fichées sans raison depuis des années, et beaucoup ne le sauront jamais, puisque la mise à jour des informations liées aux affaires résolues n'est pas encore prévue, et quand on sait qu'elles peuvent être conservées jusqu'à quarante ans, cela a de quoi laisser perplexe.

D'autre part, il n'y aura aucun contrôle effectué sur les informations recueillies par les policiers pour des affaires qu'ils classeront eux-mêmes, sans qu'aucune communication au procureur n'ait lieu d'être.

Nous allons maintenant nous intéresser à un autre aspect du STIC suscitant d'importantes controverses, les modalités d'accès à son contenu.

Chapitre 4 – L'accès aux données

212. -Concernant un fichier aussi sensible que le STIC, la question de l'accès aux données doit être envisagée sous deux angles : d'une part celui des agents habilités à la consulter, et d'autre part celui des personnes concernées.

Section 1 – Les personnes habilitées à consulter le fichier

213. -Nous décrirons d'abord le nouveau régime prévu par la loi, avant de présenter les dérives possibles qu'il peut entraîner.

§1 – Les précisions apportées par la loi

214. -La loi pour la sécurité intérieure prévoit les modalités d'accès au STIC. Ainsi, seuls « *les personnels spécialement habilités des services de la police et de la gendarmerie nationale désignés à cet effet ainsi que les personnes, spécialement habilités, de l'Etat investis par la loi d'attribution de police judiciaire, notamment les agents de douanes, peuvent accéder aux informations* [contenues dans le STIC] ». De plus, « *l'habilitation précise la nature des données auxquelles elle autorise l'accès* ». Toutefois, « *l'accès aux*

informations […] *est également ouvert : 1° aux magistrats du parquet ; 2° aux magistrats instructeurs, pour les recherches relatives aux infractions dont ils sont saisis* »[164].

215. -Même si ces catégories de destinataires des informations semblent précisément encadrées, nous nous trouvons une fois de plus face à un élargissement des cas de recours au STIC. En effet, le décret de 2001, bien que plus laconique, ne permettait l'accès au STIC qu'aux « *personnels des services de la police nationale et de la gendarmerie nationale qui exercent des missions de police judiciaire et ont fait l'objet d'une désignation par l'autorité hiérarchique ;* [et aux] *magistrats du parquet.* »[165].
Le décret permettait en outre une hypothèse de consultation administrative. Cette dérogation est permise en cas de risque d'atteinte à l'ordre public ou à la sécurité des personnes. La police nationale peut alors consulter, sans autorisation du procureur, les informations concernant « *des procédures judiciairement closes, à l'exception des données complétées par les informations transmises par le procureur de la République en application de l'article 3 et des données relatives aux victimes* »[166].

216. -Ainsi, on estime que de quarante mille officiers de police judiciaire habilités à accéder au STIC, ce seront désormais près de quatre-cent mille personnes qui pourront le consulter dans le cadre de tâches administratives[167].

217. -Heureusement, la CNIL a réussi à imposer un système de journalisation, visant à conserver des traces de chaque consultation, en conservant le matricule de l'agent interrogeant le fichier et les informations consultées.

Nous allons maintenant évoquer les problèmes que cet accès élargi peut causer.

§2 – Les risques d'utilisation hors des finalités

218. -Nous avons vu qu'une des principales infractions pouvant être commises en rapport avec un traitement de données à caractère personnel est le détournement de finalité. Concernant le STIC, les risques sont très importants.

---

[164] Article 21, loi n° 2003-239.
[165] Article 5, décret n° 2001-583.
[166] Article 6, décret n° 2001-583.
[167] S. Rozenfeld, *Fichiers de police, Nicolas Sarkozy néglige la CNIL, elle s'autosaisit*, Expertises des Système d'Information, décembre 2002, p.403

I/ Le premier problème : la déclaration de la finalité du STIC

219. -Nous avons déjà vu que la finalité du STIC est assez ambiguë. En effet, ce traitement a pour double objectif de faciliter la constatation des infractions à la loi pénale d'une part, et le rassemblement des preuves d'infractions et la recherche de leurs auteurs d'autre part.

Le ministère devait avoir conscience de ce problème, puisque dans son projet de loi, la finalité du traitement n'était même pas mentionnée, et ce sont les sénateurs qui ont dû l'exiger[168].
Un des avantages d'une définition à la fois large et vague des finalités du traitement est de permettre toutes sortes d'actions sans constituer de détournement de finalité. L'inconvénient est que cela ne sera jamais favorable aux personnes concernées.

II/ Les enquêtes administratives autres que celles prévues par la loi : la mise en place d'un casier judiciaire parallèle

220. -Avec l'extension du nombre de personnes ayant accès au fichier, les risques d'utilisation en dehors des cadres prévus par la loi augmentent. Heureusement, un système de journalisation des consultations a été mis en place, mais de là à ce qu'il soit utilisé très strictement, de nombreuses consultations constituant de réels détournements de finalité auront été effectuées.

221. -En effet, il existe un risque important que la STIC soit utilisé comme une sorte de casier judiciaire parallèle, dont le contenu serait beaucoup moins encadré. En effet, la loi pour la sécurité intérieure abroge une disposition de la loi pour la sécurité quotidienne (adoptée en 2001 sous le gouvernement Jospin) qui modifiait une article de la loi de programmation et d'orientation relative à la sécurité (adoptée en 1995 sous le gouvernement Balladur), article portant sur les cas de consultation des traitements automatisés de police judiciaire dans le cadre d'enquêtes administratives.

Désormais, la loi prévoit que « *les décisions administratives de recrutement, d'affectation, d'autorisation, d'agrément ou d'habilitation* […] *concernant soit les emplois publics participant à l'exercice des missions de souveraineté de l'Etat, soit les emplois publics ou privés relevant du domaine de la sécurité ou de la défense, soit les emplois privés ou activités privées réglementées relevant des domaines des jeux, paris et courses* […] *peuvent être*

[168] S. Rozenfeld, *Fichiers de police,* op. cit..

précédées d'enquêtes administratives destinées à vérifier que le comportement des personnes physiques ou morales intéressées n'est pas incompatible avec l'exercice des fonctions ou des missions envisagées. » et qu'un « *un décret en Conseil d'Etat fixe la liste des enquêtes administratives qui donnent lieu à la consultation des traitements automatisés de données personnelles mentionnés à l'article 21 de la loi* [pour la sécurité intérieure]*, y compris pour les données portant sur des procédures judiciaires en cours, dans la stricte mesure exigée par la protection de la sécurité des personnes et la défense des intérêts fondamentaux de la nation* »[169].

L'on voit ici que les enquêtes administratives effectuées à des fins de protection de la sûreté de l'Etat, de la défense et de la sécurité publique risquent d'être interprétées de manière assez extensive.

222. -La CNIL avait pourtant bien exigé que pour ce genre d'enquête, préalable à une embauche dans le secteur public, par exemple, la règle était de demander un extrait du casier judiciaire, le bulletin n°2 ou n°3, afin de disposer de renseignements précis et sûrs sur les condamnations éventuelles de la personne concernée. Le casier judiciaire fait l'objet d'un encadrement très strict dans le Code de procédure pénale, et sa consultation ne fait l'objet d'aucune contestation[170].

En revanche, avec l'accès au STIC, compilant comme nous l'avons vu toutes sortes d'informations, qualifiées par des policiers, et dont la mise à jour n'est pas des plus fiables, pour les enquêtes administratives de moralité, on risque de retrouver souvent l'exemple précité du gendarme qui se voyait refuser un logement en caserne parce que quinze ans auparavant, sa compagne avait été signalée, sans aucune poursuite, dans une affaire de prostitution[171].

III/ Les utilisations à des fins strictement privées

223. -Ce risque devrait disparaître grâce au système de journalisation des consultations. Nous devons rappeler ici que ce qui a vraiment attiré l'attention sur le STIC a précisément été une de ces utilisations à des fins strictement privées.

---

[169] Article 26, loi n° 2003-239.
[170] Délibération de la CNIL n° 00-064, et CNIL, 21ème rapport d'activité 2000.
[171] cf. supra n° 158.

En effet, le dossier a resurgi quand un officier de la Police aux Frontières avait été détecté grâce à ce système parce qu'il utilisait le STIC pour effectuer des enquêtes de moralité sur des membres ou futurs membres de sa loge maçonnique, hors de toute affaire sur laquelle il aurait été habilité, bien sûr. Il avait alors confié aux journalistes que « *aucune note de service ne limite l'accès au STIC... par curiosité malsaine, de nombreux policiers pianotent, passent des noms sans rapport avec les enquêtes* »[172].

224. -Heureusement, aujourd'hui, le gouvernement nous garantit que ce genre de dérive ne sera plus possible, que les habilitations seront très encadrées et limitées aux informations auxquelles l'agent a besoin d'avoir accès. Ce qui est moins rassurant, c'est que désormais, le STIC peut être utilisé de plein droit pour des enquêtes administratives qui doivent encore être déterminées par le décret d'application de la loi[173]. Nous pouvons déjà deviner que la liste devrait être assez large.

L'autre aspect de l'accès aux données concerne les personnes fichées.

Section 2 – L'exercice du droit d'accès des personnes concernées

225. -Nous avons déjà largement étudié les modalités du droit d'accès dans la partie consacrée aux apports de la CNIL dans la défense de ce droit[174].

§1 – L'exercice du droit d'accès « indirect »

226. -Comme nous l'avons vu, l'ancienne rédaction de l'article 39 de la loi ne permettait pas d'accès aux données, seulement une vérification et mise à jour effectuée par un membre de la CNIL.

§2 – L'apport de la loi pour la sécurité intérieure

227. -La loi pour la sécurité intérieure est venue étendre le système mis en place en 1991 pour les fichiers des renseignements généraux à tous les fichiers de police judiciaire. Ainsi, une personne voulant savoir si elle est fichée dans le STIC pourra désormais demander à la CNIL de faire cette demande, et si la communication des données ne met pas en cause ses

[172] Nice Matin, 11 novembre 2000.
[173] Article 25, loi n° 2003-239.
[174] cf. supra n° 117.

finalités, c’est à dire la sûreté de l’Etat, la défense ou la sécurité publique, alors les informations pourront être transmises à la personne concernée, avec l’accord du responsable du traitement.

228. -Espérons que les services de police judiciaire interprèteront de façon assez stricte la mise en cause des finalités du traitement.

Conclusion

229. -Dans ce mémoire, nous avons vu que le STIC avait eu une histoire tumultueuse, allant de son passé clandestin, justifié par des impératifs « expérimentaux », à sa reconnaissance difficile, faisant l'objet de débats entre ses partisans voulant toujours plus de répression et les défenseurs des libertés individuelles, ralliés derrière la CNIL.

230. -Malheureusement, avec le gouvernement désigné à l'issue des élections présidentielles de 2002, il semblerait que le camp de la répression ait gagné la bataille. En effet, les garanties concernant le contrôle du fonctionnement sont maigres, et la CNIL n'aurait désormais plus son mot à dire concernant les fichiers de police, elle ne pourra que servir d'intermédiaire entre les individus souhaitant exercer leur droit d'accès aux données les concernant et les services gestionnaires du traitement. Espérons au moins que l'appréciation du critère d'après lequel l'information peut être communiquée ne sera pas trop sévère, mais ici encore, le doute est permis.

Bibliographie

Ouvrages

- J. Frayssinet, *Informatique, fichiers et libertés*, Litec, Paris, 1992.
- A. Lucas, J. Devèze, J. Frayssinet, *Droit de l'informatique et de l'Internet*, PUF, Collection Thémis, Paris, 2001.
- D. Martin, *Les fichiers de police*, PUF, Collection Que sais-je ?, n° 3461, Paris, 1999.
- J. Pradel, *Procédure pénale*, Cujas, Paris, 2000.
- G. Stefani, G. Levasseur, B. Bouloc, *Précis de procédure pénale*, Dalloz, Paris, 2000.
- M. Vivant, Ch. Le Stanc (sous la direction de), *Lamy, Droit de l'informatique et des réseaux*, Lamy, Paris, 2002.

Monographies

- P. Breton, *Des herbiers aux fichiers informatiques, l'évolution du traitement de l'information dans la police*, thèse, Strasbourg II, 1991.
- M. Delmas-Marty, D. Martin, *Fichiers de police en France, dérive sécuritaire ou sécurité à la dérive ?*, thèse, Paris X, 1996.
- O. Menant, *La protection des données personnelles et les renseignements généraux*, mémoire de DEA, ERID, Montpellier, 1996.
- A.-E. Rousseau, *Informatique, police et liberté*, mémoire de DEA, ERID, Montpellier, 1990.

Articles extraits de revues juridiques

- C. Charbonneau, F. Pansier, *Le Système de Traitement des Infractions Constatées ou les faits infractionnels à l'épreuve de la « memory S.T.I.C. »*, Les Petites Affiches, 24 août 2001, n°169, p. 3.

- C. Charbonneau, F. Pansier, *Présentation de la loi du 18 mars 2003 pour la sécurité intérieure : de la LSQ à la LSI*, La Gazette du Palais, 26-27 mars 2003, p. 2.

- O. Dufour, E. Bonnet, *Une nouvelle inquiétude : les fichiers privés*, Les Petites Affiches, 2 août 1999, n° 152, p. 3.

- A. Lepage, note sur l'arrêt *Ferrari/CNIL*, Expertises des Système d'Information, janvier 2001, p. 33.

- M. Linglet, *La CNIL légalise le mégafichier policier STIC – Information criminelle ou infractions constatées ?*, Expertises des Système d'Information, janvier 1999, p.403.

- M. Linglet, *Le STIC toujours dans l'illégalité*, Expertises des Système d'Information, mai 1999, p.131.

- M. Linglet, *Le fichier informatisé STIC, Réflexions et témoignages. Un « pré-jugement » policier*, Expertises des Système d'Information, juin 2000, p.166.

- S. Portelli et M. Linglet, *Une place peu ordinaire dans la société*, Expertises des Système d'Information, décembre 2000, p.373.

- S. Rozenfeld, *Enquêtes judiciaires : les intentions informatiques de la LOPSI*, Expertises des Système d'Information, octobre 2002, p.325.

- S. Rozenfeld, *Fichiers de police, Nicolas Sarkozy néglige la CNIL, elle s'autosaisit*, Expertises des Système d'Information, décembre 2002, p.403.

- M. Vivant, N. Mallet-Poujol, Chronique : Informatique et libertés, La Semaine Juridique, Entreprise et affaires, 6 juin 2002, n° 23, p. 953.

Articles extraits de sites d'information juridique

- *Extension des fichiers de police : l'article 9 du projet de loi « sécurité intérieure »*, www.temps-reels.net, 20 décembre 2002.

- *Sommes-nous tous fichés ?*, www.transfert.net, 14 mars 2002.

- *Fichiers de sécurité publique : la Cnil règle ses comptes avec la police*, www.transfert.net, 24 avril 2003.

- *La CNIL confrontée à une « explosion » des plaintes*, www.transfert.net, 26 juin 2003.

- Fédération Informatique et libertés, *Liste des erreurs recensées par la CNIL dans le fichier STIC*, www.vie-privee.org, le 11 janvier 2003.

- Ph. Astor, J. Thorel, *L'ombre du fichier STIC plane sur la réforme de la CNIL*, www.zdnet.fr, 18 juillet 2001.

- E.C., *Le Sénat renforce la protection des données personnelles*, Le Monde Informatique, www.weblmi.com, 2 avril 2003.

- E. Dumont, *La loi sur la sécurité intérieure définitivement adoptée*, www.zdnet.fr, le 17 février 2003

- S.G., *Modernisation de la loi Informatique et Libertés : Le Sénat brouille les pistes*, www.legalbiznext.com, 4 avril 2003.

- J. Thorel, *Deux fichiers de police pas très nets risquent de retarder la loi Sarkozy*, www.zdnet.fr, 16 janvier 2003.

- L. Nachury, *Le Parlement veut tempérer les pouvoirs de la CNIL*, www.01net.com, 2 avril 2003.

Extraits de conférences

- E. Drouard, Cabinet Gide Loyrette Nouel, *La refonte du régime de déclaration à la CNIL*, Séminaire *« Informatique et libertés demain : quelles protections face à quelles menaces ?* », organisé par la Chambre de Commerce et d'Industrie de Paris, le 9 avril 2002. Compte rendu par J. Le Clainche, www.droit-ntic.com.

- R. Errera, *Le S.T.I.C. : Histoire et contenu d'une réglementation négociée*, XXIIIème Conférence internationale Commissaires à la protection des données, organisée à Paris les 24 et 26 septembre 2001.

- M. Gentot, *La CNIL et les fichiers de sécurité publique*, Conférence de Printemps des Commissaires à la protection des données, organisée à Séville les 3 et 4 avril 2003.

- C. Richard, *Le STIC (Système de Traitement des Informations Constatées)*, extrait du colloque « *Que ne peut l'informatique ?* » organisé les 27, 28 et 29 octobre 1999 au Conservatoire National des Arts et Métiers de Paris.

- F. Paoletti, *Informatique et libertés : principes et concepts*, extrait du colloque « *Que ne peut l'informatique ?* » organisé les 27, 28 et 29 octobre 1999 au Conservatoire National des Arts et Métiers de Paris.

Rapports et communiqués de la CNIL

Tous ces documents peuvent être téléchargés depuis le site de la CNIL : www.cnil.fr

- CNIL, 23ème rapport d'activité 2002, La Documentation française, 2003.
- *Position de la CNIL sur les dispositions du projet de loi pour la sécurité intérieure relatives aux fichiers de police judiciaire et au fichier national automatisé des empreintes génétiques* - Séance du 24 octobre 2002.
- CNIL, 22ème rapport d'activité 2001, La Documentation française, 2002.
- CNIL, 21ème rapport d'activité 2000, La Documentation française, 2001.
- Délibération de la CNIL n° 00-064 du 19 décembre 2000, *relative à un projet de décret en Conseil d'Etat portant création du « Système de Traitement des Infractions Constatées (STIC) » et application du troisième alinéa de l'article 31 de la loi du 6 janvier 1978.*
- *Communiqué de presse relatif au Système de Traitement des Infractions Constatées (STIC),* 3 décembre 1998.
- Délibération de la CNIL n° 98-097 du 24 novembre 1998, *portant avis sur le projet d'arrêté interministériel relatif à la création du système de traitement de l'information criminelle (STIC) et sur le projet de décret présenté par le Premier ministre en application de l'article 31 - alinéa 3 de la loi du 6 janvier 1978.*

Lois et règlements internes

Lois

- Projet de loi *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*, modifié et adopté par le Sénat le 1er avril 2003.

- Loi n° 2003-239 du 18 mars 2003, *pour la sécurité intérieure*, Journal officiel du 19 mars 2003.

- *La sécurité, première des libertés*, texte décrivant le projet de loi *pour la sécurité intérieure*, 23 octobre 2002.

- Projet de loi *pour la sécurité intérieure*, 23 octobre 2002.

- Loi n° 2001-1061 du 15 novembre 2001, *sur la sécurité quotidienne*, Journal officiel du 16 novembre 2001.

- Loi n° 2000-516 du 15 juin 2000, *renforçant la protection de la présomption d'innocence et les droits des victimes*, Journal officiel du 15 juin 2000.

- Loi n° 95-73 du 21 janvier 1995, *d'orientation et de programmation relative à la sécurité*, Journal officiel du 23 janvier 1995.

- Loi n° 85-835 du 7 août 1985, *relative à la modernisation de la police nationale*, Journal officiel du 8 août 1985.

- Loi n° 78-17 du 6 janvier 1978, *relative à l'informatique, aux fichiers et aux libertés*, Journal officiel du 7 janvier 1978.

Règlements

- Circulaire de la direction des affaires criminelles et des grâces, *présentation des dispositions du décret n° 2001-583 du 5 juillet 2001 pris pour l'application des dispositions du 3e alinéa de l'article 31 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et portant création du système de traitement des infractions constatées (STIC)*, Bulletin officiel du ministère de la Justice n°83, du 1er juillet au 30 septembre 2001.

- Décret n° 2001-583 du 5 juillet 2001 *pris pour l'application des dispositions du troisième alinéa de l'article 31 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et portant création du système de traitement des infractions constatées*, Journal officiel du 6 juillet 2001.

- Décret n° 86-326 du 7 mars 1986 *portant application à certains actes réglementaires relatifs à des traitements automatisés d'informations nominatives intéressant la sûreté de l'Etat, la défense et la sécurité publique des dispositions du deuxième alinéa de l'article 20 de la loi du 6 janvier 1978*, Journal officiel du 8 mars 1986.

- Décret n° 79-1160 du 28 décembre 1979, *fixant les conditions d'application aux traitements d'informations nominatives intéressant la sûreté de l'Etat, la défense et la sécurité publique de la loi n° 78-17 relative à l'informatique, aux fichiers et aux libertés*, Journal officiel du 31 décembre 1979.

Sources externes

- Charte des droits fondamentaux de l'Union européenne, adoptée à Nice le 7 décembre 2000.

- 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 des Communautés européennes n° L 281 du 23 novembre 1995, p. 0031 – 0050.

- Convention *pour la protection des personnes à l'égard du traitement des données à caractère personnel* du 28 janvier 1981 du Conseil de l'Europe (Convention 108).

Jurisprudence

- Conseil d'Etat, *Zanone*, 13 décembre 2002, note J. Moreau, La Semaine Juridique, Administrations et collectivités territoriales, 10 février 2002, p. 191.

- Conseil d'Etat, section du contentieux, *Jean Ferrari/CNIL*, 28 juillet 2000, note A. Lepage, Expertises des Systèmes d'Information, janvier 2001, p. 33.

- Cass. Crim., 3 février 1998, n° de pourvoi 96-82665.

- TGI Paris, 17ème ch., 5 décembre 1991, note J. Frayssinet, *Expertises*, n°148, mars 1992, p.107 ; CNIL, 12ème rapport d'activité 1991, La Documentation française, 1992, p.30.

Décisions du Conseil Constitutionnel

- Conseil Constitutionnel, décision du 13 mars 2003.

- Conseil Constitutionnel, décision n° 97-389 du 22 avril 1997.

Divers

Articles du Monde

- Auteur inconnu, *Un rassemblement de données éparses*, Le Monde, 5 décembre 1988.
- P. Boucher, *Safari ou la chasse aux Français*, Le Monde, 21 mars 1974.
- P. Ceaux, *Bien que non réglementaire, le STIC fonctionne déjà*, Le Monde, 16 février 1999.
- P. Ceaux, *Le gouvernement encadre le contenu et l'usage du fichier controversé de la police*, Le Monde, 8 juillet 2001.
- P. Ceaux et C. Prieur, *Le gouvernement élargit considérablement les pouvoirs de la police*, Le Monde 26 septembre 2002.
- C. Ducourtieux, *Des garde-fous contre la surveillance. La CNIL a réussi à s'imposer*, Le Monde, 3 octobre 2001.
- S. Foucart, *La CNIL tenue à l'écart du projet de loi pour la sécurité intérieure*, Le Monde, 4 octobre 2002.
- E. Inciyan, *Un gigantesque fichier rassemblera les données nominales des P.V. de police*, Le Monde, 5 décembre 1998.
- J.-Y. Nau, *L'informatisation des fichiers de la police criminelle. L'ordinateur mène l'enquête*. Le Monde, 9 décembre 1988.

Autres

- Nice Matin, 11 novembre 2000.
- G. Braibant, *Données personnelles et société de l'information, Rapport au Premier ministre sur la transposition en droit français de la directive n° 95/46*, 3 mars 1998, trouvé sur le site de la CNIL.
- Rapport de la Commission informatique et libertés, La Documentation française, 1975.
- S. Guinchard, G. Montagnier, *Lexique – Termes juridiques*, Dalloz, Paris, 1997.

- Juvénal, *Satires*, VI, 347.

- Ministère de l'Intérieur, *Note relative à la méthodologie des statistiques des crimes et délits constatés par la police et la gendarmerie*, 7 novembre 2002, trouvé sur le site du ministère de l'Intérieur.

- G. Orwell, *1984*, Gallimard, Paris, 1950 – Réédition Gallimard, collection Folio, Paris, 1976.

- Code pénal, Dalloz, Paris, 2003.

- Code de procédure pénale, Dalloz, Paris, 2003.

Table des matières

Résumé et abstract **3**

Plan général **4**

Introduction **5**

PARTIE 1 – LA MISE EN PLACE DU STIC **10**

Titre 1 – La déclaration des traitements automatisés d'informations nominatives *12*

Chapitre 1 – Définitions 12

Section 1 – Informations nominatives 12

§1 – La définition de la loi de 1978 : les informations nominatives 13

§2 – La définition de la directive de 1995 : les données à caractère personnel 14

Section 2 – Traitement automatisé 16

§1 – La définition de la loi de 1978 : le traitement automatisé d'informations nominatives 16

§2 – La définition de la directive 1995 : le traitement de données à caractère personnel 17

Chapitre 2 – L'exigence de déclaration de tous les traitements automatisés d'informations nominatives 19

Section 1 – Le principe 19

§1 – La demande d'avis ou la déclaration exigée par la loi de 1978 19

§2. La notification exigée par la directive de 1995 21

Section 2 – Les différents régimes applicables en fonction de la nature du traitement 22

§1 – La distinction entre fichiers privés et publics 22

I. La simple déclaration des fichiers du secteur privé 24

II – La demande d'avis pour les fichiers du secteur public 24

§2 – Les fichiers intéressant la sûreté de l'Etat, la défense et la sécurité publique 25

I – L'allègement de la demande d'avis 25

II – La dispense de publication de l'acte réglementaire portant création du fichier 26

Titre 2 – L'apparition et l'exploitation progressive du STIC *28*

Chapitre 1 – Les premières traces du projet STIC 28

Chapitre 2 – Premier dépôt du dossier à la CNIL, 1994 30

Chapitre 3 – Loi d'orientation et de programmation relative à la sécurité, 1995 31

Chapitre 4 – L' « incompréhensible » reconnaissance de l'existence du STIC par la CNIL, 1998 31

Chapitre 5 – Délibération de la CNIL "relative à un projet de décret en Conseil d'Etat portant création du STIC et application des dispositions du troisième alinéa de l'article 31 de la loi de 1978", 2000 33

Chapitre 6 – Décret portant légalisation du STIC, 2001 34

Chapitre 7 – Loi sur la sécurité quotidienne, 2001 35

Chapitre 8 – Projet de loi pour la sécurité intérieure, 2002 35

Chapitre 9 – Loi pour la sécurité intérieure, 2003 36

Section 1 – La décision du Conseil Constitutionnel 36

Section 2 – Le contenu de la loi pour la sécurité intérieure 37

Conclusion de la première partie 38

PARTIE 2 – LES ENJEUX DE LA RECONNAISSANCE LEGALE DE L'EXISTENCE DU STIC 39

Titre 1 – Une légalisation longtemps réclamée par la CNIL 41

Chapitre 1 – Le rôle de la CNIL dans cette évolution 41

Section 1 – Une protectrice de la première heure de la vie privée et des libertés individuelles 41

§1 – L'élaboration d'un « corps de règles » applicables aux fichiers de police 42

§2 La reconnaissance par le Conseil Constitutionnel 47

Section 2 – Une autorité administrative un peu trop indépendante 48

Chapitre 2 – La place de la CNIL pour l'avenir 49

Section 1 – Les nouveaux pouvoirs conférés par la future loi de transposition de la directive 49

Section 2 – La contrepartie : un retrait de toutes les prérogatives de contrôle des fichiers de police 51

Titre 2 – Le fonctionnement du STIC : un traitement difficilement contrôlable 53

Chapitre 1 – La nature des données collectées 53

Section 1 – L'origine des informations 53

Section 2 – Le type d'informations 54

§1 – Les informations ordinaires 54

§2 – Les données dites « sensibles » 55

§3 – Les risques d'erreurs 56

I/ Les risques de répétition des erreurs antérieures à la légalisation 56

II/ Les qualifications inappropriées effectuées sans contrôle et avant toute procédure 58

Chapitre 2 – Les personnes concernées par la collecte 60

Section 1 – Les personnes mises en cause 60

§1 – Le champ d'application 60

I/ Les infractions 60

II/ Les personnes 61

A/ Une définition large des personnes concernées 61

B/ Le statut des mineurs 62

§2 – Le problème posé par cette notion 63

§3 – Les modalités de conservation des données sur les personnes mises en cause 64

I/ Les dispositions de la loi 64

II/ Le cadre ordinaire du Code de procédure pénale 65

Section 2 – Les victimes 67

§1 – Les raisons de la collecte de données sur les victimes 67

I/ La confrontation avec les auteurs 67

II/ Le rapprochement entre affaires, par le profil des victimes 67

§2 – Les modalités de conservation des données sur les victimes 68

I/ Les dispositions de la loi 68

II/ Le cadre ordinaire du Code de procédure pénale 68
Chapitre 3 – La mise à jour des données 69
Section 1 – Les dispositions de la loi : la responsabilité du procureur de la République 69
Section 2 – Les difficultés probables de mise en œuvre 71
Chapitre 4 – L'accès aux données 73
Section 1 – Les personnes habilitées à consulter le fichier 73
§1 – Les précisions apportées par la loi 73
§2 – Les risques d'utilisation hors des finalités 74
I/ Le premier problème : la déclaration de la finalité du STIC 75
II/ Les enquêtes administratives autres que celles prévues par la loi : la mise en place d'un casier judiciaire parallèle 75
III/ Les utilisations à des fins strictement privées 76
Section 2 – L'exercice du droit d'accès des personnes concernées 77
§1 – L'exercice du droit d'accès « indirect » 77
§2 – L'apport de la loi pour la sécurité intérieure 77

Conclusion 79

Bibliographie 80

Ouvrages 80
Monographies 80
Articles extraits de revues juridiques 81
Articles extraits de sites d'information juridique 82
Extraits de conférences 83
Lois et règlements internes 84
Lois 85
Règlements 85
Sources externes 86
Rapports et communiqués de la CNIL 86
Jurisprudence 87
Décisions du Conseil Constitutionnel 87
Divers 88
Articles du Monde 88
Autres 88

Table des matières 90