

MINISTÈRE DE L'INTÉRIEUR  
ET DE L'AMÉNAGEMENT DU TERRITOIRE

**Circulaire du 9 mai 2007 relative aux modalités de mise en œuvre  
du système de traitement des infractions constatées (STIC)**

NOR : INTC0700059C

*Références :*

- Loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité modifiée, et notamment l'article 17-1 ;
- Loi n° 2002-1094 du 29 août 2002 d'orientation et de programmation pour la sécurité intérieure ;
- Loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure, et notamment son article 21 ;
- Décret n° 2006-1258 du 14 octobre 2006 modifiant le décret n° 2001-583 du 5 juillet 2001 portant création du système de traitement des infractions constatées « STIC » ;
- Décret n° 2005-1124 du 5 septembre 2005 fixant la liste des enquêtes administratives donnant lieu à la consultation des traitements automatisés de données personnelles ;
- Décret n° 2007-451 du 25 mars 2007 portant application de la loi « informatique et libertés » du 6 janvier 1978 ;
- Circulaire NOR/JUS/D/06/30134C du ministère de la justice du 26 décembre 2006.

*Résumé :*

- La modification du décret n° 2001-583 du 5 juillet 2001 portant création du système de traitement des infractions constatées (STIC), par le décret n° 2006-1258 du 14 octobre 2006, a tiré les conséquences des dispositions introduites par les articles 21, 22, 24 et 25 de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure.
- Les évolutions concernent la finalité du traitement, les catégories d'informations enregistrées, leurs modalités de mise à jour ainsi que les personnes qui en sont destinataires.
- Elles mettent aussi l'accent sur l'habilitation obligatoire des agents qui traitent les informations, la traçabilité de leur consultation, les sanctions encourues en cas d'utilisation illégale et les droits des personnes faisant l'objet d'un enregistrement.
- Enfin, le nouveau décret tient compte de la révision intervenue en 2004 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

*Le ministre de l'intérieur et de l'aménagement du territoire à Monsieur le préfet de police ; Mesdames et Messieurs les préfets de départements ; Madame et Messieurs les directeurs et chefs de service de la police nationale (pour attribution) ; Madame la préfète, secrétaire générale ; Monsieur le directeur général de la gendarmerie nationale ; Monsieur le directeur des libertés publiques et des affaires juridiques ; Monsieur le directeur des affaires criminelles et des grâces (pour information).*

**SOMMAIRE**

---

- 1. Les règles de fonctionnement du traitement
  - 1.1. L'alimentation du traitement
    - 1.1.1. Les catégories d'informations enregistrées
      - 1.1.1.1. Les données à caractère personnel
      - 1.1.1.2. Les données à caractère personnel dites « sensibles »
      - 1.1.1.3. La prise en compte des objets dans le traitement
    - 1.1.2. Les catégories de personnes enregistrées
      - 1.1.2.1. Les mis en cause
      - 1.1.2.2. Les victimes
  - 1.2. Les durées de conservation des informations
    - 1.2.1. Les durées de conservation des informations relatives au mis en cause

- 1.2.1.1. Le régime applicable aux majeurs
- 1.2.1.2. Le régime applicable aux mineurs
- 1.2.2. Les durées de conservation des informations relatives à la victime
- 2. Les règles d'utilisation du traitement
  - 2.1. L'habilitation des agents et leur contrôle
    - 2.1.1. Les deux types d'habilitations individuelles
      - 2.1.1.1. L'habilitation des agents des services de la police nationale
        - 2.1.1.1.1. L'attribution d'un profil d'utilisateur
        - 2.1.1.1.2. Le règlement de sécurité du système CHEOPS
      - 2.1.1.2. L'habilitation des agents des préfectures investis de missions de police administrative
        - 2.1.1.2.1. La procédure d'habilitation des agents
        - 2.1.1.2.2. Les modalités de consultation
    - 2.1.2. La traçabilité des consultations effectuées par les agents habilités
    - 2.1.3. Contrôle hiérarchique et sanctions disciplinaires et pénales
      - 2.1.3.1. La responsabilité hiérarchique
      - 2.1.3.2. Les sanctions disciplinaires
      - 2.1.3.3. Les sanctions pénales
  - 2.2. L'exploitation des données
    - 2.2.1. L'utilisation en matière de police judiciaire
      - 2.2.1.1. Les destinataires
      - 2.2.1.2. Les cadres juridiques de consultation
      - 2.2.1.3. les conditions d'utilisation des informations dans le cadre des procédures judiciaires
    - 2.2.2. L'utilisation en matière de police administrative
      - 2.2.2.1. Les enquêtes administratives donnant lieu à une consultation
        - 2.2.2.1.1. Les décisions administratives de recrutement, d'affectation, d'autorisation, d'agrément ou d'habilitation.
        - 2.2.2.1.2. Les demandes relatives au droit des étrangers et aux ordres nationaux
        - 2.2.2.1.3. Les risques d'atteinte à l'ordre public et à la sécurité des installations privées
      - 2.2.2.2. L'encadrement de la consultation à des fins de police administrative
        - 2.2.2.2.1. Les caractéristiques du module de police administrative
        - 2.2.2.2.2. La compétence non liée de l'autorité administrative pour la prise de décision
- 3. Les droits des personnes enregistrées dans le STIC
  - 3.1. Le nouveau droit d'information des victimes
  - 3.2. Le droit d'accès aux données et de rectification
    - 3.2.1. L'exercice du droit d'accès devant la CNIL
      - 3.2.1.1. Un droit d'accès ouvert à toute personne physique
      - 3.2.1.2. Les modalités d'accès aux données enregistrées dans le traitement
    - 3.2.2. Les demandes de rectification des données
      - 3.2.2.1. Demandes émanant des victimes
      - 3.2.2.2. Demandes émanant des mis en cause
        - 3.2.2.2.1. Demande de requalification des faits
        - 3.2.2.2.2. Demande de mise à jour suite à une décision de non-lieu, de relaxe, d'acquiescement ou de classement sans suite pour insuffisance de charges
  - 3.3. La mise à jour des données
    - 3.3.1. Le rôle des services de police
      - 3.3.1.1. Les services territoriaux
      - 3.3.1.2. Les services gestionnaires du STIC
    - 3.3.2. Le rôle du procureur de la République
      - 3.3.2.1. Le contrôle lors de l'enregistrement des informations
      - 3.3.2.2. Le maintien de la fiche « navette »

3.3.2.3. La transmission des informations relatives aux suites judiciaires

3.3.2.3.1. Décision de relaxe ou d'acquittement

3.3.2.3.2. Décision de non-lieu ou de classement sans suite motivée par une insuffisance de charges

## INTRODUCTION

### Présentation du STIC

Le système de traitement des infractions constatées (STIC) est un fichier de police informatisé regroupant les informations relatives aux circonstances de temps et de lieu de commission des infractions constatées ou élucidées par les services de la police nationale dans leur activité de police judiciaire. Il comprend des données relatives aux personnes formellement mises en cause au cours de l'enquête ainsi qu'aux victimes de ces infractions.

Ces informations sont issues des procédures établies pour crime, pour délit ou pour une liste de contraventions de cinquième classe (*cf.* annexe I), qui sont transmises à l'autorité judiciaire : procureur de la République ou juge d'instruction. Elles sont résumées dans les comptes rendus d'enquête après identification (CREi), les comptes rendus d'infractions (CRI) ou les rapports de synthèse.

Le régime juridique du STIC s'applique également à deux applications non interconnectées à ce jour : le logiciel de rédaction de procédures (LRP) et le STIC-CANONGE. Le STIC est alimenté par le logiciel OMEGA au sein de la préfecture de police et par le logiciel STIC-FCE (faits constatés et élucidés) pour l'ensemble des autres services de police.

Le STIC est placé sous la responsabilité du directeur général de la police nationale. Il est géré par la sous-direction de la police technique et scientifique de la direction centrale de la police judiciaire (service central de documentation criminelle-SCDC), situé à Ecully (69).

### Le nouveau contexte législatif et réglementaire

L'article 21 de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure (LSI) fixe le cadre législatif applicable aux traitements automatisés de données à caractère personnel recueillies aux cours des enquêtes judiciaires (*cf.* annexe II).

L'article 17-1 de la loi n° 95-73 du 21 janvier 1995 modifié par l'article 25 de la LSI constitue la base législative applicable aux enquêtes administratives impliquant la consultation des traitements de données visées à l'article 21 de cette même loi. Le décret n° 2005-1124 du 6 septembre 2005 énumère ces enquêtes, sans préjudice de dispositions législatives ou réglementaires ultérieures (*cf.* annexe III).

Ces évolutions normatives ont rendu nécessaire la révision du décret n° 2001- 583 du 5 juillet 2001 portant création du système de traitement des infractions constatées (STIC). Cette modification est intervenue conformément aux dispositions de la loi « informatique et libertés » du 6 janvier 1978 telle que modifiée par la loi du 6 août 2004.

### Le projet ARIANE

Les applications STIC et JUDEX (cette dernière est l'équivalent du STIC dans la gendarmerie nationale) sont à l'heure actuelle totalement distinctes, au sens de la loi « informatique et libertés » : il n'existe aucune interconnexion entre elles.

Afin de permettre la réciprocité des consultations de ces traitements informatisés, certains services de police disposent d'un accès au système JUDEX, des unités de la gendarmerie ayant parallèlement un accès au STIC.

Cette possibilité a été mise en œuvre par le biais d'une instruction conjointe DGPN-DGGN en date du 19 janvier 2005.

Enfin, conformément aux orientations de la loi d'orientation et de programmation pour la sécurité intérieure du 29 août 2002, une nouvelle application informatique est en cours de réalisation pour remplacer ces systèmes d'information en voie d'obsolescence. Dénommée ARIANE (application de rapprochement, d'identification et d'analyse pour les enquêtes), elle intégrera courant 2008 les informations des fichiers STIC et JUDEX au sein d'un traitement automatisé unique.

## 1. Les règles de fonctionnement du STIC

### 1.1. L'alimentation du traitement

#### 1.1.1. Les catégories d'informations enregistrées

##### 1.1.1.1. Les données à caractère personnel

Les services de police inscrivent dans le STIC les informations recueillies dans le cadre de leur mission de police judiciaire, lors de l'établissement des procédures par les enquêteurs. La qualité des informations enregistrées dépend donc très étroitement de l'exactitude et de la précision des renseignements retranscrits, en particulier s'agissant de l'état civil des personnes citées en procédure, victimes ou mis en cause, ainsi que de la qualification des infractions relevées.

Les personnes morales mises en cause font également l'objet d'un enregistrement au STIC depuis le décret du 14 octobre 2006.

S'y ajoutent les informations issues :

- des procédures établies par des unités de la gendarmerie nationale ou par des agents des douanes habilités à exercer des missions de police judiciaire, lorsqu'un service de police est appelé à en assurer la continuation ou la conduite commune ;
- des traitements gérés par des organismes de coopération internationale en matière de police judiciaire (comme Interpol ou Europol) ou par des services de police étrangers, dès lors qu'ils présentent, pour la protection des données personnelles, des garanties suffisantes à celles du droit interne, en application des engagements internationaux régulièrement introduits dans l'ordre juridique interne.

##### 1.1.1.2. Les données à caractère personnel dites « sensibles »

Les données « sensibles » au sens de l'article 8 de la loi « informatique et libertés » sont celles qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle.

Celles-ci ne peuvent faire l'objet d'une inscription que sous les réserves suivantes :

- d'une part, les informations concernées doivent résulter de la nature ou des circonstances de l'infraction ou se rapporter à des signes physiques particuliers, objectifs et permanents en tant qu'éléments de signalement des personnes ;
- d'autre part, l'inscription de ces informations doit rester subordonnée à la finalité du fichier, c'est-à-dire strictement nécessaire à la recherche et à l'identification des auteurs des crimes, délits et contraventions prévus par le décret.

##### 1.1.1.3. La prise en compte des objets dans le traitement

Sont enregistrés les objets saisis, volés, découverts ou remarqués lors de la commission d'une infraction. Certains d'entre eux (billets de banque, armes, documents d'identité) sont ensuite transmis au système d'information Schengen (SIS).

#### 1.1.2. Les catégories de personnes enregistrées

Seuls les mis en cause et les victimes sont enregistrés. Les témoins ne le sont en aucun cas.

##### 1.1.2.1. Les mis en cause

Il s'agit des personnes à l'encontre desquelles sont réunis, lors de l'enquête préliminaire, de flagrance ou sur commission rogatoire, des indices graves ou concordants rendant vraisemblable qu'elles aient pu participer, comme auteur(s) ou complice(s), à la commission d'un crime, d'un délit ou d'une contravention de 5<sup>e</sup> classe prévue aux articles R. 625-1 à R. 625-3, R. 625-7, R. 625-9, R. 635-1, R. 635-3 à R. 635-5, R. 645-1, R. 645-2, R. 645-4 à R. 645-12 du code pénal (*cf.* annexe I).

Sont exclues les trois contraventions réprimant respectivement la vente forcée par correspondance, l'abandon d'épaves et le défaut de vérifications de certaines dispositions du code civil par un officier d'état civil prévues par les articles R. 635-2, R. 635-8 et R. 645-3 du code pénal.

La définition du mis en cause mentionnée ci-dessus n'implique pas que la procédure donne nécessairement lieu à la mise en examen de celui-ci pour qu'il soit procédé à son enregistrement dans le fichier.

Toutefois, en évoquant la pluralité, la gravité ou la concordance des indices, le droit impose à l'enquêteur de veiller à ce que ne soient retenus que des éléments objectifs et confirmés par l'enquête, par opposition à l'indice unique ou à la simple dénonciation, insuffisants pour qualifier la mise en cause.

La mise en cause est à proscrire dans les cas suivants (liste indicative) :

- plainte contre personne dénommée si les faits ne sont pas avérés ;
- fait de nature civile ou commerciale alors même que le parquet a demandé de prendre la plainte ;

- exécution d'une enquête de curriculum vitae dans le cadre d'une commission rogatoire ;
- notification d'un mandat ;
- personne placée en garde à vue mais dont la mise en cause n'est pas confirmée au terme de la procédure.

Une mise en cause avérée entraîne l'inscription de la personne concernée sous la rubrique « mis en cause » du compte rendu d'enquête après identification (CREi), ou bien la rédaction d'un rapport de synthèse faisant expressément état de cette mise en cause.

*Rappel important* : l'identité des personnes placées en garde à vue et dont la mise en cause n'est pas avérée doit être renseignée sous la rubrique « GAV non mis en cause » du CREi.

#### 1.1.2.2. Les victimes

Il s'agit des personnes, physiques ou morales, victimes d'un crime, d'un délit ou de l'une des contraventions de 5<sup>e</sup> classe mentionnées à l'annexe I.

Peuvent être enregistrées les personnes dont la qualité de victime ressort des éléments de l'enquête, ainsi que les victimes au nom desquelles une plainte a été déposée.

### 1.2. Les durées de conservation des informations

Un système d'épurement automatique des données du STIC intervient à l'expiration de leur délai de conservation. Seules les informations à caractère personnel permettant l'identification de la personne font l'objet d'un effacement. Les autres sont conservées pour les nécessités de la recherche criminelle et les besoins de l'analyse statistique.

Le point de départ du délai de conservation des informations à caractère personnel enregistrées dans le STIC est la date de leur inscription dans le fichier. Si une nouvelle mise en cause de la même personne intervient avant l'expiration du délai de conservation des faits initiaux, le délai de conservation restant le plus long s'applique à l'ensemble des infractions enregistrées.

#### 1.2.1. Les durées de conservation des informations relatives aux mis en cause

Elles varient en fonction de la gravité des faits et de l'âge du mis en cause (*cf.* annexe IV).

##### 1.2.1.1. Le régime applicable aux majeurs

La durée de conservation est en principe de vingt ans.

Deux exceptions sont cependant prévues à cette durée de conservation :

- le délai est ramené à cinq ans quand la personne est mise en cause pour l'un des délits prévus par le code de la route, ou prévus par les articles 227-3 à 227-11 (abandon de famille et atteintes à l'autorité parentale), 221-6 (homicide involontaire), 222-19 (blessures involontaires), 225-10-1 (racolage public), 311-3 (vol simple), 314-5 (détournement de gage), 314-6 (détournement d'objet saisi), 431-1 (entrave à la liberté d'expression, du travail, d'association, de réunion ou de manifestation), 431-4 (attroupement non armé), et L. 3421-1 du code de la santé publique (usage illicite de substances ou plantes classées comme stupéfiants), ainsi que pour les contraventions de 5<sup>e</sup> classe énumérées par l'article 2 du décret (*cf.* annexe I) ;
- le délai est porté à quarante ans lorsque la personne est mise en cause pour les infractions présentant une particulière gravité et figurant dans l'annexe I du décret relatif au STIC (*cf.* annexe IV).

##### 1.2.1.2. Le régime applicable aux mineurs

La durée de conservation de principe est de cinq ans. Elle est portée à dix ou vingt ans pour les infractions les plus graves (*cf.* annexe IV).

Les informations relatives aux mineurs de moins de dix ans ne sont pas enregistrées, sauf pour des faits particulièrement graves ou en raison de la personnalité des mineurs.

#### 1.2.2. Les durées de conservation des informations relatives aux victimes

Les données concernant la victime sont en principe conservées quinze ans, sous deux réserves :

- la victime peut exercer son droit d'opposition au maintien des données la concernant, une fois que l'auteur des faits a été définitivement condamné (art. 9 du décret STIC) ;
- les informations à caractère personnel attachées à des objets identifiables en eux-mêmes, tels que les œuvres d'art, les bijoux ou les armes, sont conservées jusqu'à leur découverte afin de les restituer à leur propriétaire légitime.

## 2. Les règles d'utilisation du traitement

### 2.1. L'habilitation des agents et leur contrôle

L'accès au STIC est géré par l'application informatique CHEOPS, portail d'accès qui intègre les principales applications réglementaires et policières, dont les accès sont contrôlés et sécurisés.

Les données enregistrées dans le STIC sont directement accessibles aux fonctionnaires de la police nationale en raison de leurs missions de police judiciaire, de police administrative ou, le cas échéant, d'administration du système. Certains militaires de la gendarmerie nationale exerçant une mission de police judiciaire disposent également d'un accès direct (mais le nombre de postes d'accès est aujourd'hui limité pour des raisons techniques).

Les dispositions introduites par le décret modificatif de 2006 relatif au STIC ouvrent désormais un accès limité aux agents des préfectures chargés de l'instruction de certaines enquêtes administratives.

#### 2.1.1. Les deux types d'habilitations individuelles

##### 2.1.1.1. L'habilitation des agents des services de la police nationale

###### 2.1.1.1.1. L'attribution d'un profil d'utilisateur

Les agents doivent être individuellement désignés et spécialement habilités pour les recherches relatives aux infractions dont ils ont à connaître, respectivement par le directeur général de la police nationale et le directeur général de la gendarmerie nationale, ou par les personnels sur lesquels ils ont autorité, appartenant à la catégorie A ou ayant le rang d'officier, auxquels ils ont donné délégation à cet effet.

Chaque habilitation détermine le profil de l'utilisateur du STIC (consultation, alimentation, établissement de statistiques) correspondant à l'exercice de sa mission (police judiciaire, police administrative, gestion d'application ou documentation opérationnelle).

Un modèle d'habilitation est joint à l'annexe V.

###### 2.1.1.1.2. Le règlement de sécurité du système CHEOPS

L'habilitation, notifiée à chaque utilisateur, lui confère des droits à consulter le fichier.

Un mot de passe personnel et confidentiel, associé au matricule de l'utilisateur, lui est délivré par le système, et automatiquement renouvelé tous les trois mois. Toute disposition doit être prise par l'utilisateur pour que ce code confidentiel reste connu de lui seul.

Cette habilitation devient caduque en cas de changement d'affectation ou de fonction de l'utilisateur. Le cas échéant, il doit faire l'objet d'une nouvelle habilitation.

##### 2.1.1.2. L'habilitation des agents de préfecture investis de missions de police administrative

Certains agents de préfecture, investis de missions de police administrative et qui participent directement à l'instruction des enquêtes administratives impliquant la consultation du STIC, peuvent consulter ce dernier.

###### 2.1.1.2.1. La procédure d'habilitation des agents

Ces agents sont individuellement désignés et spécialement habilités par le préfet, ou bien le secrétaire général ou le sous-préfet d'arrondissement ayant délégation de signature à cet effet. Un modèle d'habilitation est joint à l'annexe V.

###### 2.1.1.2.2. Les modalités de consultation

Les agents de préfecture ne peuvent accéder qu'à une information très limitée, à savoir si la personne sur laquelle est conduite une enquête administrative est enregistrée ou non dans le STIC en qualité de mis en cause.

Ce module d'accès limité a pour objectif de permettre un traitement plus rapide des dossiers ne présentant aucune difficulté particulière et aucun antécédents judiciaires.

Si la consultation fait apparaître que la personne est connue du STIC en tant que mis en cause, il convient de saisir les services de police nationale du département. Grâce aux informations plus larges auxquelles ils ont accès dans le STIC, et au besoin en consultant directement la procédure judiciaire ayant motivé l'inscription, les policiers habilités sont en mesure d'approfondir l'enquête administrative au regard des antécédents judiciaires dont la prise en compte est pertinente, en prenant en compte la nature de la décision administrative considérée.

Il revient ensuite au préfet d'apprécier la situation de chaque intéressé en fonction des faits révélés par l'enquête, au regard de la décision administrative qui le concerne. Il tient compte de la gravité des faits commis, de leur ancienneté et de leur éventuelle répétition.

En effet, la seule présence dans le STIC d'une personne mise en cause ne suffit à elle seule à motiver une décision défavorable.

#### 2.1.2. La traçabilité des consultations effectuées par les agents habilités

La traçabilité des interrogations est désormais une obligation juridique précisée dans l'article 7 du décret.

Le système CHEOPS mémorise pour le STIC la trace de toutes les interventions effectuées, qui sont conservées trois ans. Une journalisation horodatée retrace nominativement aussi bien les actions d'alimentation que de consultation.

Le message de mise en garde suivant est systématiquement délivré dès la connexion au système : « Toute connexion à CHEOPS garde trace de vos interventions. Voulez-vous continuer ? ».

Les chefs de services peuvent accéder à un module statistique qui comptabilise les interrogations effectuées par les agents placés sous leur autorité.

#### 2.1.3. Contrôle hiérarchique et sanctions disciplinaires et pénales

Toute utilisation frauduleuse entraîne la mise en jeu de la responsabilité professionnelle de l'agent, sans préjudice de la responsabilité pénale.

##### 2.1.3.1. La responsabilité hiérarchique

Les responsables hiérarchiques doivent veiller au respect de la déontologie dans la consultation des fichiers. Une interrogation n'est licite que dans les cas prévus par la loi, pour les besoins exclusifs des missions de police administrative et judiciaires.

Le strict respect de ces règles est une condition indispensable à l'acceptation par les citoyens de l'existence des fichiers de police. Les organes de contrôle (Parlement, autorités judiciaires, autorités administratives indépendantes, corps d'inspection) sont particulièrement vigilants.

Aussi, les chefs de service doivent-ils prendre toutes les précautions utiles dans le choix des agents habilités. Ils rappelleront régulièrement à leurs collaborateurs les responsabilités impliquées par l'obtention d'une habilitation. Ils vérifieront périodiquement le respect des règles de bonne utilisation du STIC et veilleront au retrait effectif des habilitations devenues caduques (*cf.* note PN/CAB/CPS N° 06-13032 diffusée aux services de police le 9 mai 2006).

##### 2.1.3.2. Les sanctions disciplinaires

Tout usage non conforme peut être qualifié de faute professionnelle de nature à justifier une sanction disciplinaire conformément aux dispositions prévues par le décret n° 86-592 du 18 mars 1986 portant code de déontologie de la police nationale et au nouveau règlement d'emploi de la police nationale.

Ce règlement énonce les sanctions disciplinaires encourues par un fonctionnaire en cas de consultation non autorisée.

Il en va de même pour les agents de préfecture, au regard des règles de déontologie qui leur sont applicables.

##### 2.1.3.3. Les sanctions pénales

En application de la loi « informatique et libertés » du 6 janvier 1978, le code pénal réprime un certain nombre d'infractions liées à une utilisation frauduleuse des données. Le fait de procéder à une consultation dans une situation non autorisée, de faire un usage détourné des informations ou de les divulguer à des tiers non autorisés, expose l'agent responsable à des sanctions pénales.

Les incriminations et sanctions sont prévues par les articles 226-17 et 226-20 à 226-23 du code pénal, qui édictent des peines de un à cinq ans d'emprisonnement et de 100 000 à 300 000 € d'amende.

### 2.2. L'exploitation des données

L'exploitation de ces données dans les procédures doit être assortie de certaines précautions relatives au cadre juridique de la consultation et à l'usage des informations recueillies.

#### 2.2.1. L'utilisation en matière de police judiciaire

##### 2.2.1.1. Les destinataires

Le décret révisé a élargi en application de la loi du 18 mars 2003 les catégories de destinataires des informations contenues dans le STIC pour les besoins des enquêtes judiciaires. Sont désormais destinataires :

- les personnels de la police nationale, de la gendarmerie nationale et des services des douanes qui exercent des missions de police judiciaire individuellement désignés et spécialement habilités pour les recherches relatives aux infractions dont ils ont à connaître ;
- les personnels de l'Etat investis par la loi de missions de police judiciaire ;

- les magistrats du parquet ;
- les magistrats instructeurs, pour les recherches relatives aux infractions dont ils sont saisis ;
- les organismes de coopération internationale en matière de police judiciaire et les services de police étrangers.

Etre destinataire des données n'implique pas nécessairement de disposer d'un accès direct au traitement. Actuellement, seuls les services de police et certaines unités de gendarmerie accèdent directement aux données contenues dans le STIC. En raison d'obstacles techniques, les magistrats ne disposent pas à ce jour d'un accès direct au traitement, mais ils peuvent se faire communiquer les données à tout moment.

Les services qui consultent le STIC pour le compte de destinataires non connectés doivent tenir un journal de ces consultations, dans lequel est systématiquement reporté, le nom et la qualité de la personne sollicitant la consultation (autres services de police ou de gendarmerie, procureur de la République, juge d'instruction...) et le cadre juridique dans lequel elle intervient.

#### 2.2.1.2. Les cadres juridiques de consultation

La consultation du STIC est autorisée dans tous les cadres d'enquête judiciaire, quelle que soit la nature de l'infraction : crime, délit ou contravention.

L'utilisation du STIC est exclue lors d'une opération de contrôle d'identité prévue à l'article 78- 2 du code de procédure pénale.

En revanche, elle est autorisée pour une vérification d'identité conduite en application de l'article 78-3 du même code pour trouver un élément d'identification (par recoupement, par exemple). Celui-ci devra être toutefois conforté par des vérifications complémentaires, le STIC ne pouvant à lui seul établir directement l'identité d'une personne.

#### 2.2.1.3. Les conditions d'utilisation des informations dans le cadre des procédures judiciaires

L'article 5 du décret n° 2001-583 du 5 juillet 2001 énonce que seules les informations enregistrées dans le STIC et relatives à la procédure judiciaire en cours peuvent être jointes au dossier de la procédure. Il en résulte qu'il est en principe interdit de faire figurer dans celui-ci l'ensemble des antécédents de la personne mise en cause. Parce qu'elle comporte d'autres renseignements, la jonction d'une édition du STIC doit donc être proscrite.

Toutefois, sur réquisition expresse, le magistrat du parquet ou de l'instruction peut solliciter à partir du STIC l'édition « antécédent de la personne physique » et demander qu'elle soit jointe à la procédure. Cette opération présente actuellement un intérêt d'autant plus grand pour les magistrats qu'ils ne disposent pas à ce jour, pour des raisons techniques, d'un terminal de consultation.

En outre, si des investigations menées dans le STIC grâce à ses fonctionnalités de recherche criminelle ont permis, au cours de l'enquête, d'identifier la personne mise en cause, il convient de retranscrire précisément en procédure le cheminement suivi. Les informations ainsi recueillies doivent figurer au dossier.

Enfin, obligation est faite à l'enquêteur de vérifier l'exactitude des éléments de réponse issus du STIC avant de les adresser au parquet ou au juge mandant.

#### 2.2.2. L'utilisation en matière de police administrative par les services de police

Autorisée par l'article 17-1 de la LOPSI du 21 janvier 1995 et régie par l'article 6 du décret STIC, la consultation en police administrative est strictement encadrée afin de concilier la sauvegarde de l'ordre public, d'une part, et le respect de la vie privée et des droits et libertés constitutionnellement protégés, d'autre part.

##### 2.2.2.1. Les enquêtes administratives donnant lieu à une consultation

Trois catégories d'enquêtes sont à distinguer :

###### 2.2.2.1.1. *Les décisions administratives de recrutement, d'affectation, d'autorisation, d'agrément ou d'habilitation*

Le décret n° 2005-1124 du 6 septembre 2005 énumère les enquêtes relatives :

- aux affectations et agréments concernant les emplois publics participant à l'exercice des missions de souveraineté de l'Etat ;
- aux emplois publics ou privés relevant du domaine de la sécurité ou de la défense ;
- aux emplois privés ou activités privées réglementées relevant des domaines des jeux, paris et courses ;
- aux missions concernant des zones protégées en raison des activités qui s'y exercent, aux missions concernant les matériels, produits ou activités présentant un danger pour la sécurité publique (*cf.* annexe III).

La loi n° 2007-297 du 5 mars 2007 relative à la prévention de la délinquance a prévu qu'il en soit de même pour le recrutement des volontaires citoyens de la police nationale (art. 30).



#### 2.2.2.1.2. *Les demandes relevant du droit des étrangers ou relatives aux ordres nationaux*

L'instruction des demandes d'acquisition de la nationalité française, de la délivrance et le renouvellement des titres relatifs à l'entrée et au séjour des étrangers peut donner lieu à consultation du STIC.

La nomination et la promotion dans les ordres nationaux peuvent également donner lieu à une telle consultation.

#### 2.2.2.1.3. *Les risques d'atteinte à l'ordre public et à la sécurité des installations privées*

L'exercice de missions ou d'interventions, lorsque la nature de celles-ci ou les circonstances particulières dans lesquelles elles doivent se dérouler, comportent des risques d'atteinte à l'ordre public ou à la sécurité des personnes et des biens, et les mesures de protection ou de défense prises dans les secteurs de sécurité de certaines installations prioritaires de défense, peuvent justifier la consultation du STIC (cf. annexe III).

Aucune autre enquête administrative n'autorise la consultation du STIC, en dehors des dispositions législatives prévoyant expressément la consultation de ce fichier ou l'obligation de communiquer des renseignements qui en sont extraits à une autre administration. Par exemple, les services fiscaux peuvent recevoir communication d'informations en qualité de tiers autorisés dans le cadre d'une réquisition prévue par les articles L. 81 et L. 83 du livre des procédures fiscales.

#### 2.2.2.2. L'encadrement de la consultation à des fins de police administrative

Seul le module spécifique de consultation administrative du STIC doit être utilisé pour conduire une enquête administrative.

##### 2.2.2.2.1. *Les caractéristiques du module de police administrative*

L'accès aux informations par les personnels de police ou de gendarmerie habilités à consulter le STIC dans le cadre de leurs missions de police administrative est plus étroit qu'en police judiciaire. En effet, certaines informations sont occultées par rapport au module de police judiciaire :

- celles pour lesquelles le procureur de la République a transmis au gestionnaire du STIC des suites judiciaires favorables au mis en cause : décision d'acquiescement, de relaxe, de non-lieu ou de classement sans suite motivé par insuffisance de charges ;
- toutes les informations nominatives relatives aux victimes.

##### 2.2.2.2.2. *La compétence non liée de l'autorité administrative pour la prise de décision*

La consultation du STIC à des fins administratives est de surcroît encadrée par les exigences de l'article 10 de la loi « informatique et libertés » du 6 janvier 1978 selon laquelle « aucune [autre] décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données destinées à établir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité. »

Une grande attention doit être portée à cet impératif rappelé solennellement par le Conseil constitutionnel en 2003.

Aussi, les éléments d'information communiqués par les services de police aux autorités administratives dans le cadre d'une enquête ne doivent pas se limiter à la simple transmission des éléments de la fiche STIC. Ils doivent comprendre une analyse et une appréciation critique issue de la consultation.

En cas d'inscription, il incombe aux services de police de vérifier la pertinence des informations recueillies en fonction de la nature de l'enquête sollicitée. Il y a lieu de s'appuyer sur le ou les dossiers de procédure judiciaire, en s'attachant notamment à la réalité des faits imputés au requérant, à leur gravité, à leur répétition éventuelle et à l'âge du mis en cause au moment de leur commission. Cette vérification doit intervenir même s'il s'agit d'une personne ayant déjà fait l'objet d'une enquête administrative (renouvellement d'agrément par exemple).

La qualification pénale des faits telle qu'elle apparaît sur la fiche, et qui confère à ces derniers leur caractère délictueux, ne doit pas être transmise en l'état à l'autorité administrative. Les faits étant susceptibles d'être amnistiés et de perdre en conséquence leur caractère infractionnel, il incombe de les rapporter sans les qualifier pénalement.

Il est par conséquent interdit de joindre la copie de l'édition tirée du STIC à un rapport rédigé dans le cadre d'une mission de police administrative.

Seuls les sites de référence d'archivage tels que le service central de documentation criminelle à Ecully, les services régionaux de documentation criminelle des services régionaux de police judiciaire et la division de la statistique et de la documentation criminelle de la préfecture de police de Paris, procèdent aux mises à jour des suites judiciaires de manière exhaustive. Ce sont donc ces archives qu'il convient de consulter.

### 3. Les droits des personnes enregistrées dans le STIC

#### 3.1. *Le nouveau droit d'information des victimes*

Le décret du 14 octobre 2006 a introduit un droit à l'information des victimes enregistrées dans le STIC, et à elles seules. Une information claire doit leur être délivrée, leur précisant que des données à caractère personnel les concernant peuvent être enregistrées, dans le seul but de faciliter l'identification des auteurs d'infractions.

En vertu du décret, elles disposent :

- d'un droit d'accès indirect aux données ;
- en cas d'erreur, d'un droit de rectification de ces données ;
- lorsque l'auteur des faits a été définitivement condamné, d'un droit d'opposition à leur conservation dans le STIC.

Cette information sera assurée dans la « Charte de l'accueil du public et de l'assistance aux victimes », dont l'affichage est effectué dans tous les commissariats. Cette charte fera l'objet d'une très prochaine révision afin qu'un article nouveau y soit inséré (*cf.* annexe VI).

En outre, sur simple demande orale ou écrite, la notice explicative figurant en annexe VII devra être remise à toute victime.

#### 3.2. *Le droit d'accès et de rectification des personnes*

##### 3.2.1. L'exercice du droit d'accès devant la CNIL

###### 3.2.1.1. Un droit d'accès ouvert à toute personne physique

Sans préjudice de ses pouvoirs de contrôle de tout fichier, sur place et sur pièces, la CNIL exerce pour le compte des citoyens un contrôle de nature spécifique prévu par l'article 41 de la loi « informatique et libertés » : le droit d'accès indirect au fichier.

En effet, alors que le droit commun dispose que le droit d'accès ouvert à tout citoyen s'exerce directement auprès du gestionnaire du fichier, la loi assure la protection des finalités des fichiers de police judiciaire en prévoyant un droit d'accès indirect.

L'exercice de ce droit est ouvert aux seules personnes physiques. Les personnes morales inscrites au STIC n'en bénéficient pas.

###### 3.2.1.2. Les modalités d'accès aux données enregistrées dans le traitement

Le requérant désireux d'exercer son droit d'accès doit saisir la CNIL, qui procède en son nom aux vérifications le concernant. A cette fin, cette dernière désigne l'un de ses membres appartenant ou ayant appartenu au Conseil d'Etat, à la Cour de cassation ou à la Cour des comptes, pour mener toute investigation utile et faire procéder aux modifications nécessaires par le gestionnaire du fichier.

Lorsque la CNIL et le gestionnaire du fichier constatent d'un commun accord que la communication de données à caractère personnel ne met pas en cause la sûreté de l'Etat, la défense ou la sécurité publique, la CNIL les communique à la personne intéressée.

A l'inverse, lorsque le gestionnaire du fichier, ou encore le procureur de la République si l'affaire n'est pas judiciairement close, estiment que les informations ne sont pas communicables, la CNIL informe le requérant qu'il a été procédé aux vérifications nécessaires sans préciser la nature de celles-ci. Il convient de préciser que le refus de communication s'effectue sous le contrôle du juge administratif.

Par souci de simplification, le nouveau décret dispense désormais, lorsque la procédure judiciaire est close, de l'obligation de recueillir l'accord du procureur de la République.

##### 3.2.2. Les demandes de rectifications des données

Les demandes de mise à jour adressées au gestionnaire du fichier peuvent émaner soit des victimes, soit des mis en cause.

###### 3.2.2.1. Demandes émanant des victimes

Une fois que l'auteur des faits a été condamné définitivement, toute personne inscrite dans le fichier en qualité de victime peut demander à ce que les informations nominatives la concernant soient supprimées du fichier. A l'appui de sa demande, le requérant est tenu de fournir une attestation de l'autorité judiciaire.

Le gestionnaire du STIC territorialement compétent (*cf.* 3.3.1.2) est le seul habilité à traiter une telle requête, soit qu'elle lui parvienne directement, soit qu'elle lui soit réadressée par un autre service en ayant été saisi.

La mise à jour est portée à la connaissance du demandeur.

### 3.2.2.2. Demandes émanant des mis en cause

#### 3.2.2.2.1. *Demande de requalification des faits*

Lorsque l'autorité judiciaire a retenu une qualification des faits différente de celle initialement adoptée par l'officier de police judiciaire et enregistrée dans le STIC, l'article 3 (troisième alinéa) du décret relatif au STIC ouvre aux mis en cause la possibilité de saisir la CNIL ou le procureur de la République pour demander la rectification. Il en va ainsi aussi bien en cas de requalification en cours d'instruction qu'à l'occasion du jugement.

Dans le cas où le procureur a été directement saisi par le requérant, il informe le gestionnaire du fichier de l'opportunité de procéder ou non aux corrections demandées. Si c'est un service de police qui a été saisi, la consultation du parquet est bien évidemment nécessaire pour vérifier le bien-fondé de la demande.

La réponse au requérant lui est adressée par la CNIL.

#### 3.2.2.2.2. *Demande de mise à jour suite à une décision de non-lieu, de relaxe, d'acquittement ou de classement sans suites pour insuffisance de charges*

Les décisions judiciaires « favorables » donnent lieu à une mise à jour du STIC, mais selon des modalités différentes selon leur nature.

En cas de décision de relaxe ou d'acquittement devenue définitive, l'effacement pur et simple des données est le principe. Toutefois, dans l'intérêt des finalités du fichier, le procureur de la République peut prescrire le maintien des données, qui font alors l'objet d'une mention relative au jugement.

A l'inverse, la conservation des données dans le fichier est le principe pour les décisions de non lieu ainsi que, parmi les décisions de classement sans suite, celles et seulement celles qui sont motivées par une insuffisance de charges. Toutefois, le Procureur de la République peut ordonner leur suppression.

Toute personne ayant bénéficié de l'une de ces décisions peut solliciter la CNIL ou le procureur de la République pour vérifier si la mise à jour correspondante est intervenue ou, à défaut, pour l'obtenir. Comme précédemment, le procureur de la République sera saisi pour avis par le gestionnaire régional du STIC des requêtes qui ne lui aurait pas été adressées à l'origine.

Le droit de rectification est souvent exercé pour s'assurer qu'une mention au STIC n'aura pas d'incidence défavorable à l'occasion d'une enquête administrative puisque les données complétées d'une mention sont rendues invisibles dans le module de police administrative (cf. 2.2.2.2.1.).

Dans tous les cas autres que ces décisions « favorables », et notamment pour les décisions de classement sans suite portant sur des faits avérés et non motivées pour une insuffisance de charges (désistement de la victime, médiation pénale, rappel à la loi), les informations sont conservées selon la durée de conservation applicable (cf. annexe VIII).

Enfin, les personnes morales ne disposant pas du droit d'accès aux fichiers de police prévu par la loi « informatique et libertés », elles doivent présenter leurs demandes de mise à jour ou de requalification au procureur de la République territorialement compétent.

### 3.3. *La mise à jour des données*

#### 3.3.1. Le rôle des services de police

L'article 6 de la loi « informatique et libertés » du 6 janvier 1978 fait obligation au gestionnaire du fichier de compléter ou de corriger, même d'office, toute information contenue dans ce fichier lorsqu'il a connaissance de son inexactitude ou de son caractère incomplet.

##### 3.3.1.1. Les services territoriaux

Les services de police territoriaux ayant établi la procédure procèdent aux corrections et aux modifications des informations obsolètes ou erronées qu'ils auraient enregistrées et en avisent le gestionnaire du STIC territorialement compétent.

##### 3.3.1.2. Les services gestionnaires du STIC

L'obligation de mise à jour pour tenir compte des suites judiciaires incombe au gestionnaire du fichier. Si la loi prescrit que cette mise à jour doit intervenir systématiquement, le gestionnaire du fichier est cependant tributaire de la transmission des informations par l'autorité judiciaire.

Les services gestionnaires du STIC sont :

- les services régionaux suivants, chargés de l'administration régionale du STIC dans leur ressort territorial :
  - les directions interrégionales de police judiciaire, les directions régionales de police judiciaire ou les services régionaux de police judiciaire, et en leur sein le service régional de documentation criminelle (SRDC) ;
  - la direction régionale de la police judiciaire de la Préfecture de police – division de la statistique et de la documentation criminelle (DSDC) ;

- le service central de documentation criminelle (SCDC) de la direction centrale de la police judiciaire – sous-direction de la police technique et scientifique, qui est la direction d'application du STIC.

Le gestionnaire régional procède à la rectification ou à la mise à jour des informations erronées ou incomplètes et porte toute difficulté à la connaissance de la direction d'application, qui assure par ailleurs un contrôle supplémentaire et procède aux corrections qu'elle jugera nécessaires.

### 3.3.2. Le rôle du procureur de la République

La circulaire du directeur des affaires criminelles et des grâces du 26 décembre 2006 rappelle le rôle et les pouvoirs de l'autorité judiciaire, relativement à l'utilisation du STIC.

L'article 3 du décret n° 2001-583 du 5 juillet 2001 place le STIC sous le contrôle du procureur de la République, qui a accès aux informations.

Ce dernier exerce ses attributions de contrôle sur les informations issues des procédures judiciaires relevant de sa compétence territoriale au moment de leur transmission ou concernant des personnes mises en cause dans les procédures dont il est saisi.

Conformément à la loi du 18 mars 2003, le procureur de la République est tenu de transmettre au SRDC de son ressort territorial les décisions judiciaires favorables au mis en cause justifiant une mise à jour.

#### 3.3.2.1. Le contrôle lors de l'enregistrement des informations

Ce contrôle repose sur la transmission des comptes-rendus d'enquête après identification (CREi), des comptes-rendus d'infraction (CRI) et des rapports de synthèse. Il s'appuie également sur la transmission d'une fiche de suites judiciaires, dite fiche « navette », automatiquement éditée lors de l'impression du CREi par le logiciel de rédaction de procédures (LRP), et jointe à la procédure par l'enquêteur.

Le ministère de la justice renouvellera prochainement son système d'informations, grâce à l'application informatique CASSIOPEE, de même que les services de police adopteront de nouveaux logiciels (ARDOISE et ARIANE, destinés à remplacer le LRP et le STIC).

Il est prévu à terme (courant 2008) qu'une passerelle informatique fonctionnant dans les deux sens permette l'échange de certaines données contenues dans les procédures pénales entre les services d'enquête et les tribunaux, afin d'automatiser les opérations de mise à jour.

Dans l'attente de cette mise en place, les magistrats du parquet, qui ne disposent pas d'un accès informatique à l'application STIC peuvent se déplacer dans les services de leur ressort pour le consulter.

#### 3.3.2.2. Le maintien de la fiche « navette »

La fiche-navette (*cf.* annexe IX) est indispensable pour permettre au parquet de contrôler les données inscrites dans le STIC et de transmettre en retour les suites judiciaires apportées à la procédure.

Comme elle ne constitue pas une pièce de procédure, elle ne doit pas faire l'objet d'une cotation. Elle a vocation à permettre au magistrat de transmettre ultérieurement au gestionnaire du STIC une éventuelle information de non-lieu, de relaxe, d'acquiescement ou de classement sans suite pour insuffisance de charge.

Lors de la réception du compte rendu ou du rapport de synthèse et des fiches annexées, le procureur de la République exerce son contrôle sur les données enregistrées dans le STIC et peut à cette occasion, demander une rectification, un complément ou un effacement.

C'est la qualification des faits établie par l'enquêteur qui détermine l'inscription initiale des mentions dans le STIC. En revanche, il appartient au procureur de la République de vérifier cette qualification juridique et, le cas échéant, de lui substituer la qualification appropriée, voire de solliciter l'effacement de la mention dans le cas où la qualification finalement retenue ne permettrait pas d'inscription au STIC sur la base de l'article 2 du décret.

Enfin, l'inscription au STIC peut également intervenir à l'occasion d'investigations réalisées en exécution d'une commission rogatoire. Dans ce cas, les procès-verbaux et le compte rendu d'enquête (ou compte rendu d'infraction) avec, le cas échéant, les fiches-navettes relatives à chaque mis en cause, sont adressés au juge d'instruction mandant et non au procureur de la République, conformément aux dispositions du dernier alinéa de l'article 151 du code de procédure pénale.

Dans ce dernier cas, le procureur de la République prend l'initiative d'exercer son contrôle lors de la communication du dossier d'instruction, soit sur sa demande de consultation en application des dispositions de l'article 82 du code de procédure pénale, soit à l'occasion d'une ordonnance de soit-communicé du juge d'instruction aux fins de réquisitions, relative au dossier.

Il conviendra de s'assurer que le compte rendu d'infraction ou le rapport de synthèse ainsi que les fiches-navette annexées restent joints au dossier d'instruction de manière visible mais mobile, par exemple dans une sous-chemise agrafée en début de dossier.

### 3.3.2.3. Transmission des informations relatives aux suites judiciaires

Le décret fait obligation au procureur de la République de transmettre les décisions judiciaires favorables au mis en cause.

Ainsi sont adressées au service régional de police judiciaire compétent, les décisions de relaxe, d'acquiescement, de non-lieu et de classement sans suite motivé par une insuffisance de charge. Certaines entraînent un effacement, d'autres l'ajout d'une mention dans le traitement.

#### 3.3.2.3.1. *Décision de relaxe ou d'acquiescement*

Une telle décision, lorsqu'elle est définitive, entraîne l'effacement par le gestionnaire du fichier des données personnelles relatives à la personne mise en cause en ayant bénéficié.

Le procureur de la République peut toutefois prescrire d'initiative le maintien des données personnelles concernées pour des raisons liées à la finalité du fichier.

#### 3.3.2.3.2. *Une décision partielle de relaxe ou d'acquiescement ne donne pas lieu à une mise à jour, sauf à ce que la qualification initiale ait été modifiée*

Décision de non-lieu ou de classement sans suite motivée par une insuffisance de charges

Une telle décision conduit le gestionnaire du fichier à compléter les données à caractère personnel relatives à la personne mise en cause qui en a bénéficié, par une mention indiquant l'intervention de cette décision.

Le classement sans suite prononcé pour un autre motif que l'insuffisance de charges, tel que le classement pour un motif juridique, en opportunité ou en raison du recours à une procédure alternative aux poursuites, ne permet pas de compléter les mentions enregistrées au STIC.

Seuls les classements sans suite correspondant en pratique aux motifs n° 11 et 21 dans la nomenclature de la Chancellerie (absence d'infraction, infraction insuffisamment caractérisée, cf. annexe VIII), exigent une transmission des suites judiciaires par le parquet au gestionnaire du fichier pour adjonction de la mention précitée.

Cependant, le procureur de la République peut ordonner l'effacement des données à caractère personnel dès lors que la personne a été totalement mise hors de cause et que le maintien des informations la concernant dans le STIC n'est plus justifié au regard des finalités du fichier.

En pratique, le procureur de la République retourne au gestionnaire du fichier la fiche-navette, complétée par la mention relative à un classement sans suite motivé par l'insuffisance de charge (motifs 11 ou 21). Le cas échéant, le parquet précise sur la même fiche s'il ordonne l'effacement des données concernées.

Enfin l'attention des services est attirée sur le fait que l'amnistie n'est plus considérée comme un motif susceptible d'entraîner une mise à jour du STIC.

\*  
\* \*

Outil très performant de lutte contre la délinquance grâce à ses fonctions de recherche criminelle, dont c'est la vocation première, le STIC doit être mis en œuvre en garantissant son efficacité dans le parfait respect des libertés individuelles et des règles de droit. Chaque chef de service doit donc veiller scrupuleusement à la diffusion et à l'application de ses modalités d'exploitation. Enfin, son utilisation encadrée à des fins de police administrative, irremplaçable, nécessite aussi la plus grande rigueur afin de préserver la légitimité des enquêtes qui sont menées en le consultant.

Pour le ministre et par délégation :  
*Le directeur général de la police nationale,*  
M. GAUDIN