Ordonnance sur le système de traitement des données relatives à la protection de l'Etat

(Ordonnance ISIS)

du 30 novembre 2001

Le Conseil fédéral suisse,

vu les art. 15, al. 3 et 5, et 30 de la loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI)[1],
vu l'art. 39, al. 3, de la loi fédérale du 20 juin 1997 sur les armes, les accessoires d'armes et les munitions (LArm)[2],

arrête:

Section 1 Dispositions générales

Art. 1 Objet

La présente ordonnance règle l'exploitation, le contenu des données et l'utilisation du système de traitement des données relatives à la protection de l'Etat (ISIS).

Art. 2 Buts

1 ISIS a pour but de faciliter:

a. la mise en œuvre de mesures préventives dans le domaine de la protection fédérale de l'Etat;

b. les tâches de police de sécurité et de police administrative;

c. l'exécution de la législation sur les armes;

2 ISIS est utilisé pour:

a. l'exécution de travaux d'analyse des données saisies et de documentation;

b. l'élaboration de rapports de situation;

c. l'exécution de travaux administratifs;

d. le classement et la gestion de dossiers.

RS **120.3**

1 RS **120**
2 RS **514.54**

Art. 3 Définitions

Dans la présente ordonnance, on entend par:

a. données: les informations mémorisées dans ISIS;

b. données de base: les informations générales se rattachant à certaines ou plusieurs données sur les antécédents;

c. indications principales sur la personne: affichage des données de base: nom(s), prénom(s), organisation ou entreprise; nom(s) d'emprunt; année de naissance; année de naissance d'emprunt; date de naissance; date de naissance d'emprunt; écriture phonétique de tous les noms et prénoms; nationalité, lieu d'origine pour les Suisses;

d. données sur les antécédents: les informations relatives à chaque fait en particulier.

e. données marginales: toutes les données sur les antécédents (sans texte «Vorgang»);

f. consultation ponctuelle: consultation combinée de données relatives à des personnes et à des tiers; seules les données de base et les données marginales s'affichent;

g. données d'image: documents consultés sous forme d'image;

h. données statistiques: inventaires chiffrés établis à partir des informations mémorisées dans ISIS;

i. tiers: personnes ou organisations qui ont un lien avec une personne enregistrée ou avec un bloc de données de base, mais qui ne remplissent pas elles-mêmes les conditions nécessaires pour un enregistrement.

Art. 4 Banques de données

ISIS se compose des banques de données suivantes:

a. «protection de l'Etat» (ST): informations relatives aux personnes et aux événements, tirées des activités préventives déployées dans le domaine de la protection de l'Etat;

b. «police administrative» (VP): informations relatives aux personnes et aux événements relevant du domaine des offices centraux de police administrative du Service d'analyse et de prévention (SAP);

c. «administration» (VE): informations qui sont nécessaires au contrôle des affaires;

d. «documentation» (DO): informations provenant de l'ensemble des domaines d'activité du SAP, conformément à l'art. 11 de l'ordonnance du 27 juin 2001 sur les mesures visant au maintien de la sûreté intérieure (OMSI)[3];

e. «système numérique» (NU), où sont enregistrées des informations relatives à des événements, tirées de programmes déterminés de recherches;

3 RS **120.2**

f. «acquisition d'armes par des étrangers» (DEWA): informations personnelles concernant l'acquisition d'armes par des ressortissants étrangers non titulaires d'un permis d'établissement en Suisse;

g. «révocation d'autorisations et mise sous séquestre d'armes» (DEBBWA): informations personnelles concernant la révocation d'autorisations et la mise sous séquestre d'armes en Suisse;

h. «gestion électronique des documents» (EAV): données d'image des documents sur lesquels se fondent les données de base et les données sur les antécédents;

i. «analyse stratégique et situation» (STRALAG): informations servant à l'élaboration des rapports d'analyse et de situation du SAP;

j. «INFOPRESS»: informations issues de sources accessibles au public.

Art. 5 Données traitées

1 Les données sur les antécédents mémorisées dans les banques de données d'ISIS sont ventilées par matières, pour autant que cela s'avère utile pour la gestion de l'accès.

2 Les différents champs de données sont mentionnés à l'annexe 1[4].

Art. 6 Intranet

1 L'Intranet ISIS est un système de communication fermé et codé. Il se compose d'un Intranet et d'une messagerie électronique.

2 Le SAP ne met ce système qu'à la disposition des utilisateurs d'ISIS.

Section 2 Utilisateurs, raccordement et accès aux données

Art. 7 Utilisateurs

1 Les utilisateurs d'ISIS sont les agents du SAP et ceux des organes cantonaux chargés du maintien de la sûreté intérieure. Ils sont raccordés au système par une procédure d'appel.

2 Les utilisateurs du Service fédéral de sécurité (SFS), de la Police judiciaire fédérale (PJF) et ceux du service fédéral chargé des contrôles de sécurité relatifs aux personnes peuvent être raccordés au système par une procédure d'appel pour en consulter ponctuellement les données ou pour consulter les indications principales sur la personne.

3 Les utilisateurs ont accès aux données qui leur sont nécessaires pour l'accomplissement de leurs tâches légales.

4 Le texte des annexes 1 et 2 de l'ordonnance du 30 novembre 2001 sur le système de traitement des données relatives à la protection de l'Etat n'est publié ni au Recueil officiel ni au Recueil systématique. Des tirés à part peuvent être obtenus auprès de l'OCFIM, 3003 Berne.

4 Le droit d'accès aux données d'ISIS est réglé par le Département fédéral de justice et police (département) à l'annexe 2[5]. Le chef du SAP statue sur les demandes individuelles.

Art. 8 Raccordement des cantons

Les organes cantonaux sont raccordés à ISIS dès que le canton, par ses mesures organisationnelles, offre la garantie d'une utilisation correcte des données et de leur sécurité, et que le département a approuvé la demande cantonale de raccordement.

Art. 9 Accès à la banque de données ST

1 Les agents du SAP peuvent consulter dans la banque de données ST l'ensemble des données de base, données sur les antécédents et données d'image qui leur sont nécessaires à l'accomplissement de leurs tâches légales.

2 Les agents des organes cantonaux préposés au maintien de la sûreté intérieure peuvent consulter dans la banque de données ST l'ensemble des données de base, données sur les antécédents et données d'image qui leur sont nécessaires à l'accomplissement de leurs tâches légales, à l'exception des données classifiées issues des contacts directs avec les autorités de sécurité étrangères.

3 Les agents de la PJF et du SFS peuvent être autorisés sur demande à consulter ponctuellement les données de la banque ST.

4 D'autres organes de police et de poursuite pénale de la Confédération peuvent avoir accès à la banque ST au moyen d'une procédure d'appel pour consulter les données nécessaires à l'accomplissement de leurs tâches légales.

5 Les agents du service fédéral chargé des contrôles de sécurité relatifs aux personnes peuvent se voir attribuer, en vue de l'accomplissement de leurs tâches légales, l'autorisation de consulter ponctuellement les données de la banque ST.

Section 3 Traitement des données

Art. 10 Saisie des données et contrôle de qualité

1 Seules peuvent être traitées dans ISIS des informations qui répondent aux buts définis à l'art. 2.

2 La Section Analyse préliminaire du SAP introduit les données dans ISIS, détermine la catégorie d'antécédents et fixe la durée de conservation.

3 Les données destinées aux banques ST et VP sont, dans un premier temps, saisies provisoirement (code «p»). Leur fiabilité est appréciée en fonction de la provenance, du mode de transmission, du contenu et des informations déjà disponibles (code «g»

5 Le texte des annexes 1 et 2 de l'ordonnance du 30 novembre 2001 sur le système de traitement des données relatives à la protection de l'Etat n'est publié ni au Recueil officiel ni au Recueil systématique. Des tirés à part peuvent être obtenus auprès de l'OCFIM, 3003 Berne.

pour les données fiables sur les antécédents et code «u» pour celles qui sont peu fiables).

4 Le service d'Assurance qualité ISIS du SAP (Assurance qualité) vérifie les saisies provisoires, notamment l'indication des sources, l'appréciation de la fiabilité, la date de la prochaine appréciation générale et la durée de conservation; enfin, il confirme l'enregistrement définitif des données (code «k» pour les données contrôlées).

5 Le chef du SAP ou l'un de ses remplaçants peuvent charger l'Assurance qualité d'apprécier le contenu des autres banques de données.

Art. 11 Gestion électronique des documents

1 Il est possible de renoncer au classement-papier des dossiers dans la mesure où les informations à l'origine des données de base et des données sur les antécédents sont saisies comme données d'image dans la gestion électronique des dossiers.

2 La gestion électronique des dossiers doit garantir leur gestion et leur archivage conformément aux instructions.

Art. 12 Consultation des banques de données

1 Les données peuvent être consultées suivant les critères ci-après: indications principales sur la personne, données de base, données sur les antécédents, ou données de base et données sur les antécédents. Les données d'image ne peuvent pas être appelées séparément.

2 La consultation des données sur les antécédents n'est possible que dans une seule banque de données à la fois.

3 Les agents du SAP spécialement formés peuvent procéder à des appréciations dans le cadre de leur domaine d'activité.

Art. 13 Communication de données

1 Dans des cas déterminés, le SAP peut communiquer des données personnelles traitées dans ISIS, à l'exception des données contenues dans les banques DEWA et DEBBWA et des données prélevées dans le cadre de contrôles de sécurité relatifs aux personnes:

a. aux autorités pénales cantonales, aux fins de prévenir et de poursuivre les actes punissables;

b. au Département fédéral des affaires étrangères, pour l'appréciation des demandes d'accréditation et du droit de séjourner en Suisse de ressortissants d'Etats étrangers ou de membres d'organisations internationales, en vue du respect des engagements de protection découlant du droit international public ainsi que dans le cadre du droit de coopérer du DFAE dans le domaine de la législation régissant les échanges extérieurs;

c. aux autres unités administratives de l'Office fédéral de la police:

   1. pour soutenir les enquêtes de police judiciaire, ainsi que dans le cadre de recherches préliminaires utiles à l'établissement de faits dans le do-

maine de la lutte contre le crime organisé et le trafic illicite des stupéfiants;

2. dans le cadre de l'entraide administrative internationale liée à des affaires pénales (INTERPOL);
3. pour inscrire des informations dans le système de recherches informatisées de police RIPOL;
4. pour apprécier les risques sur le plan sécuritaire lors de la mise en œuvre de mesures de protection en faveur de personnes ou de bâtiments.

d. à l'Office fédéral de la justice, pour compléter ou exécuter une requête d'entraide judiciaire en matière pénale;

e. à l'Office fédéral des étrangers, pour l'application de mesures contre des étrangers, notamment en vue de leur éloignement, ainsi que pour traiter des demandes de naturalisation;

f. à l'Office fédéral des réfugiés, pour apprécier des demandes d'asile;

g. au Département fédéral de la défense, de la protection de la population et des sports, pour l'exercice de son droit de coopérer dans le domaine de la législation régissant les échanges extérieurs;

h. au Service de sécurité militaire pour:

1. apprécier la situation militaire en matière de sécurité,
2. protéger des informations et des ouvrages militaires,
3. exécuter, dans le domaine de l'armée, des tâches en matière de police criminelle et de police de sécurité,

et, lorsque les membres du service sont mis sur pied pour un service actif, pour:

4. garantir la sécurité préventive de l'armée à l'égard de l'espionnage, du sabotage et d'autres activités illicites,
5. rechercher des renseignements,
6. veiller à la protection de personnes occupant des postes de représentants de l'Etat;

i. au Service de renseignements du Département fédéral de la défense, de la protection de la population et des sports, dans le contexte d'informations importantes pour la politique de sécurité;

j. à la justice militaire, pour l'exécution de tâches de police judiciaire et de police de sécurité;

k. aux organes des gardes-frontière et de la douane, pour localiser des personnes, opérer des contrôles douaniers et effectuer des enquêtes pénales administratives;

l. au Secrétariat d'Etat à l'économie, pour l'application de la loi fédérale du 13 décembre 1996 sur le matériel de guerre[6], et pour l'exécution de mesures dans le domaine de la législation régissant les échanges extérieurs;

6 RS **514.51**

m. à l'Office fédéral de la formation professionnelle et de la technologie, pour l'octroi de permis d'emploi de substances explosibles;

n. à l'Office fédéral de l'aviation civile et à La Poste Suisse, pour l'exécution des mesures en matière de police de sécurité;

o. à l'Office fédéral de l'énergie, pour l'application de la loi du 23 décembre 1959 sur l'énergie atomique[7] et pour l'exercice de son droit de coopérer dans le domaine de la législation régissant les échanges extérieurs;

p. aux services compétents de la Confédération et des cantons, pour procéder à des contrôles de sécurité relatifs aux personnes;

q. aux organes administratifs concernés, pour assurer leur sécurité;

r. à des organes administratifs et à des particuliers, pour leur permettre de motiver une demande de renseignements;

s. à des particuliers, pour écarter un danger considérable.

2 Pour la communication à l'étranger, sont applicables les art. 17, al. 3 à 5, et 7 LMSI.

3 La communication de données n'est pas autorisée lorsque des intérêts prépondérants publics ou privés s'y opposent.

4 Lors de toute communication, le destinataire doit être renseigné sur la fiabilité et l'actualité des données (art. 10). Il ne peut utiliser les données que dans le but pour lequel elles lui ont été transmises. Il doit être rendu attentif aux restrictions d'emploi et au fait que l'autorité qui communique les données se réserve le droit de se renseigner sur l'utilisation qui en aura été faite.

5 La communication, ainsi que ses destinataires, son objet et ses motifs, doivent être enregistrés.

6 La communication des données issues des banques DEWA et DEBBWA est régie par l'art. 43 de l'ordonnance du 21 septembre 1998 sur les armes, les accessoires d'armes et les munitions (OArm)[8].

Art. 14 Copie de données

1 Les données d'ISIS ne peuvent être reportées dans d'autres fichiers ni par le biais d'installations de communication ni au moyen de supports de données. L'archivage électronique des données d'ISIS aux Archives fédérales n'est pas soumis à la présente disposition.

2 Des données d'ISIS peuvent être passagèrement transférées dans des banques de données de travail aux fins de travaux d'exploitation particuliers. Ceux-ci terminés, les données doivent être effacées.

7 RS **732.0**
8 RS **514.541**

Art. 15 Droit d'être renseigné

1 Le droit d'être renseigné est régi par l'art. 18 LMSI.

2 Le droit d'être renseigné sur les banques de données DEWA et DEBBWA est régi par les art. 8 et 9 de la loi fédérale du 19 juin 1992 sur la protection des données[9].

Art. 16 Appréciation générale périodique des données de la banque ST

1 L'Assurance qualité procède à une appréciation générale de chaque bloc de données (données de base et données sur les antécédents) au plus tard cinq ans après la saisie de la première donnée ou trois ans après la dernière appréciation générale.

2 Elle vérifie, à la lumière des dangers et risques qui menacent la sécurité du pays, si les antécédents enregistrés dans un bloc présentent un degré de vraisemblance élevé s'agissant du risque pour la sûreté intérieure, en vue d'une appréciation administrative, et si les données sont nécessaires pour d'autres tâches de protection de l'Etat.

3 Les données sur les antécédents d'une personne qui figurent dans la banque de données depuis plus de trois ans, avec l'appréciation «peu fiables», ne peuvent continuer d'être traitées comme telles (code «u») jusqu'à la prochaine appréciation générale que si elles sont nécessaires à l'accomplissement de tâches légales et si le chef du SAP ou l'un de ses remplaçants en a autorisé le traitement.

4 Les informations concernant des tiers qui sont enregistrées depuis plus de trois ans sans titre propre («Stamm»), sont rendues anonymes lors de l'appréciation générale.

5 L'Assurance qualité efface les données devenues inutiles. En cas de traitement ultérieur de données encore nécessaires, la date de la dernière appréciation générale doit être enregistrée.

Art. 17 Durée de conservation des données

1 Les données de police préventive peuvent être mémorisées dans ISIS pendant une durée maximum de quinze ans.

2 Pour les données ci-après, la durée de conservation maximale est la suivante:

a. 20 ans pour les données relatives à des programmes de recherches de police préventive en cours;

b. dix ans au plus pour les données relatives à des interdictions d'entrée, à compter de leur expiration;

c. cinq ans pour les données recueillies dans le cadre de procédures de contrôles de sécurité relatifs aux personnes;

d. 30 et 10 ans respectivement pour les données relevant de la correspondance avec des organes administratifs et des particuliers.

3 Les données des banques DO, STRALAG et INFOPRESS peuvent être conservées pendant une durée illimitée.

9 RS **235.1**

4 La conservation des données dans les banques DEWA et DEBBWA est régie par l'art. 45 OArm[10].

Art. 18 Effacement des données

1 A l'expiration de leur durée de conservation, les données sur les antécédents sont effacées dans un délai de trois mois, à moins que le chef du SAP ou l'un de ses remplaçants ne décide, à la lumière des dangers et risques existants, qu'elles sont indispensables à l'accomplissement de tâches légales.

2 Dans les cas visés à l'al. 1, la durée de conservation ultérieure des données s'élève à trois ans. Elle ne peut être prolongée qu'une fois.

3 Tout le bloc de données (données de base et données sur les antécédents) doit être supprimé avec l'effacement du dernier fait.

Art. 19 Communication de l'effacement aux cantons

Lorsque des données ISIS qui provenaient d'organes cantonaux chargés de tâches de sécurité sont effacées, l'Assurance qualité doit en informer ces derniers afin qu'ils détruisent les données et documents tenus parallèlement.

Art. 20 Obligation de proposer les documents aux Archives fédérales

1 Les données et les documents devenus inutiles ou destinés à être effacés sont proposés aux Archives fédérales aux fins d'archivage.

2 Les données classifiées émanant des relations avec les autorités de sécurité étrangères ne sont pas proposées aux fins d'archivage.

3 Les documents que les Archives fédérales jugent sans valeur archivistique sont détruits. Les autres dispositions légales en matière de destruction de données sont réservées.

4 Avant la remise des documents d'un dossier personnel aux Archives fédérales, le SAP introduit dans la banque de données VE la date de livraison, le numéro d'enregistrement, ainsi que les données établissant l'identité de la personne concernée; ces informations sont conservées pendant dix ans, puis effacées.

Section 4 Dispositions relatives à l'organisation

Art. 21 Sécurité des données et journalisation

1 Pour assurer la sécurité des données, sont applicables l'art. 20 de l'ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données[11] et le chap. 3 de l'ordonnance du 23 février 2000 sur l'informatique et la télécommunication dans l'administration fédérale.[12]

10 RS **514.541**
11 RS **235.11**
12 RS **172.010.58**

2 Le SAP précise dans un règlement ISIS les mesures organisationnelles et techniques contre le traitement non autorisé des données et les modalités de la journalisation automatique des données.

3 Les données ISIS ne peuvent être transmises que sous forme chiffrée durant toute l'opération de transmission.

Art. 22 Responsabilités et compétences

1 Le SAP assume la responsabilité d'ISIS. Il en édicte le règlement.

2 L'Assurance qualité veille à ce que les utilisateurs se conforment à la présente ordonnance, à ses annexes et au règlement ISIS.

3 Le Centre de service informatique du département veille à l'exploitation et à la sécurité d'ISIS.

4 Le conseiller à la protection des données de l'Office fédéral de la police peut vérifier au cas par cas que le traitement de données dans ISIS se fait bien conformément aux dispositions relatives à la protection des données.

Art. 23 Financement

1 La Confédération finance le transport des données jusqu'aux centraux de raccordement des cantons.

2 Les cantons prennent en charge:

a. les frais d'acquisition et de maintenance de leurs appareils;

b. les frais d'installation et d'exploitation de leur réseau de distribution.

Art. 24 Exigences techniques

1 Le département détermine les exigences techniques auxquelles doivent satisfaire les terminaux des cantons.

2 Les détails sont fixés dans le règlement ISIS.

Section 5 Dispositions finales

Art. 25 Abrogation du droit en vigueur

L'ordonnance du 1er décembre 1999 sur le système de traitement des données relatives à la protection de l'Etat[13] est abrogée.

13 RO **1999** 3461, **2000** 1227 et 2027

Art. 26 Dispositions transitoires

[1] Les données issues des procédures d'enquêtes de police judiciaire de la Confédération qui ont été saisies dans ISIS sont transférées dans la banque de données JANUS de la PJF.

[2] Le SAP vérifie au préalable quelles sont les données issues de procédures d'enquêtes de police judiciaire de la Confédération qui doivent continuer d'être traitées dans ISIS pour servir dans le cadre des activités de police préventive. Les autres données sont effacées après le transfert décrit à l'al. 1.

Art. 27 Entrée en vigueur

La présente ordonnance entre en vigueur le 1er janvier 2002.

30 novembre 2001 Au nom du Conseil fédéral suisse:

Le président de la Confédération, Moritz Leuenberger
La chancelière de la Confédération, Annemarie Huber-Hotz