Ordonnance sur les systèmes d'information du Service de renseignement de la Confédération (OSI-SRC)

du 4 décembre 2009

Le Conseil fédéral suisse,

vu l'art. 5, al. 1 et 4, de la loi fédérale du 3 octobre 2008 sur le renseignement civil (LFRC)[1],
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)[2],
vu l'art. 17*a* de la loi fédérale du 19 juin 1992 sur la protection des données[3],

arrête:

Section 1 Objet et définitions

Art. 1 Objet

La présente ordonnance règle l'exploitation, le contenu des données et l'utilisation des systèmes d'information du Service de renseignement de la Confédération (SRC) suivants:

a. Système d'information sécurité extérieure (ISAS);

b. Système d'information sécurité intérieure (ISIS).

Art. 2 Définitions

Dans la présente ordonnance, on entend par:

a. données: les informations mémorisées dans les systèmes d'information du SRC;

b. objet: le regroupement de données se rapportant à une ou plusieurs personnes, organisations, faits ou événements;

c. communication: toute nouvelle information relative à un ou plusieurs objets;

d. relation: le lien entre un objet et une communication;

e. bloc de données: l'ensemble des communications et des relations relatives à un objet;

RS **121.2**

1 RS **121**
2 RS **120**
3 RS **235.1**

f. données OCR: les documents saisis de telle manière qu'une recherche plein texte est possible;

g. données d'image: les documents saisis sous forme d'image;

h. consultation brève: une consultation en ligne limitée pour déterminer si une personne figure dans un système d'information du SRC;

i. tiers: une personne ou une organisation revêtant une importance du point de vue de la protection de l'Etat de par son lien avec un objet;

j. feuille d'information: les appréciations périodiques standardisées de l'analyse stratégique relative à un objet.

Section 2
Dispositions générales concernant les systèmes d'information du SRC

Art. 3 But des systèmes d'information du SRC

1 Les systèmes d'information du SRC ont pour but de faciliter l'accomplissement des tâches qui incombent à ce dernier en vertu de l'art. 1 LFRC.

2 Ils sont utilisés pour:

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

b. l'élaboration de rapports de situation;

c. l'exécution de travaux administratifs;

d. le classement et la gestion de dossiers;

e. l'exécution de travaux de documentation;

f. la gestion des affaires.

Art. 4 Droits de consultation

1 Les utilisateurs des systèmes d'information du SRC ont accès aux données nécessaires à l'accomplissement de leurs tâches légales.

2 Le Département fédéral de la défense, de la protection de la population et des sports (DDPS) règle les droits de consultation.

3 Le directeur du SRC ou son suppléant rend une décision sur les demandes individuelles.

4 La Gestion de l'information du SRC est chargée de la mise en œuvre des droits de consultation.

Art. 5 Consultation et représentation visuelle des données

1 Les utilisateurs des systèmes d'information du SRC peuvent consulter les données selon les critères suivants: objets, relations, communications, activités et plein texte.

2 Les objets et leurs relations peuvent être représentés visuellement et les représentations peuvent être enregistrées.

Art. 6 Outil informatisé d'analyse et d'appréciation

Les utilisateurs des systèmes d'information du SRC peuvent, dans les limites de leur droit d'accès, consulter simultanément tous les systèmes d'information du SRC au moyen d'outils informatisés d'analyse et d'appréciation.

Art. 7 SILAN

1 SILAN est un système de communication chiffré au sein du SRC traitant les données classifiées «secret».

2 Le SRC ne met ce système qu'à la disposition des utilisateurs du SRC.

Art. 8 Intranet du SRC

1 L'Intranet du SRC est un système de communication chiffré traitant les données classifiées «confidentiel».

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

Art. 9 Documentation générale

1 Le SRC gère dans ses systèmes d'information une documentation provenant de sources d'information accessibles au public contenant:

a. des informations sur des personnes, des organisations et des faits relevant de la LFRC;

b. des informations sur des personnes et des organisations dont la sécurité pourrait être menacée en Suisse;

c. des informations sur des pays et sur des contextes sociaux et politiques pouvant influer sur l'appréciation de la situation;

d. des informations scientifiques et techniques relevant du domaine d'activité des autorités de sécurité.

2 Il exploite un portail personnalisé permettant d'utiliser des sources d'information accessibles au public (Portail interactif pour Open Sources; IPOS).

3 Il gère un service de documentation sur le matériel propageant le racisme ou la violence. Ce service appuie les procédures pénales ou administratives qui traitent de cas impliquant ce genre de matériel.

Art. 10 Communication de données personnelles

1 Le SRC peut communiquer les données personnelles traitées dans ses systèmes d'information aux autorités et organes officiels aux fins et aux conditions définies dans l'annexe 3 de l'ordonnance du 4 décembre 2009 sur le Service de renseignement de la Confédération (OSRC)[4].

2 Pour la communication à l'étranger, sont applicables:

a. pour les informations concernant l'étranger: les art. 5, al. 3, LFRC, et 14 OSRC;

b. pour les informations concernant la Suisse: l'art. 17, al. 3 à 5, 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 SRC renseigne le destinataire sur la fiabilité et l'actualité des données.

5 Il signale au destinataire:

a. qu'il ne peut utiliser les données que dans le but pour lequel elles lui ont été transmises, et

b. que le SRC se réserve le droit de se renseigner sur l'utilisation qui en aura été faite.

6 Il enregistre la communication de données ISIS, ainsi que le destinataire, l'objet et les motifs de la communication.

Art. 11 Copie de données

1 Les données des systèmes d'information du SRC ne peuvent être copiées dans d'autres fichiers ni par le biais d'installations de communication ni au moyen de supports de données.

2 Des données des systèmes d'information du SRC peuvent être temporairement transférées dans des banques de données de travail aux fins de travaux d'analyse particuliers. Ceux-ci terminés, les données doivent être détruites.

Art. 12 Destruction de données

1 A l'expiration de leur durée de conservation, les données sont détruites dans un délai de trois mois, conformément aux art. 24 et 33.

2 Le directeur du SRC ou son suppléant peut prolonger de trois ans la durée de conservation des données qu'il juge, à la lumière des dangers et des risques existants, indispensables à l'accomplissement des tâches légales du SRC. La durée de conservation ne peut être prolongée qu'une fois.

3 Tout le bloc de données ainsi que toute feuille d'information éventuelle sont détruits avec la suppression de la dernière communication (y compris les relations, données d'image et mandats correspondants).

4 RS **121.1**

4 Les données destinées à être détruites, à l'exception des informations définies à l'art. 13, al. 2, de la présente ordonnance, sont transférées dans le module d'archivage.

Art. 13 Archivage

1 Le SRC propose les données et les dossiers devenus inutiles ou destinés à être détruits aux Archives fédérales aux fins d'archivage.

2 Il ne propose pas d'archiver les documents classifiés (données et dossiers) émanant des relations avec les autorités de sécurité étrangères et de la recherche opérative. Il les conserve en interne, d'entente avec les Archives fédérales, et les détruit après 45 ans.

3 Il détruit les données du module d'archivage et les dossiers correspondants que les Archives fédérales jugent sans valeur archivistique. Les autres dispositions légales en matière de destruction de données sont réservées.

Art. 14 Sécurité des données et journalisation

1 Pour assurer la sécurité des données, sont applicables:

a. l'art. 20 de l'ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données[5];

b. l'ordonnance du 26 septembre 2003 sur l'informatique et la télécommunication dans l'administration fédérale[6];

c. les conditions fixées par le DDPS selon l'art. 28 de la présente ordonnance pour le raccordement des organes cantonaux chargés du maintien de la sécurité intérieure.

2 Le SRC précise dans un règlement de traitement:

a. les mesures organisationnelles et techniques contre le traitement non autorisé des données;

b. 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. 15 Responsabilités et compétences

1 Le SRC assume la responsabilité de ses systèmes d'information.

2 Il édicte les règlements de traitement.

3 La Gestion de l'information du SRC est chargée de la formation et de l'assistance aux utilisateurs et veille à la mise en œuvre des règlements de traitement.

5 RS **235.11**
6 RS **172.010.58**

4 La responsabilité technique intégrale des systèmes d'information du SRC incombe au DDPS.

5 Le prestataire de services TED veille à l'exploitation, à l'entretien et à la sécurité.

6 Les conseillers à la protection des données du SRC peuvent vérifier au cas par cas que le traitement des données dans ses systèmes d'information est bien conforme aux dispositions relatives à la protection des données.

Art. 16 Exigences techniques

1 Le DDPS détermine les exigences techniques auxquelles doivent satisfaire les terminaux des utilisateurs.

2 Les règlements de traitement déterminent les particularités pour chaque système d'information.

Section 3 Système d'information sécurité extérieure (ISAS)

Art. 17 Phase d'essai d'ISAS

1 ISAS est exploité dans le cadre d'un essai pilote de durée déterminée au sens de l'art. 17*a* de la loi fédérale du 19 juin 1992 sur la protection des données[7].

2 Le SRC présente, dans les deux ans qui suivent la mise en exploitation d'ISAS, un rapport d'évaluation au Conseil fédéral.

3 Le Conseil fédéral décide de la fin de l'essai pilote d'ISAS et du début de son exploitation régulière.

4 Les dispositions des sections 1 et 2 (art. 1 à 16) sont applicables dans le cadre de l'essai pilote d'ISAS.

Art. 18 Banques de données

1 ISAS se compose des banques de données suivantes:

a. Données brutes (RD);
b. Extrémisme (EX);
c. Terrorisme (TE);
d. Non-prolifération (NP);
e. Service de renseignement (ND);
f. Affaires militaires (MI);
g. Economie et ressources (WR);
h. Politique internationale et stratégie (IPS);
i. Documentation (DO).

7 RS **235.1**

2 Les banques de données contiennent les informations ci-après, relatives à l'étranger et revêtant une importance pour l'accomplissement des tâches du SRC définies à l'art. 1 LFRC:

a. RD: données OCR non structurées ou semi-structurées pouvant être traitées dans le cadre des EX, TE, NP, ND, MI, WR, IPS et DO;

b. EX: informations sous forme structurée relatives aux personnes et aux événements relevant du domaine de l'extrémisme violent;

c. TE: informations sous forme structurée relatives aux personnes et aux événements relevant du domaine du terrorisme;

d. NP: informations sous forme structurée relatives aux personnes et aux événements relevant du domaine de la non-prolifération; les informations peuvent aussi contenir des données relatives à la Suisse;

e. ND: informations sous forme structurée relatives aux personnes et aux événements relevant du domaine des activités liées au renseignement prohibé;

f. MI: informations sous forme structurée relatives aux personnes, aux événements et aux faits relevant du domaine des affaires militaires;

g. WR: informations sous forme structurée relatives aux personnes et aux événements relevant du domaine de l'économie et des ressources;

h. IPS: informations sous forme structurée relatives aux personnes et aux événements relevant du domaine de la politique internationale et de la stratégie;

i. DO: informations documentaires relatives aux personnes et aux événements, tirées des activités préventives déployées dans le domaine de la protection de l'Etat et des informations tirées de sources d'information accessibles au public, conformément à l'art. 9.

Art. 19 Données traitées

1 Les banques de données d'ISAS EX, TE, NP, ND, MI, WR, IPS et DO sont structurées selon les critères suivants: communications, objets et relations.

2 Les différents champs de données sont réglés par le DDPS.

Art. 20 Droits de consultation

Les collaborateurs du SRC chargés de mener à bien l'essai pilote d'ISAS ont accès à ISAS pour consulter les données nécessaires à l'accomplissement de leurs tâches légales.

Art. 21 Saisie des données et contrôle de qualité

1 Seules peuvent être traitées dans ISAS des informations qui répondent aux buts définis à l'art. 3.

2 L'Analyse préliminaire du SRC introduit les données dans ISAS.

3 Peuvent également introduire les données dans les banques ci-après et déterminer les catégories des communications les personnes suivantes:

a. les collaborateurs du ComCenter du SRC: données dans la banque RD;

b. les collaborateurs de la section Analyse du SRC: données dans les banques EX, TE, NP, ND, MI, WR, IPS et DO.

4 Le directeur du SRC, ou son suppléant, peut charger la section Assurance qualité ISIS d'apprécier le contenu des banques de données d'ISAS.

Art. 22 Classement des dossiers

1 Le classement des dossiers doit garantir leur gestion et leur archivage, conformément aux instructions.

2 Les informations à l'origine des objets et des communications peuvent être saisies comme données OCR.

3 Il est possible de renoncer au classement-papier des dossiers dans la mesure où les informations à l'origine des objets et des communications sont saisies comme données OCR.

Art. 23 Droit d'être renseigné

Le droit d'être renseigné est régi par les dispositions de la loi fédérale du 19 juin 1992 sur la protection des données[8].

Art. 24 Durée de conservation des données

1 Les données et les dossiers apparentés peuvent être mémorisés dans ISAS pendant une durée maximale de 30 ans à compter de la date de leur dernier traitement.

2 La durée de conservation maximale est de 45 ans.

Section 4 Système d'information sécurité intérieure (ISIS)

Art. 25 Systèmes et banques de données

1 ISIS se compose des systèmes et banques de données suivants:

a. «ISIS00 Général» avec classement des dossiers, gestion des mandats, analyse des risques, statistique et module d'archivage;

b. «ISIS01 Protection de l'Etat» avec les banques de données:
   1. «Protection de l'Etat»,
   2. «Police administrative»,
   3. «Documentation»,
   4. «Système numérique»;

8 RS **235.1**

c. «ISIS02 Administration» avec la banque de données «Administration»;

d. «ISIS05 News» avec les banques de données:
   1. «NEWS»,
   2. «ELIS»,
   3. «IPIS»,
   4. «Infopress»,
   5. «ISIS-Info»;

e. «ISIS06 Contrôles de sécurité relatifs aux personnes» avec la banque de données «Contrôles de sécurité relatifs aux personnes»;

f. «ISIS07 Politique de sécurité» avec la banque de données «Politique de sécurité».

2 Les banques de données contiennent les informations ci-après, relatives à la sécurité intérieure et revêtant une importance pour l'accomplissement des tâches du SRC, conformément à l'art. 1 LFRC:

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 de l'Office fédéral de la police (fedpol);

c. «Documentation» (DO): informations documentaires, tirées des activités préventives déployées dans le domaine de la protection de l'Etat et des informations tirées de sources d'information accessibles au public, conformément à l'art. 9;

d. «Système numérique» (NU): informations relatives aux événements, tirées de programmes choisis de recherches;

e. «Administration» (VE): informations nécessaires au contrôle des affaires;

f. «NEWS»: communiqués de presse relevant de la protection de l'Etat, tirés d'Internet;

g. «ELIS»: représentation électronique de la situation en matière de sécurité intérieure;

h. «IPIS»: communiqués des agences de presse relevant de la protection de l'Etat;

i. «Infopress»: revue de presse quotidienne établie par le SRC;

j. «ISIS-Info»: plate-forme d'information destinée aux utilisateurs d'ISIS;

k. «Contrôles de sécurité relatifs aux personnes» (PSP): informations nécessaires au contrôle des affaires dans le domaine des contrôles de sécurité relatifs aux personnes;

l. «ISIS07 Politique de sécurité» (SIPOL): informations revêtant une importance pour la politique de sécurité relatives aux affaires militaires, à l'économie, aux ressources, à la politique internationale et à la stratégie.

Art. 26 Données traitées

1 Les données enregistrées dans les banques de données ISIS sont classées en catégories en fonction des domaines spécialisés, dans la mesure où cette classification est judicieuse pour la gestion des accès.

2 Les banques de données d'ISIS sont structurées selon les critères suivants: communications, objets et relations.

3 Les différents champs de données sont réglés par le DDPS.

Art. 27 Droits de consultation

1 Les autorités et organes officiels ci-après ont accès à ISIS pour consulter les données nécessaires à l'accomplissement de leurs tâches légales:

a. les collaborateurs du SRC et ceux des organes cantonaux chargés du maintien de la sécurité intérieure; ils accèdent au système en ligne;

b. les collaborateurs du Service fédéral de sécurité (SFS), de la Police judiciaire fédérale (PJF), de la Coopération policière opérationnelle, de la Centrale d'engagement et du service compétent pour décider de mesures d'éloignement à l'encontre d'étrangers, conformément aux art. 67, al. 2, et 68 de la loi fédérale du 16 décembre 2005 sur les étrangers[9]; ils peuvent effectuer des consultations ponctuelles en ligne;

c. les collaborateurs du service fédéral chargé des contrôles de sécurité relatifs aux personnes; ils peuvent effectuer des consultations ponctuelles en ligne.

2 Les organes cantonaux chargés du maintien de la sécurité intérieure ne peuvent pas consulter les données classifiées issues des contacts directs avec les autorités de sécurité étrangères.

Art. 28 Exigences techniques pour le raccordement des cantons

1 Le DDPS détermine les exigences techniques auxquelles les organes cantonaux chargés du maintien de la sécurité intérieure doivent satisfaire pour être raccordés au système.

2 Les organes cantonaux ne peuvent se raccorder à ISIS qu'après avoir satisfait aux exigences techniques.

9 RS **142.20**

Art. 29 Saisie des données et contrôle de qualité

1 Seules peuvent être traitées dans ISIS des informations qui répondent aux buts définis à l'art. 3.

2 L'Analyse préliminaire du SRC introduit les données dans ISIS et détermine la catégorie des communications.

3 Peuvent également introduire les données ci-après et déterminer les catégories des communications les personnes suivantes:

a. les collaborateurs du Service des étrangers du SRC: données issues du contrôle des photos d'identité;

b. les collaborateurs de la section Analyse du SRC: feuilles d'information;

c. les collaborateurs du domaine Contrôles de sécurité relatifs aux personnes: données issues de la banque de données PSP.

4 Les données destinées aux banques de données ST 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 de la manière suivante:

a. avec le code «g» pour les communications fiables;

b. avec le code «u» pour les communications qui ne sont pas fiables.

5 L'Assurance qualité ISIS vérifie les saisies provisoires, notamment l'indication des sources, l'appréciation de la fiabilité et la date de la prochaine appréciation globale; enfin, elle confirme l'enregistrement définitif des données (code «k»).

6 Le directeur du SRC, ou son suppléant, peut charger la section Assurance qualité ISIS d'apprécier le contenu des autres banques de données.

Art. 30 Classement des dossiers

1 Le classement des dossiers doit garantir leur gestion et leur archivage, conformément aux instructions.

2 Les informations à l'origine des objets et des communications peuvent être saisies comme données OCR, sauf dans les banques de données ST et PSP, où elles sont uniquement saisies comme données d'image.

3 Il est possible de renoncer au classement-papier des dossiers dans la mesure où les informations à l'origine des objets et des communications sont saisies comme données d'image.

Art. 31 Droit d'être renseigné

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

Art. 32 Appréciation générale périodique des données de la banque ST

1 L'Assurance qualité ISIS procède à une appréciation générale de chaque bloc de données au plus tard cinq ans après la saisie de la première communication et trois ans après la dernière appréciation générale.

2 Elle vérifie, à la lumière des dangers et des risques existants, si les communications et les objets saisis dans un bloc de données présentent un degré de vraisemblance élevé s'agissant du risque pour la sécurité intérieure et si les données sont nécessaires pour d'autres tâches de protection de l'Etat.

3 Les communications et les relations 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:

a. si elles sont nécessaires à l'accomplissement de tâches légales, et

b. si le directeur du SRC ou son suppléant en a autorisé le traitement.

4 En cas de traitement ultérieur de données encore nécessaires, la date de la dernière appréciation générale doit être enregistrée.

5 Les objets identifiés depuis plus de trois ans comme des données relatives à des tiers sont effacés lors de l'appréciation générale.

6 La section Assurance qualité ISIS efface les données devenues inutiles.

Art. 33 Durée de conservation des données

1 Pour les données ci-après enregistrées dans ISIS, la durée de conservation maximale est la suivante:

a. 15 ans pour les données préventives;

b. 20 ans pour les données relatives à des programmes de recherches préventives en cours;

c. 10 ans pour les données relatives aux interdictions d'entrée, à compter de leur expiration;

d. 5 ans pour les données recueillies dans le cadre des contrôles de sécurité relatifs aux personnes;

e. 30 ans pour les données relevant de la correspondance avec des organes administratifs;

f. 10 ans pour les données relevant de la correspondance avec des particuliers;

g. 45 ans pour les données des banques DO, NEWS, IPIS, Infopress et ISIS-Info.

2 A l'expiration de leur durée de conservation, les données et les dossiers doivent être détruits.

Art. 34 Données et dossiers des organes cantonaux chargés du maintien de la sécurité intérieure

[1] Les organes cantonaux chargés du maintien de la sécurité intérieure peuvent conserver cinq ans au plus les données et les dossiers établis dans le cadre des tâches de protection de l'Etat qu'ils effectuent pour la Confédération.

[2] A l'expiration de leur durée de conservation, les données et les dossiers doivent être détruits.

Art. 35 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.

Section 5 Dispositions finales

Art. 36 Abrogation du droit en vigueur

L'ordonnance ISIS du 30 novembre 2001[10] est abrogée.

Art. 37 Entrée en vigueur et durée de validité

[1] La présente ordonnance entre en vigueur le 1er janvier 2010.

[2] La durée de validité des dispositions de la section 3 (art. 17 à 24) est limitée au 31 décembre 2014.

4 décembre 2009

Au nom du Conseil fédéral suisse:

Le président de la Confédération, Hans-Rudolf Merz
La chancelière de la Confédération, Corina Casanova

10 RO **2001** 3173, **2004** 3495 4813, **2006** 921, **2008** 4943 5525 6305