

Ordonnance sur les mesures de police administrative et les systèmes d'information de l'Office fédéral de la police

du 4 décembre 2009

Le Conseil fédéral suisse,

vu les art. 5, al. 2, 11, al. 1, 15, al. 3 et 5, 24a, al. 7 et 8, 26, al. 3, et 30 de la loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sécurité intérieure (LMSI)¹,

vu les art. 31c, 32a et 32b de la loi du 20 juin 1997 sur les armes (LArm)²,
arrête:

Section 1 Dispositions générales

Art. 1 Objet

La présente ordonnance règle:

- a. l'exécution de mesures de police administrative par l'Office fédéral de la police (fedpol) sur la base de la LMSI;
- b. le système d'information HOOGAN de fedpol;
- c. les banques de données de l'Office central des armes et de l'Office central pour les explosifs et la pyrotechnie au sein de fedpol.

Art. 2 Collaboration scientifique et technique

¹ Fedpol peut collaborer avec des organes scientifiques et techniques, notamment avec le Service scientifique et de recherches de la ville de Zurich (WFD). La collaboration est réglée par contrat.

² Les dispositions du droit fédéral relatives à la protection des données s'appliquent aux mandats attribués à des organes scientifiques et techniques. Les organes mandatés sont tenus au secret de fonction.

RS 120.52

¹ RS 120

² RS 514.54

Section 2

Mesures de police administrative relatives au matériel de propagande

Art. 3

¹ Fedpol décide du séquestre et de la confiscation de matériel de propagande au sens de l'art. 13a LMSI après avoir consulté le Service de renseignement de la Confédération (SRC).

² L'autorité qui effectue la saisie transmet immédiatement le matériel de propagande au SRC et lui indique les circonstances de la saisie, de même que les personnes et les entreprises impliquées.

³ Fedpol confisque le matériel de propagande si l'appel à la violence est concret et sérieux.

⁴ Fedpol détruit le matériel confisqué dans la mesure où celui-ci ne peut être utilisé à des fins d'instruction.

Section 3

Mesures de police administrative contre la violence lors de manifestations sportives

Art. 4 Comportement violent

¹ Il y a notamment comportement violent lorsqu'une personne a commis ou incité à commettre une des infractions suivantes:

- a. les infractions contre la vie et l'intégrité corporelle visées aux art. 111 à 113, 117, 122, 123, 125, al. 2, 129, 133 et 134, du code pénal (CP)³;
- b. les dommages à la propriété visés à l'art. 144 CP;
- c. la contrainte visée à l'art. 181 CP;
- d. l'incendie intentionnel visé à l'art. 221 CP;
- e. l'explosion visée à l'art. 223 CP;
- f. la provocation publique au crime ou à la violence visée à l'art. 259 CP;
- g. l'émeute visée à l'art. 260 CP;
- h. la violence ou la menace contre les autorités et les fonctionnaires visée à l'art. 285 CP.

² Est aussi considéré comme comportement violent le fait de menacer la sécurité publique en transportant ou en utilisant des armes, des explosifs, de la poudre de guerre ou des engins pyrotechniques sur les lieux de manifestations sportives, dans leurs environs ainsi que lors des déplacements en direction ou en provenance de ces lieux.

³ RS 311.0

Art. 5 Preuve du comportement violent

¹ Sont considérés comme preuve d'un comportement violent:

- a. les décisions judiciaires ou les dénonciations policières allant dans ce sens;
- b. les témoignages crédibles ou les prises de vue de la police, de l'administration des douanes, du personnel de sécurité ou des fédérations et associations sportives;
- c. les interdictions de stade prononcées par les fédérations ou associations sportives;
- d. les communications d'une autorité étrangère compétente.

² Les témoignages visés à l'al. 1, let. b, doivent être déposés par écrit et signés.

Art. 6 Compétences et devoirs de communication

¹ Les cantons ainsi que les autorités et offices mentionnés à l'art. 13 LMSI communiquent spontanément à fedpol les informations et les renseignements relatifs à des actes de violence perpétrés lors de manifestations sportives.

² Les cantons informent en outre fedpol:

- a. des mesures qu'ils ont prononcées, levées ou modifiées concernant:
 1. une interdiction de stade,
 2. une interdiction de périmètre,
 3. une obligation de se présenter à la police,
 4. une garde à vue;
- b. des infractions aux mesures visées à la let. a;
- c. des périmètres qu'ils ont délimités, ainsi que des plans correspondants.

³ Fedpol détermine l'échelle des plans visés à l'al. 1, let. c.

Art. 7 Interdiction de se rendre dans un pays donné

¹ Fedpol est chargé d'ordonner les interdictions de se rendre dans un pays donné.

² La durée de l'interdiction et les pays de destination concernés doivent être précisés dans la décision.

³ Une manifestation sportive commence par le premier événement officiel la concernant et se termine par le dernier événement officiel qui y est lié.

⁴ Il y a lieu de croire qu'une personne participera à des actes de violence lors d'une manifestation sportive dans un pays donné notamment lorsque cette personne:

- a. a participé à des actes de violence en Suisse;
- b. est déjà connue en raison d'informations fournies par des services de police étrangers relatives à la participation à des actes de violence à l'étranger, ou

- c. est membre d'un groupe qui a déjà participé à des actes de violence en Suisse ou à l'étranger.

⁵ La possibilité d'ordonner une interdiction de se rendre dans un pays donné est en outre subordonnée à l'existence d'éléments indiquant que la personne ou le groupe envisage de se rendre à l'étranger pour assister à l'événement sportif.

⁶ Il y a des éléments concrets et actuels pouvant motiver une interdiction de se rendre dans un pays donné, sans qu'une interdiction de périmètre en raison de violences commises lors de manifestations sportives ait été prononcée par une autorité cantonale, lorsqu'une personne:

- a. a, selon les informations de services de police étrangers, commis des actes de violence à l'étranger;
- b. est membre d'un groupe qui a déjà participé à plusieurs reprises à des actes de violence en Suisse ou à l'étranger, et
- c. a certainement l'intention de se rendre à l'étranger, seule ou en groupe, pour assister à un événement sportif déterminé.

⁷ L'interdiction de se rendre dans un pays donné doit être consignée dans le système de recherches informatisées de la police (RIPOL) et communiquée aux autorités douanières suisses et aux autorités policières et douanières étrangères compétentes.

Section 4 Système d'information HOOGAN

Art. 8 Données

¹ Le système électronique d'information HOOGAN permet la saisie de données relatives aux personnes qui ont commis des actes de violence lors de manifestations sportives en Suisse et à l'étranger et contre lesquelles une mesure visée à l'art. 6, al. 2, let. a, a été décidée.

² Les manifestations sportives et les événements qui y sont liés ainsi que les périmètres délimités par les cantons sont saisis dans HOOGAN.

Art. 9 Droits d'accès

¹ Les autorités ci-après ont accès à HOOGAN exclusivement aux fins suivantes:

- a. les services de fedpol suivants:
 - 1. Le domaine Hooliganisme: pour l'exploitation de HOOGAN, les décisions d'interdiction de se rendre dans un pays donné, l'échange d'informations prévu par la loi, ainsi que l'évaluation de l'analyse et l'appréciation de la situation,
 - 2. la centrale d'engagement de fedpol: pour l'identification des personnes en cas de violence lors de manifestations sportives,

3. le préposé de fedpol à la protection des données et à la protection des informations: pour le traitement des demandes de renseignement et d'effacement liées à HOOGAN;
- b. les collaborateurs des autorités cantonales de police chargés d'empêcher la violence lors de manifestations sportives: pour les interdictions de périmètre, les obligations de se présenter à la police et les gardes à vue, pour l'évaluation de l'analyse et l'appréciation de la situation, ainsi que pour la communication de données personnelles aux organisateurs de manifestations sportives en Suisse;
- c. les services des autorités cantonales de police: pour l'identification des personnes en cas de violence lors de manifestations sportives;
- d. les services du Corps des gardes-frontière (Cgfr) de l'Administration fédérale des douanes (AFD): pour l'exécution des interdictions de se rendre dans un pays donné et d'entrer sur le territoire suisse;
- e. les services de l'Observatoire suisse du hooliganisme: pour l'examen préalable des communications reçues concernant les interdictions de stade et les rapports relatifs aux manifestations sportives des organisateurs de manifestations sportives, ainsi que pour les demandes d'interdiction de se rendre dans un pays donné, d'interdiction de périmètre et d'obligation de se présenter à la police.

² Un accès complet ou un accès partiel à HOOGAN peut être autorisé. L'accès complet permet la lecture, la saisie, la modification et l'effacement de données. L'accès partiel ne permet que la lecture de données actives.

³ Disposent d'un accès complet:

- a. le domaine Hooliganisme;
- b. l'Observatoire suisse du hooliganisme;
- c. les collaborateurs des autorités cantonales de police et du Cgfr chargés d'empêcher la violence lors de manifestations sportives.

⁴ Disposent d'un accès partiel:

- a. la centrale d'engagement de fedpol;
- b. le préposé de fedpol à la protection des données et à la protection des informations;
- c. les autorités cantonales de police;
- d. le Cgfr.

⁵ L'accès partiel des autorités cantonales de police et du Cgfr passe par l'interface du système d'information RIPOL.

⁶ Le Département fédéral de justice et police (DFJP) règle les détails des droits d'accès et les conditions de raccordement à HOOGAN des autorités.

⁷ Le directeur de fedpol, ou son suppléant, statue sur les demandes d'accès individuelles.

⁸ La responsabilité du système HOOGAN incombe au domaine Hooliganisme de fedpol.

Art. 10 Utilisation et communication des données par les organisateurs
de manifestations sportives

¹ Les organisateurs de manifestations sportives ne peuvent communiquer les données enregistrées dans HOOGAN aux responsables de la sécurité de ces manifestations qu'avec l'approbation de l'autorité qui a fourni les données et que dans la perspective de l'application de mesures destinées à lutter contre la violence lors de manifestations sportives.

² Les responsables de la sécurité ne peuvent traiter les données qu'en relation avec la manifestation sportive désignée par l'autorité. Les données peuvent être traitées dans des systèmes électroniques de reconnaissance des personnes.

³ Les responsables de la sécurité et, le cas échéant, les organisateurs des manifestations doivent détruire les données immédiatement après la manifestation sportive. L'autorité qui a fourni les données doit être informée de leur destruction dans les 24 heures.

⁴ Fedpol règle l'utilisation et le traitement des données par les organisateurs de manifestations sportives et les responsables de la sécurité dans un règlement de traitement.

Art. 11 Communication des données à des autorités étrangères

¹ Fedpol peut communiquer des données personnelles à des autorités étrangères de police et à des organes étrangers chargés de la sécurité lors de manifestations sportives.

² Il enregistre la communication de données à des autorités étrangères.

³ Il indique au destinataire la fiabilité et l'actualité des données lors de la communication d'informations et de données personnelles.

⁴ Il signale au destinataire que:

- a. les informations et les données personnelles ne peuvent être utilisées que dans le but pour lequel elles ont été communiquées;
- b. fedpol se réserve le droit de se renseigner sur l'utilisation qui en aura été faite.

Art. 12 Durée de conservation et effacement des données

¹ Les données personnelles et les informations concernant chaque mesure sont effacées trois ans après que la mesure a pris fin.

² Si, durant ces trois années, une nouvelle mesure est prononcée contre la même personne, la durée de la première inscription est prolongée de trois ans, à compter de la date d'inscription de la deuxième mesure.

³ Les données relatives à une mesure donnée sont effacées au plus tard après dix ans.

Art. 13 Dispositions relatives à l'organisation

¹ Pour garantir 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 (OLPD)⁴;
- b. l'ordonnance du 26 septembre 2003 sur l'informatique et la télécommunication dans l'administration fédérale (OIAF)⁵.

² Fedpol 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;
- c. les exigences techniques auxquelles doivent satisfaire les terminaux des utilisateurs.

Section 5

Les banques de données de l'Office central des armes et de l'Office central pour les explosifs et la pyrotechnie

Art. 14 Banques de données

L'Office central des armes et l'Office central pour les explosifs et la pyrotechnie au sein de fedpol travaillent avec les banques de données et les informations associées suivantes:

- a. «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;
- b. «Acquisition d'armes par des personnes domiciliées dans un autre Etat Schengen» (DEWS): informations personnelles concernant l'acquisition d'armes ou d'éléments essentiels d'armes par des personnes domiciliées dans un autre Etat lié par l'un des accords d'association à Schengen;
- c. «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;

⁴ RS 235.11

⁵ RS 172.010.58

- d. «Remise et retrait d'armes de l'armée» (DAWA): informations relatives aux personnes qui se sont vu remettre une arme en toute propriété lorsqu'elles ont été libérées de leurs obligations militaires ou qui se sont vu retirer en vertu de la législation militaire leur arme personnelle ou l'arme qui leur avait été remise en prêt;
- e. «Exploitation des traces laissées par des armes à feu» (ASWA): informations personnelles destinées à l'exploitation des traces laissées par des armes à feu sur des armes, sur des munitions, en particulier des munitions utilisées pour la commission d'actes punissables, et sur des personnes impliquées dans des actes punissables ou concernées par de tels actes;
- f. «BARBARA»: informations relatives aux événements, tirées du domaine d'activité de l'Office central pour les explosifs et la pyrotechnie.

Art. 15 Définitions

Concernant les banques de données des offices centraux, on entend par:

- a. données: les informations mémorisées dans les banques des offices centraux;
- b. objet: le regroupement de données se rapportant à une ou plusieurs personnes, 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;
- 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. accès complet: la possibilité de consulter, de saisir, de modifier et d'effacer des données.

Art. 16 Droits d'accès

Les services de fedpol indiqués ci-après disposent d'un accès complet aux banques de données des offices centraux aux fins suivantes:

- a. concernant les banques de données visées à l'art. 14, let. a à e: le personnel de l'Office central des armes, pour l'exécution de la législation sur les armes, la recherche et l'analyse des données saisies;
- b. concernant la banque de données visée à l'art. 14, let. f: le personnel de l'Office central pour les explosifs et la pyrotechnie, pour l'exécution de la législation sur les explosifs, la recherche et l'analyse des données saisies.

Art. 17 Données traitées

¹ Les données enregistrées dans les banques de données des offices centraux 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 des offices centraux sont structurées selon les critères suivants: communications, objets et relations.

³ Le DFJP règle les différents champs de données et les droits d'accès.

Art. 18 Saisie des données et contrôle de qualité

¹ Seules peuvent être traitées dans les banques de données des offices centraux des informations qui répondent aux buts définis à l'art. 16, al. 1.

² Les collaborateurs des offices centraux saisissent les données dans les banques de données des offices centraux et fixent la catégorie de communications.

³ Le directeur de fedpol, ou son suppléant, peut charger l'organe compétent auprès de fedpol de vérifier les banques de données des offices centraux dans leur domaine de compétence selon l'art. 34 OLPD⁶.

Art. 19 Classement des dossiers

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

² Les dossiers relatifs aux objets et aux communications peuvent être saisis comme données OCR, sauf dans la banque de données BARBARA. Dans la banque de données BARBARA, ils sont saisis uniquement comme données d'image.

³ Il est possible de renoncer au classement-papier des dossiers dans la mesure où les objets et les communications à la base des dossiers sont saisis comme données OCR ou comme données d'image.

Art. 20 Consultation des données

¹ Les données peuvent être consultées suivant les critères suivants: objets, relations, communications, mandats et recherche plein texte. Les données d'image ne peuvent pas être consultées séparément.

² La consultation simultanée des communications mémorisées dans les banques de données DEWA, DEWS, DEBBWA DAWA et ASWA, d'une part et dans la banque de données BARBARA, d'autre part, n'est pas autorisée.

³ Les collaborateurs des offices centraux spécialement formés peuvent procéder à des appréciations dans leur domaine d'activité.

⁴ Les objets et leurs relations peuvent être représentés et enregistrés visuellement.

⁶ RS 235.11

Art. 21 Communication de données par l'Office central des armes

¹ La communication de données issues des banques DEWA, DEWS, DEBBWA, DAWA et ASWA est régie par les art. 63 et 64 de l'ordonnance du 2 juillet 2008 sur les armes (OArm)⁷.

² La communication de données n'est pas autorisée lorsque des intérêts prépondérants publics ou privés s'y opposent.

³ Lors de toute communication, le destinataire doit être renseigné sur la fiabilité et l'actualité des données.

⁴ Il doit être:

- a. informé du but dans lequel il peut exclusivement utiliser les données;
- b. rendu attentif 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 son destinataire, son objet et ses motifs doivent être enregistrés.

Art. 22 Copies de données dans des fichiers

¹ Les données des banques de données des offices centraux 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 issues des banques de données des offices centraux 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 détruites.

Art. 23 Droit d'être renseigné

Le droit d'être renseigné sur les banques de données DEWA, DEWS, DEBBWA, DAWA et ASWA est régi par l'art. 32g LArm.

Art. 24 Durée de conservation

¹ Les données des banques DEWA, DEWS, DEBBWA, DAWA et ASWA sont régies par l'art. 66 OArm⁸.

² Les données de la banque BARBARA peuvent être conservées pendant une durée illimitée.

⁷ RS 514.541

⁸ RS 514.541

Art. 25 Effacement des données

¹ A l'expiration de leur durée de conservation, les données sont effacées dans un délai de trois mois, à moins que le directeur de fedpol, ou son suppléant, ne décide, à la lumière des risques et des dangers 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 est supprimé avec l'effacement de la dernière communication, y compris les relations et données d'image correspondantes.

⁴ Les données destinées à être supprimées sont transférées dans le module d'archivage.

Art. 26 Obligation de proposer des documents aux Archives fédérales

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

² Les données que les Archives fédérales jugent sans valeur archivistique sont éliminées du module d'archivage. Les dossiers jugés sans valeur archivistiques sont détruits. Les autres dispositions légales en matière de destruction des données sont réservées.

Art. 27 Sécurité des données et journalisation

¹ Pour assurer la sécurité des données, sont applicables:

- a. l'art. 20 OLPD⁹;
- b. l'OIAF¹⁰.

² Fedpol 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;
- c. les exigences techniques auxquelles doivent satisfaire les terminaux des utilisateurs.

³ Les données des banques de données des offices centraux ne peuvent être transmises que sous forme chiffrée durant toute l'opération de transmission.

⁹ RS 235.11

¹⁰ RS 172.010.58

Art. 28 Responsabilités et compétences

¹ Fedpol assume la responsabilité des données pour les banques de données des offices centraux. Il en édicte le règlement de traitement.

² Le service compétent de fedpol est chargé de la formation et de l'assistance aux utilisateurs et veille à la mise en œuvre du règlement de traitement.

³ La responsabilité technique intégrale des banques de données des offices centraux incombe au Département fédéral de la défense, de la protection de la population et des sports (DDPS).

⁴ Le prestataire de services TED du DDPS veille à l'exploitation, à l'entretien et à la sécurité des banques de données. Les développements ultérieurs s'effectuent en accord avec le responsable de l'application au sein de fedpol. Les détails de la collaboration sont réglés dans un accord administratif.

⁵ Le préposé de fedpol à la protection des données et à la protection des informations peut vérifier au cas par cas que le traitement de données des banques de données des offices centraux est bien conforme aux dispositions relatives à la protection des données.

Section 6 Entrée en vigueur

Art. 29

La présente ordonnance entre en vigueur le 1^{er} janvier 2010.

4 décembre 2009

Au nom du Conseil fédéral suisse:

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