

Ordonnance sur le système informatisé des Offices centraux de police criminelle de la Confédération

(Ordonnance JANUS)

du 17 mai 2000

Le Conseil fédéral suisse,

vu les art. 11, al. 1, 12, al. 2, 13, al. 1, et 15 de la loi fédérale du 7 octobre 1994 sur les Offices centraux de police criminelle de la Confédération (LOC)¹,

arrête:

Section 1 Dispositions générales

Art. 1 Objet

La présente ordonnance règle la gestion et l'utilisation du système informatisé commun des Offices centraux de police criminelle de la Confédération (JANUS).

Art. 2 But du système informatisé

JANUS a pour but de faciliter:

- a. les tâches légales d'information, de coordination et d'analyse des Offices centraux de police criminelle de la Confédération (offices centraux);
- b. l'exécution, dans les domaines de compétence des offices centraux, des enquêtes préventives et des enquêtes de police judiciaire;
- c. la coopération des offices centraux avec les autorités cantonales de poursuite pénale et les services de police criminelle des cantons qui participent dans le cadre de leurs compétences à la lutte contre le crime intercantonal ou international;
- d. la collaboration des offices centraux avec les autorités étrangères dans la lutte contre la criminalité internationale;
- e. la gestion des documents et des dossiers utilisés par les offices centraux.

Art. 3 Champ d'application

Sont saisies dans le système JANUS les données nécessaires à l'accomplissement des tâches assignées aux offices centraux à l'art. 2 LOC dans les domaines suivants:

RS 360.2

¹ RS 360; RO 2000 1367

- a. la lutte contre le trafic illicite des stupéfiants selon l'art. 29 de la loi fédérale du 3 octobre 1951 sur les stupéfiants² ainsi que les art. 9 et 10 LOC;
- b. la lutte contre le crime organisé selon les art. 7 et 8 LOC
- c. la lutte contre la fausse monnaie selon de la Convention internationale du 20 avril 1929 pour la répression du faux monnayage³;
- d. la lutte contre la traite des blanches selon l'Arrangement international du 18 mai 1904 en vue d'assurer une protection efficace contre le trafic criminel connu sous le nom de traite des blanches⁴, la Convention internationale du 4 mai 1910 relative à la répression de la traite des blanches⁵, la Convention internationale du 30 septembre 1921 pour la suppression de la traite des femmes et des enfants⁶ et la Convention du 11 octobre 1933 relative à la répression de la traite des femmes majeures⁷;
- e. la lutte contre la circulation des publications obscènes selon l'Arrangement international du 4 mai 1910 relatif à la répression de la circulation des publications obscènes⁸ et la Convention internationale du 12 septembre 1923 pour la répression de la circulation et du trafic des publications obscènes⁹.

Art. 4 Structure de JANUS

Le système JANUS se compose des sous-systèmes suivants:

- a. «Personnes et antécédents» (PV), où sont enregistrées des données sur des personnes et leurs antécédents recueillis dans le cadre d'enquêtes préventives, d'enquêtes de police judiciaire ou de sources accessibles au public;
- b. «Journaux» (JO), où sont enregistrées par affaire des données provenant d'enquêtes préventives, d'enquêtes de police judiciaire ou de sources accessibles au public (notamment surveillances des télécommunications, observations, mains courantes d'enquête);
- c. «Contrôle des affaires et des délais» (GT), où sont enregistrées les données nécessaires au suivi des affaires;
- d. «Renseignements généraux» (ER), où sont enregistrées des données utiles à l'accomplissement des tâches telles que répertoires téléphoniques, extraits de presse, descriptifs des compétences de diverses administrations ou informations provenant de sources accessibles au public;
- e. «lexiques techniques, répertoires et méthodes d'action criminelle» (TL);
- f. «Rapport de situation» (LA), où sont enregistrés des rapports décrivant la situation nationale et internationale;

² RS 812.121
³ RS 0.311.51
⁴ RS 0.311.31
⁵ RS 0.311.32
⁶ RS 0.311.33
⁷ RS 0.311.34
⁸ RS 0.311.41
⁹ RS 0.311.42

- g. «Analyses» (AN), où sont enregistrés les résultats des mandats d'analyse;
- h. «Blüte» (BL), où sont enregistrés les différents types de fausse monnaie et les techniques de faux monnayage.

Art. 5 Structure des sous-systèmes «Personnes et antécédents» et «Journaux»

¹ Le sous-système «Personnes et antécédents» (PV) se compose:

- a. des données de base relatives à l'identité des personnes;
- b. des antécédents, soit les données relatives aux faits, répertoriées en fonction de différentes catégories criminologiques;
- c. des sous-champs dont l'utilisation permet, entre autres, de marquer les éléments de comparaison, notamment avec des tierces personnes, dans le texte d'un antécédent et de consulter des données d'après ces éléments de comparaison. La liste complète des sous-champs figure à l'annexe 1¹⁰.

² Le sous-système «Journaux» se compose:

- a. de l'en-tête, soit les données relatives aux journaux tenus dans le cadre d'une affaire;
- b. des inscriptions, soit les données relatives aux faits.

³ Les données de base et les antécédents qui s'y rapportent ou l'en-tête et les inscriptions qui s'y rapportent constituent un bloc de données.

⁴ Dans les sous-systèmes «Personnes et antécédents» et «Journaux», les données recueillies dans le cadre d'une enquête préventive ou d'une enquête de police judiciaire après son ouverture par une autorité d'instruction, de même que celles provenant de sources accessibles au public sont classées dans trois catégories distinctes.

Art. 6 Données traitées

¹ En matière de lutte contre le trafic illicite des stupéfiants, seules les données concernant des personnes qui sont soupçonnées d'effectuer un tel trafic, d'y être impliquées, d'y participer ou d'en tirer profit peuvent être traitées dans le système JANUS. Les données se rapportant à des personnes qui ne font que consommer des stupéfiants n'y sont pas enregistrées.

² En matière de lutte contre le crime organisé, les données traitées dans le système JANUS concernent:

- a. les organisations que l'on peut raisonnablement soupçonner d'être des organisations criminelles au sens de l'art. 260^{ter} du code pénal¹¹;
- b. les personnes que l'on peut raisonnablement soupçonner de préparer, de commettre ou de faciliter des actes délictueux auxquels on présume qu'une organisation au sens de la let. a participe;

¹⁰ Les annexes 1 et 2 de la présente ordonnance ne sont publiées ni dans le RO, ni dans le RS. Des tirés à part peuvent être obtenus à l'EDMZ, 3003 Berne.

¹¹ RS 311.0

- c. les personnes que l'on peut raisonnablement soupçonner d'appartenir à une organisation au sens de la lettre a ou de lui apporter leur soutien.

³ En vue de la lutte contre la fausse monnaie, la traite des êtres humains et la circulation des publications obscènes, les données concernant des personnes qui sont soupçonnées de se livrer à une telle activité délictueuse, d'y être impliquées, d'y participer ou d'en retirer bénéfice sont traitées dans le système JANUS.

⁴ Les données concernant des tierces personnes au sujet desquelles aucune donnée de base n'a été enregistrée peuvent être traitées dans le système JANUS que si cela s'avère nécessaire à la réalisation des buts mentionnés à l'art. 2.

⁵ Les données provenant de sources accessibles au public peuvent être traitées dans les sous-systèmes «Personnes et antécédents» et «Journaux» pour autant qu'elles soient en rapport avec une identité ou une affaire déjà traitée en vertu des al. 1 à 3;

⁶ Seules les données énumérées à l'annexe 1¹² peuvent être traitées dans le système JANUS.

Art. 7 Provenance des données

Les données enregistrées dans le système JANUS proviennent:

- a. d'enquêtes de police menées par les autorités fédérales ou cantonales avant l'ouverture d'une enquête de police judiciaire;
- b. d'enquêtes de police judiciaire menées par les autorités cantonales de poursuite pénale et de police;
- c. d'enquêtes de police judiciaire menées par les autorités fédérales de poursuite pénale et de police;
- d. des organes de sûreté de la Confédération, selon la loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI)¹³;
- e. de renseignements communiqués conformément aux art. 2, let. b à d, 4, 8, al. 1, et 10 LOC;
- f. de vérifications effectuées dans le cadre de l'exécution de demandes d'entraide judiciaire avec recherche de preuves;
- g. de sources accessibles au public.

Art. 8 Droit des personnes concernées à être renseignées

Toute demande de renseignements concernant les données du système JANUS est régie par l'art. 14 LOC.

¹² Les annexes 1 et 2 de la présente ordonnance ne sont publiées ni dans le RO, ni dans le RS. Des tirés à part peuvent être obtenus à l'EDMZ, 3003 Berne.

¹³ RS 120

Art. 9 Intranet

L'Office fédéral de la police (office) met à la disposition des utilisateurs du système JANUS un système fermé d'échange d'informations appelé Intranet JANUS. Ce système, chiffré, se compose de services intranet et d'une messagerie électronique. Les données administratives contenues dans intranet, ainsi que la messagerie électronique, peuvent être mises à la disposition d'autres personnes, pour autant que celles-ci apportent un soutien logistique ou organisationnel à la bonne marche du système JANUS et contribuent à la gestion et à la formation de ses utilisateurs.

Section 2 Utilisateurs et accès**Art. 10** Accès en général

¹ Ont accès au système JANUS au moyen d'une procédure d'appel, pour autant que cela soit nécessaire à l'accomplissement de leurs tâches légales:

- a. les offices centraux;
- b. les services de police criminelle des cantons qui, dans le cadre de leurs attributions, collaborent avec les offices centraux (art. 12 LOC);
- c. le service de contrôle de l'office (service de contrôle);
- d. le conseiller à la protection des données de l'office;
- e. le chef de projet et les gestionnaires du système.

² Sur demande et pour des procédures déterminées, l'accès au sous-système «Journaux» peut être accordé aux autorités d'instruction pénale des cantons. L'office précise les modalités dans le règlement sur le traitement des données.

³ Les organes de surveillance des frontières et les services douaniers ont accès au sous-système «Lexiques techniques, répertoires et méthodes d'action criminelle» (TL).

⁴ Les autorisations d'accès par catégories d'utilisateurs aux différentes données du système JANUS sont fixées à l'annexe 2¹⁴.

Art. 11 Accès aux sous-systèmes «Personnes et antécédents» et «Journaux»

¹ Dans des cas spéciaux, les organes ayant introduit les données dans le sous-système «Personnes et antécédents» peuvent restreindre l'accès à ces données, en déterminant la sphère des personnes autorisées à les traiter.

² Dans le cadre d'une enquête, seuls les services de police criminelle et les autorités de poursuite pénale des cantons qui mènent cette enquête ont accès aux données du sous-système «Journaux» relatives à cette enquête. Les spécialistes des offices centraux désignés dans le règlement sur le traitement des données peuvent aussi accéder

¹⁴ Les annexes 1 et 2 de la présente ordonnance ne sont publiées ni dans le RO, ni dans le RS. Des tirés à part peuvent être obtenus à l'EDMZ, 3003 Berne.

à ces données. Dans des cas spéciaux, les autorités cantonales chargées de l'enquête peuvent leur refuser cet accès.

³ Si un autre canton est concerné par l'enquête, les offices centraux ou le service cantonal compétent peuvent étendre l'accès aux données à l'autorité correspondante du canton concerné. Ils prennent auparavant contact avec les autorités cantonales chargées de l'enquête.

Section 3 Traitement des données

Art. 12 Saisie des données

¹ Les offices centraux et les services de police criminelle concernés des cantons introduisent eux-mêmes dans le système JANUS les données concernant les antécédents qu'ils ont recueillis. Ce faisant, ils déterminent les catégories d'antécédents et qualifient ces antécédents comme étant fiables ou peu fiables en fonction de leur provenance, de leur mode d'obtention, de leur contenu et des données déjà disponibles.

² Les données destinées aux sous-systèmes «Personnes et antécédents» et «Journaux» sont saisies provisoirement jusqu'à ce qu'elles soient vérifiées par le service de contrôle.

Art. 13 Contrôle des données

¹ Le service de contrôle s'assure que les données saisies dans le système JANUS sont conformes aux dispositions de la présente ordonnance et qu'elles sont exploitables sur le plan technique et policier.

² Il confirme la saisie définitive des données enregistrées provisoirement après avoir vérifié leur exactitude, leur attribution correcte à une catégorie criminologique, leur qualification correcte quant à leur fiabilité ainsi que l'état de l'enquête. Pour ce faire, il tient compte en particulier de la provenance et du contenu des informations, ainsi que des autres données déjà disponibles dans le système.

³ Les enregistrements insuffisants sont corrigés ou effacés par le service de contrôle. Ce dernier communique au préalable les modifications importantes et les effacements à l'organe ayant effectué la saisie.

⁴ Le service de contrôle peut demander de consulter les dossiers cantonaux afin de comparer les documents avec les informations saisies et de vérifier leur conformité aux dispositions de la présente ordonnance.

⁵ L'office précise les modalités de la vérification des données dans le règlement sur le traitement des données.

Art. 14 Appréciation générale et périodique des données des sous-systèmes «Personnes et antécédents» et «Journaux»

¹ Le service de contrôle procède à une appréciation générale de chaque bloc de données des sous-systèmes «Personnes et antécédents» et «Journaux» au plus tard

cinq ans après la saisie de la première donnée. Après cette appréciation générale, une nouvelle vérification est faite tous les trois ans.

² Il examine en particulier:

- a. si les données saisies sont conformes aux dispositions de la présente ordonnance. Si tel n'est pas le cas, il les corrige ou les efface. L'organe ayant effectué la saisie est informé au préalable des effacements et corrections ayant une influence sur la teneur de l'information;
- b. si l'ensemble des informations contenu dans un bloc de données est encore proportionnel et si l'ensemble des enregistrements est susceptible d'apporter des éléments de suspicion pour des investigations supplémentaires. Si ces conditions ne sont pas remplies, il efface le bloc de données après en avoir informé l'organe ayant effectué la saisie.

³ Les informations concernant des tierces personnes enregistrées depuis plus de trois ans sans qu'un bloc de données propre n'ait été ouvert pour elles sont rendues anonymes lors de l'appréciation générale, à moins qu'elles ne servent dans une procédure pénale déterminée.

Art. 15 Interconnexions

¹ Afin d'éviter une double saisie:

- a. les offices centraux peuvent copier les données faisant l'objet d'une mention spéciale à l'annexe 1¹⁵ de la présente ordonnance et transmises par le canal d'INTERPOL dans l'Index central des dossiers (ZAN) ou dans le système informatisé de gestion et d'indexation de dossiers et de personnes (IPAS) qui le remplacera. Cette fonction n'est pas automatisée.
- b. les utilisateurs dans les cantons peuvent copier les données contenues dans leurs systèmes cantonaux dans le système JANUS.

² L'office précise les modalités de cette opération dans le règlement sur le traitement des données.

Art. 16 Communication de données à des autorités tenues de fournir des renseignements

¹ Si cela leur est nécessaire pour obtenir les renseignements dont ils ont besoin et motiver leurs demandes d'entraide administrative, les offices centraux peuvent communiquer des données personnelles enregistrées dans le système JANUS aux autorités suivantes tenues de coopérer au sens de l'art. 4 LOC:

- a. les autorités de poursuite pénale, notamment les ministères publics, les juges d'instruction, les autorités d'entraide judiciaire et les organes de police judiciaire de la Confédération et des cantons;

¹⁵ Les annexes 1 et 2 de la présente ordonnance ne sont publiées ni dans le RO, ni dans le RS. Des tirés à part peuvent être obtenus à l'EDMZ, 3003 Berne.

- b. les services de police, notamment les organes de la police de sûreté et de la police administrative de la Confédération et des cantons, ainsi que les autorités fédérales chargées de l'application de la LMSI¹⁶;
- c. les organes de surveillance des frontières et les services douaniers;
- d. les autorités de la Confédération et des cantons assumant des tâches de police des étrangers, compétentes en matière d'entrée et de séjour des étrangers, d'octroi du droit d'asile ou encore chargées de rendre les décisions d'admission provisoire;
- e. les contrôles des habitants et les autorités chargées de l'administration des registres du commerce, des registres d'état civil, des registres fiscaux, des registres de la circulation routière, des registres de l'aviation civile et des registres fonciers;
- f. les autorités compétentes en matière de relations diplomatiques et consulaires;
- g. les autres autorités chargées de délivrer les autorisations de circulation pour certains biens.

² Afin de les assister dans l'accomplissement de leurs tâches légales, les offices centraux peuvent en outre communiquer, spontanément ou en réponse à des requêtes fondées, des données personnelles enregistrées dans le système JANUS aux autorités suivantes:

- a. les autorités mentionnées à l'al. 1, let. a, dans le cadre de procédures pénales, d'enquêtes de police judiciaire et de procédures d'entraide judiciaire;
- b. les autorités mentionnées à l'al. 1, let. b et c, dans le cadre d'enquêtes de police judiciaire, ainsi que pour l'accomplissement de tâches relatives à l'application de la LMSI;
- c. les autorités mentionnées à l'al. 1, let. d, chargées d'accomplir des tâches de police des étrangers, d'empêcher ou de réprimer les infractions aux dispositions relatives à l'entrée et au séjour des étrangers et à la législation en matière d'asile.

³ L'étendue du devoir de renseigner et les conditions auxquelles il est soumis sont régies par l'art. 6, al. 2 à 4, de l'ordonnance du 19 novembre 1997 sur les Offices centraux de police criminelle près l'Office fédéral de la police¹⁷. Ceci s'applique de manière analogue aux requêtes émanant des autorités mentionnées à l'al. 2.

Art. 17 Communication de données à d'autres destinataires

¹ Si cela leur est nécessaire pour obtenir les renseignements dont ils ont besoin et motiver leurs demandes d'entraide administrative, les offices centraux peuvent communiquer des données personnelles enregistrées dans le système JANUS à d'autres destinataires, à savoir:

¹⁶ RS 120

¹⁷ RS 172.213.711

- a. les autorités d'autres Etats exerçant des fonctions de poursuite pénale et de police, dans la mesure où les conditions énumérées à l'art. 13, al. 2, LOC sont remplies;
- b. les tribunaux internationaux, ainsi que les organisations internationales exerçant des fonctions de poursuite pénale et de police (notamment EUROPOL et INTERPOL), dans la mesure où les conditions énumérées à l'art. 13, al. 2, LOC sont remplies;
- c. les autorités financières de la Confédération et des cantons;
- d. l'Administration fédérale des finances;
- e. la Commission fédérale des banques;
- f. l'autorité de contrôle en matière de lutte contre le blanchiment d'argent;
- g. la Commission fédérale des maisons de jeu;
- h. le Secrétariat d'Etat à l'économie;
- i. les autorités fédérales chargées des contrôles de sécurité relatifs à des personnes et des mesures de protection au sens de l'art. 2, al. 4, let. c et d, de la LMSI¹⁸;
- j. l'Office fédéral de l'aviation civile;
- k. les autorités compétentes en matière d'acquisition de terrains par des personnes résidant à l'étranger;
- l. les organisations non étatiques, qui œuvrent notamment en faveur de la lutte contre l'exploitation sexuelle à des fins commerciales, dans la mesure où il s'agit de prévenir et d'identifier des formes spécifiques de criminalité;
- m. les autorités de surveillance de la Confédération et des cantons.

² Afin de les assister dans l'accomplissement de leurs tâches légales, les offices centraux peuvent en outre communiquer spontanément ou en réponse à des requêtes fondées, des données personnelles enregistrées dans le système JANUS aux autorités suivantes:

- a. les autorités d'autres Etats exerçant des fonctions de poursuite pénale, pour leurs enquêtes de police judiciaire, dans la mesure où les conditions énumérées à l'art. 13, al. 2, LOC sont remplies;
- b. les tribunaux internationaux ainsi que les organisations internationales exerçant des fonctions de poursuite pénale et de police (notamment EUROPOL et INTERPOL), pour le traitement d'affaires déterminées, dans la mesure où les conditions énumérées à l'art. 13, al. 2, LOC sont remplies;
- c. les autorités financières de la Confédération et des cantons, pour leurs enquêtes de police judiciaire dans le domaine fiscal;
- d. l'Administration fédérale des finances, dans le cadre des procédures pénales administratives qu'elle mène;

- e. la Commission fédérale des banques, pour l'assister dans son activité de surveillance découlant de la législation sur les banques, les bourses et les fonds de placement, s'il s'agit d'informations fiables qui sont nécessaires à une procédure ou de nature à entraîner l'ouverture d'une procédure;
 - f. l'autorité de contrôle en matière de lutte contre le blanchiment d'argent, pour l'assister dans son activité de surveillance découlant de la loi du 10 octobre 1997 concernant le blanchiment d'argent dans le secteur financier¹⁹, s'il s'agit d'informations fiables qui sont nécessaires à une procédure ou de nature à entraîner l'ouverture d'une procédure;
 - g. la Commission fédérale des maisons de jeu, pour l'assister dans son activité de surveillance découlant de la législation sur les jeux de hasard;
 - h. les autorités fédérales chargées des contrôles de sécurité relatifs à des personnes et des mesures de protection au sens de l'art. 2, al. 4, let. c et d, de la LMSI, pour leurs investigations, s'il s'agit d'informations fiables;
- ³ Toutes les données personnelles sont communiquées sur requête aux autorités de surveillance de la Confédération et des cantons, ainsi qu'au Préposé fédéral à la protection des données, pour leurs fonctions de contrôle.

Art. 18 Autres dispositions relatives à la communication de données

¹ Lors de la communication de données du système JANUS, les interdictions portant sur l'utilisation doivent être respectées. Les offices centraux ne peuvent communiquer à des Etats étrangers des données concernant des demandeurs d'asile, des réfugiés ou des personnes provisoirement admises qu'après consultation de l'office fédéral compétent.

² Les offices centraux refusent la communication de données du système JANUS si des intérêts prépondérants publics ou privés s'y opposent. Les données qui ne sont pas destinées à être communiquées doivent être signalées comme telles dans le système par les utilisateurs des offices centraux ou des cantons.

³ Les services de police criminelle concernés des cantons peuvent, dans l'intérêt d'une enquête de police judiciaire, communiquer des données du système JANUS aux autres autorités de poursuite pénale et de police de leur canton. Les offices centraux doivent en être informés.

⁴ Lors de toute communication de données du système JANUS, le destinataire doit être informé de leur fiabilité et de leur actualité. Il ne peut les utiliser que dans le but en vue duquel elles lui ont été communiquées. Il doit être prévenu des restrictions d'emploi et du fait que les offices centraux se réservent le droit d'exiger des informations sur l'utilisation qui aura été faite de ces données.

⁵ La communication, ainsi que le destinataire, l'objet et le motif de la demande de renseignements doivent être enregistrés dans le système JANUS.

¹⁹ RS 955.0

Art. 19 Traitement de données dans des systèmes d'analyse externes

¹ Les données personnelles du système JANUS peuvent être copiées et traitées dans un système externe spécifiquement destiné à l'analyse pour exécuter une mission d'analyse dont le contenu et la durée sont définis:

- a. par la direction des offices centraux; une telle mission ne peut être entreprise que par des spécialistes des offices centraux expressément autorisés et avec l'approbation du conseiller à la protection des données de l'office fédéral;
- b. par l'autorité de police judiciaire compétente; une telle mission ne peut être entreprise que par des spécialistes de police criminelle des cantons expressément autorisés et après information de l'autorité cantonale compétente en matière de protection des données.

² Une fois la mission accomplie, les données copiées dans le système externe doivent être immédiatement détruites.

³ L'office précise les modalités dans le règlement sur le traitement des données.

Art. 20 Durée de conservation

La durée de conservation de chaque bloc de données relatives aux personnes contenues dans le système JANUS échoit cinq ans après la saisie du premier antécédent ou de la première inscription se rapportant à ce bloc de données. Chaque nouvelle saisie d'un antécédent fait courir un nouveau délai de trois ans. Si ce dernier dépasse la durée de conservation générale, celle-ci sera prolongée en conséquence. Un effacement préalable selon les dispositions des art. 13 et 14 demeure réservé.

Art. 21 Communication de l'effacement des données

Lorsque des données du système JANUS sont effacées, le service de contrôle doit préalablement en informer l'organe ayant effectué la saisie.

Art. 22 Obligation de proposer les documents aux Archives fédérales

¹ Les offices centraux proposent aux Archives fédérales, au plus tard lors de l'effacement d'un bloc de données, les données et documents qui s'y rapportent.

² Ils proposent également aux Archives fédérales les données et documents qui ne font pas partie d'un dossier personnel, au plus tard dès l'effacement, dans le système JANUS, du dernier antécédent ou de la dernière inscription qui s'y rapporte.

Section 4 Mesures organisationnelles

Art. 23 Sécurité des données

La sécurité des données est garantie par l'ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données²⁰, le paragraphe concernant la sécurité informatique de l'ordonnance du 23 février 2000 sur l'informatique et la télécommunication dans l'administration fédérale²¹, ainsi que les recommandations de l'Unité de stratégie informatique de la Confédération.

Art. 24 Journalisation

Le Département fédéral de justice et police (département) précise, dans une directive, les modalités de l'évaluation de la journalisation du traitement des données.

Art. 25 Règlement sur le traitement des données

L'office précise les autres dispositions de surveillance dans le règlement sur le traitement des données.

Art. 26 Surveillance et responsabilité

¹ L'office est responsable du système JANUS.

² Le service de contrôle veille à ce que les utilisateurs se conforment à la présente ordonnance, à ses annexes et au règlement sur le traitement des données.

³ Le Centre de service informatique du département est responsable de l'exploitation du système JANUS.

Art. 27 Financement

¹ La Confédération finance la transmission des données jusqu'au distributeur principal sis dans les cantons.

² Les cantons assument:

- a. les frais d'acquisition et d'entretien de leurs appareils;
- b. les frais d'installation et d'exploitation de leur réseau de distribution.

Art. 28 Exigences techniques

¹ Les terminaux utilisés par les cantons doivent répondre aux exigences techniques de la Confédération.

² L'office règle les détails dans le règlement sur le traitement des données.

²⁰ RS 235.11

²¹ RS 172.010.58

Section 5 Dispositions finales

Art. 29 Abrogation du droit en vigueur

Sont abrogées:

- a. l'ordonnance du 26 juin 1996 sur le système de traitement des données en matière de lutte contre le trafic illicite de stupéfiants²²;
- b. l'ordonnance du 19 novembre 1997 sur le système de traitement des données en matière de lutte contre le crime organisé²³;
- c. l'ordonnance du 28 septembre 1998 sur le système de traitement des données en matière de lutte contre la fausse monnaie, la traite des êtres humains et la pornographie²⁴.

Art. 30 Modification du droit en vigueur

Les ordonnances ci-après sont modifiées comme suit:

1. Ordonnance du 1^{er} décembre 1986 concernant le Service d'identification²⁵

Art. 13a, al. 1

¹ Afin d'éviter une double saisie, les données concernant les domaines de compétences des Offices centraux qui sont transmises par le canal d'INTERPOL peuvent être copiées dans le système informatisé des Offices centraux de police criminelle de la Confédération (JANUS). Cette fonction n'est pas automatisée et le texte de l'enregistrement ainsi copié doit être effacé dans le système ZAN.

2. Ordonnance du 16 mars 1998 sur le Bureau de communication en matière de blanchiment d'argent²⁶

Art. 3, al. 1, let. d et e

¹ En vue de l'accomplissement de ses tâches légales, le bureau peut être raccordé au moyen d'une procédure d'appel (on line) aux banques de données suivantes:

- d. le système de traitement des données en matière des Offices centraux de police criminelle de la Confédération (JANUS);
- e. *abrogée*

²² RO 1996 2287, 1998 72 2337

²³ RO 1998 43 2337

²⁴ RO 1998 2337

²⁵ RS 172.213.57

²⁶ RS 955.23

Art. 31 Entrée en vigueur

La présente ordonnance entre en vigueur le 15 juin 2000.

17 mai 2000

Au nom du Conseil fédéral suisse:

Le président de la Confédération, Adolf Ogi

La chancelière de la Confédération, Annemarie Huber-Hotz