Ordonnance sur la protection contre les cyberrisques dans l'administration fédérale

(Ordonnance sur les cyberrisques, OPCy)

du 27 mai 2020 (Etat le 1er juillet 2020)

Le Conseil fédéral suisse,

vu l'art. 30 de la loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure[1] et les art. 43, al. 2 et 3, 47, al. 2, et 55 de la loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration[2],

arrête:

1 Chapitre 1 Dispositions générales

Art. 1 Objet

La présente ordonnance règle l'organisation de l'administration fédérale de manière à assurer la protection contre les cyberrisques de même que les tâches et les compétences des différents offices dans le domaine de la cybersécurité.

Art. 2 Champ d'application

La présente ordonnance s'applique:

a. aux unités administratives de l'administration fédérale centrale au sens de l'art. 7 de l'ordonnance du 25 novembre 1998 sur l'organisation du gouvernement et de l'administration[3];

b. aux autorités et offices qui, en vertu de l'art. 2, al. 2 et 3, de l'ordonnance du 9 décembre 2011 sur l'informatique dans l'administration fédérale (OIAF)[4], s'engagent à la respecter.

Art. 3 Définitions

Dans la présente ordonnance, on entend par:

a. *cybersécurité:* la situation dans laquelle le traitement des données, notamment l'échange de données entre les personnes et les organisations par l'intermédiaire d'infrastructures d'information et de communication, fonctionnent comme prévu;

RO **2020** 2107

1 RS **120**
2 RS **172.010**
3 RS **172.010.1**
4 RS **172.010.58**

b. *cyberincident:* tout événement nuisant à la confidentialité, à l'intégrité, à la disponibilité ou à la traçabilité des données ou pouvant occasionner des dysfonctionnements, qu'il soit accidentel ou provoqué intentionnellement par un tiers non autorisé;

c. *cyberrisque:* le risque de survenance d'un cyberincident, son ampleur résultant du produit de la probabilité de survenance et de l'étendue des dommages;

d. *résilience:* l'aptitude d'un système, d'une organisation ou d'une société à faire face à des perturbations internes ou externes et à maintenir son bon fonctionnement ou à le rétablir aussi rapidement et complètement que possible;

e. *sécurité informatique:* l'aspect de la cybersécurité qui concerne les systèmes techniques;

f. *directives en matière de sécurité informatique:* les exigences de sécurité concernant l'organisation, les processus, les prestations et la technique;

g. *infrastructures critiques:* les processus, systèmes et installations indispensables au fonctionnement de l'économie et au bien-être de la population.

Chapitre 2 Principes régissant la protection contre les cyberrisques

Art. 4 Objectifs

1 L'administration fédérale veille à ce que ses organes et ses systèmes présentent une résilience appropriée face aux cyberrisques.

2 Elle collabore avec les cantons, les communes, les milieux économiques et scientifiques, la société et les partenaires internationaux, dans la mesure où cette collaboration est utile à la protection de ses intérêts en matière de sécurité; elle encourage l'échange d'informations.

Art. 5 Stratégie nationale de protection de la Suisse contre les cyberrisques

La stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) définie par le Conseil fédéral établit le cadre stratégique régissant la prévention et la détection précoce des cyberrisques, ainsi que la réaction et la résilience en cas de cyberincident.

Art. 6 Domaines

Les mesures de protection contre les cyberrisques sont subdivisées en trois domaines:

a. domaine de la cybersécurité: ensemble des mesures visant à prévenir et à gérer les incidents et à améliorer la résilience face aux cyberrisques ainsi qu'à développer la coopération internationale à cet effet;

b. domaine de la cyberdéfense: ensemble des mesures prises par les services de renseignement et l'armée dans le but de protéger les systèmes critiques dont dépend la défense nationale, de se défendre contre les cyberattaques, de garantir la disponibilité opérationnelle de l'armée dans toutes les situations ayant trait au cyberespace et de développer ses capacités et compétences afin qu'elle puisse apporter un appui subsidiaire aux autorités civiles; ce domaine inclut également des mesures visant à identifier les menaces et les attaquants ainsi qu'à entraver et à bloquer les attaques;

c. domaine de la poursuite pénale de la cybercriminalité: ensemble des mesures prises par la police et les ministères publics de la Confédération et des cantons pour lutter contre la cybercriminalité.

Chapitre 3 Organisation et compétences

Section 1 Collaboration interdépartementale

Art. 7 Conseil fédéral

Le Conseil fédéral assume les fonctions suivantes:

a. surveiller la mise en œuvre de la SNPC au moyen du contrôle de gestion stratégique et adopter des mesures si nécessaire;

b. décider, dans les limites de ses compétences, dans quels domaines il convient d'édicter ou de modifier des directives en matière de protection contre les cyberrisques;

c. édicter des instructions sur la protection de l'administration fédérale contre les cyberrisques;

d. autoriser des dérogations à ses directives.

Art. 8 Groupe Cyber

1 Le Groupe Cyber se compose:

a. du délégué à la cybersécurité (art. 6*a* de l'ordonnance du 17 février 2010 sur l'organisation du Département fédéral des finances[5]), qui représente le Département fédéral des finances (DFF);

b. d'un représentant du Département fédéral de la défense, de la protection de la population et des sports (DDPS);

c. d'un représentant du Département fédéral de justice et police (DFJP);

d. d'un représentant des cantons, désigné par la conférence des gouvernements cantonaux compétente.

2 Il est présidé par le délégué à la cybersécurité.

5 RS **172.215.1**

3 Il informe les représentants des autres unités administratives actives dans le domaine des cyberrisques sur les points inscrits à l'ordre du jour et peut les inviter à assister à certaines de ses séances. S'agissant des aspects de politique extérieure, il fait appel au Département des affaires étrangères (DFAE). Il peut également recourir à des experts des milieux économiques et des hautes écoles.

4 Le Groupe Cyber assume notamment les tâches suivantes:

a. évaluer les cyberrisques et leur évolution probable au moyen d'informations relevant des domaines de la cybersécurité, de la cyberdéfense et de la poursuite pénale de la cybercriminalité;

b. évaluer en permanence les dispositifs existants dans les domaines de la cybersécurité, de la cyberdéfense et de la poursuite pénale de la cybercriminalité et vérifier leur adéquation à la situation;

c. accompagner, au besoin en collaboration avec d'autres services, la gestion interdépartementale des incidents;

d. informer le Groupe Sécurité de la Confédération des cyberincidents et des développements relevant de la politique extérieure et de la politique de sécurité.

5 Les trois départements représentés au sein du Groupe Cyber mettent à disposition les informations permettant une évaluation commune de la situation.

6 Le Service de renseignement de la Confédération (SRC) fournit au Groupe Cyber une vue d'ensemble de la situation en matière de cybermenace.

Art. 9 Comité de pilotage de la stratégie nationale de protection de la Suisse contre les cyberrisques

1 Le Conseil fédéral met en place un comité de pilotage de la stratégie nationale de protection de la Suisse contre les cyberrisques (CP SNPC).

2 Le CP SNPC se compose du délégué à la cybersécurité, de représentants des cantons désignés par la conférence des gouvernements cantonaux compétente, de représentants des milieux économiques et des hautes écoles ainsi que de représentants des unités administratives qui ont la haute main sur la mise en œuvre de mesures de la SNPC. Chaque département et la Chancellerie fédérale disposent au moins d'un représentant au sein du CP SNPC.

3 Le CP SNPC est présidé par le délégué à la cybersécurité.

4 Il assume les tâches suivantes:

a. veiller à la cohérence stratégique lors de la mise en œuvre des mesures de la SNPC et évaluer en permanence leur état d'avancement au moyen d'un contrôle de gestion stratégique;

b. proposer des mesures d'urgence en cas de mise en œuvre tardive ou incomplète des mesures de la SNPC;

c. assurer le développement continu de la SNPC en suivant l'évolution de la menace en concertation avec le Groupe Cyber et proposer au besoin des ajustements de la SNPC;

d. rendre compte chaque année au Conseil fédéral et au grand public de la mise en œuvre de la SNPC;

e. veiller à ce que les acteurs de la Confédération, des cantons, des milieux économiques et des hautes écoles adoptent une approche coordonnée dans la mise en œuvre des mesures de la SNPC;

f. veiller à ce que la mise en œuvre des mesures de la SNPC tienne compte de la politique de gestion des risques menée par la Confédération, de la stratégie nationale de protection des infrastructures critiques et des stratégies informatiques du Conseil fédéral.

Art. 10 Comité pour la sécurité informatique

1 Le comité pour la sécurité informatique (C-SI) se compose d'un représentant du Centre national pour la cybersécurité (NCSC[6]), des délégués à la sécurité informatique des départements et de la Chancellerie fédérale et du délégué à la sécurité informatique des services standard.

2 Il peut faire appel à d'autres personnes à titre consultatif.

3 Il est présidé par le représentant du NCSC.

4 Il est l'organe consultatif du NCSC pour les questions de sécurité informatique dans l'administration fédérale.

Art. 11 Délégué à la cybersécurité

1 Le délégué à la cybersécurité assume les tâches suivantes:

a. diriger le NCSC;

b. veiller à une coordination optimale des travaux interdépartementaux des domaines de la cybersécurité, de la cyberdéfense et de la poursuite pénale de la cybercriminalité;

c. assurer la visibilité des activités de la Confédération dans le domaine des cyberrisques, contribuer à la création de conditions favorables à l'innovation dans le secteur de la cybersécurité, assumer le rôle d'interlocuteur de référence de la Confédération en matière de cyberrisques et représenter celle-ci au sein des commissions et groupes de travail concernés; veiller à une coordination optimale des travaux des cantons et de la Confédération afin d'assurer la protection de la Suisse contre les cyberrisques;

d. représenter le NCSC dans les états-majors de crise de la Confédération;

e. édicter des directives en matière de sécurité informatique;

6 National Cyber Security Centre

f. décider de dérogations aux directives qu'il a édictées; si ces dérogations concernent également les directives informatiques de l'Unité de pilotage informatique de la Confédération (UPIC), consulter cette dernière au préalable.

2 Il informe régulièrement le DFF, à l'intention du Conseil fédéral, de l'état de la sécurité informatique au sein des départements et de la Chancellerie fédérale.

3 Il peut participer à l'élaboration de directives informatiques de l'administration fédérale qui concernent la cybersécurité et à des projets informatiques ayant une incidence sur la sécurité. Il peut notamment demander des informations, se prononcer à ce sujet et formuler des modifications.

4 Il peut demander, après consultation du Contrôle fédéral des finances, des vérifications de la sécurité informatique.

Section 2 Organes du domaine de la cybersécurité

Art. 12 Centre national pour la cybersécurité

1 Le NCSC est le centre de compétences de la Confédération en matière de cyberrisques et coordonne les travaux de la Confédération dans le domaine de la cybersécurité. Il assume les tâches suivantes:

a. exploiter le guichet unique suisse en matière de cyberrisques, qui centralise les notifications émanant de l'administration fédérale, des milieux économiques, des cantons et de la population, les analyse et peut émettre des recommandations;

b. fournir, en collaboration avec les partenaires compétents au sein de l'administration fédérale, un appui subsidiaire aux exploitants d'infrastructures critiques et encourager entre eux l'échange d'informations concernant les cyberrisques;

c. diriger l'équipe d'intervention en cas d'urgence informatique (*Computer Emergency Response Team*, GovCERT), qui est le service spécialisé national pour la gestion technique des cyberincidents, l'analyse des questions techniques, l'évaluation technique des menaces et l'appui technique au guichet unique suisse;

d. diriger le service spécialisé de sécurité informatique de la Confédération, qui élabore des directives en matière de sécurité informatique, conseille les unités administratives lors de leur application et vérifie le niveau de sécurité informatique au sein des départements et de la Chancellerie fédérale;

e. désigner les délégués à la sécurité informatique de la Confédération (DSIC);

f. coordonner la mise en œuvre de la SNPC, effectuer un contrôle de gestion stratégique de la SNPC et préparer les séances du Groupe Cyber et du CP SNPC;

g. disposer d'un pool d'experts chargés d'assister les offices spécialisés dans la mise en œuvre de mesures de la SNPC ainsi que dans le développement, la mise en œuvre et l'évaluation de normes et de réglementations en matière de cybersécurité;

h. contribuer à sensibiliser l'administration fédérale et le grand public aux cyberrisques au moyen d'informations ciblées, informer sur l'état de la situation et publier des instructions sur les mesures préventives ou réactives à prendre;

i. exploiter une infrastructure d'analyse et de communication résiliente qui fonctionne indépendamment du reste de l'informatique de la Confédération;

j. informer le Groupe Cyber des cyberincidents et, lorsque ceux-ci sont importants du point de vue de la politique extérieure et de la politique de sécurité, en informer également le Groupe Sécurité de la Confédération.

2 Il peut traiter les données relatives aux cyberincidents et aux flux de communication correspondants pour autant que ce traitement soit utile, directement ou indirectement, à la protection de l'administration fédérale contre les cyberrisques. Il peut communiquer ces données à des équipes de sécurité publiques ou privées si:

a. le fournisseur des données y consent; et

b. aucune obligation légale de garder le secret n'est enfreinte.

3 La communication de données personnelles à l'étranger n'est autorisée que si la législation fédérale sur la protection des données est respectée.

4 Les données sensibles ne peuvent être traitées que si une base légale autorise leur traitement par des moyens informatiques de la Confédération.

5 En concertation avec les services concernés de l'administration fédérale, le NCSC prend la haute main sur la gestion des cyberincidents présentant une menace pour le bon fonctionnement de l'administration fédérale. Le cas échéant, il assume les tâches et compétences suivantes:

a. il peut obtenir des fournisseurs et des bénéficiaires de prestations concernés toutes les informations nécessaires;

b. il peut ordonner des mesures d'urgence;

c. il informe de son action la direction des unités administratives concernées

6 Si les mesures prises à la suite d'un cyberincident ont permis de réduire à un niveau acceptable la menace pour la confidentialité ou le fonctionnement de l'administration fédérale et que les travaux de suivi nécessaires et leur financement ont été arrêtés, le NCSC rend la responsabilité de la gestion aux services concernés.

Art. 13 Départements et Chancellerie fédérale

1 À la fin de chaque année, les départements et la Chancellerie fédérale informent le NCSC de l'état de la sécurité informatique.

2 Les fournisseurs de prestations internes visés aux art. 23 et 24 OIAF[7] rendent régulièrement compte au NCSC des failles de sécurité et des cyberincidents détectés ainsi que des mesures prises ou prévues pour y remédier.

3 Les départements et la Chancellerie fédérale désignent chacun un délégué à la sécurité informatique (DSID).

Art. 14 Unités administratives et fournisseurs de prestations

1 Les unités administratives désignent chacune un délégué à la sécurité informatique (DSIO). L'UPIC désigne par ailleurs un délégué à la sécurité informatique des services standard.

2 Les unités administratives sont responsables de la protection de leurs systèmes informatiques, de leurs applications et de leurs données (éléments protégés). Elles assument les fonctions suivantes:

a. examiner régulièrement les éléments protégés et prendre les mesures de sécurité nécessaires; veiller notamment à ce que ces mesures soient consignées sous une forme actualisée pour chaque élément protégé;

b. s'assurer du respect des directives en matière de sécurité informatique et des décisions du Conseil fédéral, du NCSC et des départements ou de la Chancellerie fédérale dans leurs domaines de compétences respectifs;

c. sous réserve de l'art. 12, al. 5, gérer tout cyberincident touchant les éléments protégés;

d. s'assurer qu'en cas d'acquisition de prestations auprès d'un fournisseur externe, les directives en matière de sécurité informatique font partie intégrante du contrat;

e. vérifier de manière appropriée que les directives en matière de sécurité informatique sont respectées par les fournisseurs externes.

3 Les fournisseurs veillent à disposer des capacités nécessaires pour gérer les cyberincidents qui se produisent chez eux et chez les destinataires des prestations.

4 Ils informent sans délai les destinataires des prestations des failles et des incidents de sécurité détectés.

5 Les destinataires des prestations définissent en collaboration avec les fournisseurs un processus de gestion des cyberincidents. Celui-ci règle en particulier les compétences décisionnelles dont relèvent les mesures d'urgence.

6 Si un cyberincident ne peut être géré dans le cadre du processus défini, les personnes concernées informent le NCSC afin de définir la marche à suivre.

7 Les unités administratives consultent le NCSC pour ce qui concerne les directives et projets informatiques ayant une incidence sur la sécurité.

8 Elles sont responsables du développement, de la mise en œuvre et de l'évaluation de normes et de réglementations en matière de cybersécurité dans leurs secteurs

7 RS **172.010.58**

respectifs. Le NCSC met à leur disposition, dans la mesure de ses possibilités, des experts du pool visé à l'art. 12, al. 1, let. g.

Chapitre 4 Dispositions finales

Art. 15 Modification d'autres actes

La modification d'autres actes est réglée en annexe.

Art. 16 Disposition transitoire relative à l'art. 2, let. b

[1] Les autorités et offices qui, avant l'entrée en vigueur de la présente ordonnance, se sont engagés par le biais d'un accord avec l'UPIC à respecter les dispositions de l'OIAF[8] sont soumis jusqu'au 31 décembre 2021 aux obligations de la présente ordonnance dans la mesure de la réglementation actuelle.

[2] Ils sont soumis à la présente ordonnance à partir du 1er janvier 2022 pour autant que l'accord n'ait pas été résilié avant cette date.

Art. 17 Disposition transitoire relative à l'art. 11, al. 1, let. e

[1] Si l'UPIC a édicté des directives en matière de sécurité informatique et approuvé des dérogations à ces directives avant l'entrée en vigueur de la présente ordonnance, ces directives et dérogations conservent leur validité.

[2] Le NCSC décide des éventuelles modifications des directives et des dérogations à ces directives.

Art. 18 Entrée en vigueur

La présente ordonnance entre en vigueur le 1er juillet 2020.

8 RS **172.010.58**

Annexe
(art. 15)

Modification d’autres actes

Les ordonnances suivantes sont modifiées comme suit:

...[9]

9 Les mod. peuvent être consultées au RO **2020** 2107.