Ordonnance Souveraine n° 8.504 du 18 février 2021 portant application de l'article 24 de la loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique

Type	Texte réglementaire
Nature	Ordonnance Souveraine
Date du texte	18 février 2021
Publication	Journal de Monaco du 26 février 2021[1 p.6]
Thématiques	Nouvelles technologies de l'information et de la communication ; Lutte contre le terrorisme et le crime organisé ; Défense, paix et sécurité

Vu la loi n° 975 du 12 juillet 1975 portant statut des fonctionnaires de l'État, modifiée ;

Vu la loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives, modifiée ;

Vu la loi n° 1.383 du 2 août 2011 pour une Principauté numérique, modifiée ;

Vu la loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale ;

Vu la loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique ;

Vu l'Ordonnance Souveraine n° 6.365 du 17 août 1978 fixant les conditions d'application de la loi n° 975 du 12 juillet 1975, modifiée, susvisée ;

Vu l'Ordonnance Souveraine n° 16.605 du 10 janvier 2005 portant organisation des Départements ministériels, modifiée ;

Vu Notre Ordonnance n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée ;

Vu Notre Ordonnance n° 5.664 du 23 décembre 2015 créant l'Agence Monégasque de Sécurité Numérique, modifiée ;

Vu Notre Ordonnance n° 6.526 du 16 août 2017 portant application des articles 35 et 36 de la loi n° 1.383 du 2 août 2011, modifiée, pour une Principauté numérique ;

Vu Notre Ordonnance n° 7.997 du 12 mars 2020 portant création de la Direction des Plateformes et Ressources Numériques ;

Vu Notre Ordonnance n° 8.099 du 16 juin 2020 fixant les conditions d'application de la loi n° 1.383 du 2 août 2011 pour une Principauté numérique, modifiée, relative aux services de confiance ;

Vu Notre Ordonnance n° 8.337 du 5 novembre 2020 relative aux données de santé à caractère personnel produites ou reçues par les professionnels et établissements de santé ;

Article 1er

L'autorité administrative spécialisée dénommée « Agence Monégasque de Sécurité Numérique » (A.M.S.N.) est placée sous l'autorité directe du Ministre d'État.

Article 2

L'Agence Monégasque de Sécurité Numérique est l'autorité nationale en charge de la sécurité numérique des systèmes d'information.

À ce titre, elle :

a) constitue un centre d'expertise, de réponse et de traitement en matière d'attaques numériques et a, en particulier, pour missions de prévenir, détecter et traiter les cyberattaques, notamment par l'élaboration de plans, de procédures, plus généralement, de toutes mesures à proposer au titre de la sécurité des systèmes d'information ;

b) propose au Ministre d'État les mesures destinées à répondre aux crises affectant ou menaçant la sécurité des systèmes d'information ;

c) anime et coordonne les travaux interministériels en matière de sécurité des systèmes d'information ;

d) élabore les mesures de protection des systèmes d'information proposées au Ministre d'État, conformément à l'article 24 de la loi n° 1.435 du 8 novembre 2016, susvisée. Elle veille à l'application des mesures adoptées, conformément à l'article 27 de la loi n° 1.435 du 8 novembre 2016, susvisée ;

e) mène des contrôles sur les systèmes d'information des services de l'État et des opérateurs publics ou privés, avec la collaboration de la Direction des Plateformes et des Ressources Numériques en ce qui concerne les opérateurs de communications électroniques exploitant de réseau ou fournisseur de services de télécommunications ou d'accès à Internet, conformément à l'article 28 de la loi n° 1.435 du 8 novembre 2016, susvisée ;

f) met en œuvre des dispositifs de détection qualifiés des événements susceptibles d'affecter la sécurité des systèmes d'information de l'État, des services publics et des opérateurs publics et privés, conformément à l'article 27 de la loi n° 1.435 du 8 novembre 2016, susvisé et coordonne la réaction à ces événements. Lorsque l'Agence Monégasque de Sécurité numérique, à la demande d'un opérateur, public ou privé, met en œuvre des dispositifs de détection qualifiés des événements susceptibles d'affecter la sécurité de ses systèmes d'information, elle conclut une convention d'assistance avec ledit opérateur lui permettant d'exploiter les systèmes de détection ;

g) recueille les informations techniques relatives aux incidents affectant les systèmes d'information des entités mentionnées à l'alinéa précédent. Elle peut apporter son concours pour répondre à ces incidents conformément à l'article 25 de la loi n° 1.435 du 8 novembre 2016, susvisée ;

h) représente la Principauté dans les instances internationales de sécurité numérique et auprès des autres centres d'expertise, de réponse et de traitement en matière d'attaques numériques ;

i) participe aux négociations internationales en matière de sécurité numérique et assure la liaison avec ses homologues étrangers ;

j) sensibilise et incite les services publics et les opérateurs publics et privés aux exigences de la sécurité numérique.

Article 2 bis

Créé par l'Ordonnance Souveraine n° 10.350 du 25 janvier 2024

L'Agence Monégasque de Sécurité Numérique est organisée autour de deux pôles de compétences, comme suit :

- le Pôle Expertise, spécifiquement chargé des missions définies aux lettres *c)*, *d)*, *e)* et *j)* de l'article 2 ainsi qu'aux articles 3 et 4 ;
- le « *Centre de réponse et de traitement en matière d'attaques numériques* » ou « *CERT-MC* » composé des trois divisions suivantes :
  - la division en charge de la supervision et de la détection des événements de sécurité numérique ou « *Security Operations Center* » (SOC-MC) ;
  - la division en charge de la réponse aux incidents de sécurité numérique ou « *Computer Security Incident Response Team* » (CSIRT-MC) ;
  - la division en charge de l'analyse et du partage et de l'information ou « *Information Sharing and Analysis Center* » (ISAC-MC).

Les missions du Centre de réponse et de traitement en matière d'attaques numériques sont déterminées par arrêté ministériel.

Article 3

L'Agence Monégasque de Sécurité Numérique a également pour mission de se prononcer sur la sécurité des dispositifs et des services, offerts par les prestataires, nécessaires à la protection des systèmes d'information.

Elle est en particulier chargée :

a) de mettre en place, actualiser et publier la liste des prestataires de services de confiance qualifiés ainsi que les informations relatives aux services qu'ils fournissent, dénommée « liste de confiance » ;

b) de mettre en place, si besoin, un service de certification électronique pour les services de l'État, la Commune, les personnes physiques ou morales portées aux répertoires et registres tenus par les services de l'État, en tant que prestataire de services de confiance conformément à l'Ordonnance Souveraine n° 8.099 du 16 juin 2020, susvisée ;

c) de l'instruction de la délivrance d'autorisations et de la gestion des déclarations relatives aux moyens et aux prestations de cryptologie prévues par l'Ordonnance Souveraine n° 6.526 du 16 août 2017, modifiée, susvisée ;

d) de l'instruction de la délivrance et du retrait des autorisations prévues à l'article 28-9 de la loi n° 1.383 du 2 août 2011, modifiée, susvisée ;

e) de l'élaboration des fonctions de sécurité prévus au titre IV de l'Ordonnance Souveraine n° 3.413 du 29 août 2011, modifiée, susvisée.

Article 4

Aux fins d'assurer l'accomplissement des missions définies à l'article 3, l'Agence Monégasque de Sécurité Numérique peut notamment :

a) analyser les rapports d'évaluation de la conformité des prestataires de services de confiance qualifiés et des services de confiance qualifiés ;

b) informer d'autres organes de contrôle et le public d'atteintes à la sécurité ou de pertes d'intégrité ;

c) procéder à des audits ou demander à des organismes compétents d'effectuer une évaluation de la conformité des prestataires de services de confiance qualifiés et des services de confiance qualifiés ;

d) vérifier l'existence et l'application de dispositions relatives au plan d'arrêt d'activité lorsque le prestataire de services de confiance qualifié cesse son activité ;

e) vérifier l'existence et l'application de dispositions relatives au plan d'arrêt de service lorsque le prestataire de services de confiance qualifié cesse de fournir un service de confiance qualifié ;

f) exiger que les prestataires de services de confiance remédient à tout manquement aux obligations fixées par arrêté ministériel.

Article 5

L'Agence Monégasque de Sécurité Numérique est chargée de concevoir, réaliser, mettre en œuvre et exploiter, en tous lieux et en tout temps, les moyens classifiés de communications électroniques de l'État.

Article 6

Modifié par l'Ordonnance Souveraine n° 10.350 du 25 janvier 2024

L'Agence Monégasque de Sécurité Numérique est dirigée par un directeur, ayant qualité de chef de service au sens de la loi n° 975 du 12 juillet 1975, modifiée, susvisée. Le directeur a en outre pour mission :

a) l'évaluation, la certification, et la qualification des produits de sécurité ;

b) la qualification des prestataires de services de confiance et des services de confiance (PSCO) ;

c) la qualification des prestataires d'audit de la sécurité des systèmes d'information (PASSI) ;

d) la qualification des prestataires de réponse aux incidents (PRIS) ;

e) la qualification des prestataires de détection d'incidents de sécurité (PDIS) ;

f) la qualification des prestataires d'informatique en nuage et d'hébergement (PINH) ;

g) la qualification d'hébergeur de données de santé à caractère personnel ;

h) la certification de sécurité des dispositifs de création et de vérification de signature électronique conformément à l'Ordonnance Souveraine n° 8.099 du 16 juin 2020, susvisée ;

i) la qualification d'hébergeur de données de santé à caractère personnel conformément à l'Ordonnance Souveraine n° 8.337 du 5 novembre 2020, susvisée ;

j) la qualification des Prestataires de Vérification d'Identité à Distance (PVID) ;

k) la qualification des Prestataires d'Administration et de Maintenance Sécurisées (PAMS) ;

l) la qualification des Prestataires d'Accompagnement et de Conseil en Sécurité des systèmes d'information (PACS).

Les modalités d'évaluation, de certification et de qualification des produits de sécurité ainsi que les conditions de délivrance de la qualification des divers prestataires sont déterminées par arrêté ministériel.

Le directeur assure en outre toutes autres missions qui lui sont confiées par des dispositions légales ou réglementaires.

Il est assisté d'un directeur adjoint qui le supplée en cas d'absence ou d'empêchement.

Article 7

Modifié par la loi n° 1.565 du 3 décembre 2024

Aux fins d'assurer l'accomplissement des missions définies aux articles 2, 3, 4 et 6, le directeur peut mettre en œuvre des traitements, automatisés ou non, d'informations nominatives permettant l'identification, par tous procédés techniques et /ou moyens informatiques, des personnes et des biens, dans le respect des dispositions de la loi n° 1.565 du 3 décembre 2024.

Lesdits traitements ont la qualité de traitements de sécurité publique au sens de la loi précitée.

Le directeur est tenu de prendre toutes mesures utiles, au regard de la nature des données, pour préserver leur sécurité en empêchant, notamment, qu'elles soient déformées ou endommagées et pour veiller à ce qu'elles soient inaccessibles à des tiers non autorisés.

Seuls les personnels dûment et spécialement habilités par le directeur peuvent accéder aux données figurant dans les traitements d'informations nominatives susmentionnés.

L'habilitation précise les traitements auxquels elle autorise l'accès.

L'accès aux traitements fait l'objet d'une traçabilité sous la forme d'une journalisation périodique conservée par le responsable du traitement au sens de la loi n° 1.565 du 3 décembre 2024, pendant dix ans.

Le directeur est tenu d'assurer la mise à jour des données et de veiller, selon les besoins, à ce qu'elles soient complétées, rectifiées ou effacées.

Article 8

Les données figurant dans les traitements d'informations nominatives mentionnés à l'article précédent peuvent être transmises, conformément à des engagements internationaux exécutoires dans la Principauté, à des organismes de coopération de sécurité numérique ou à des services d'États étrangers dans le respect des dispositions des articles 20 et 20.1 de la loi n° 1.165 du 23 décembre 1993, modifiée, susvisée, compétents en matière de prévention ou de répression d'infractions relatives à la sécurité numérique.

L'Agence Monégasque de Sécurité Numérique peut, quant à elle, recevoir des données contenues dans les traitements d'informations nominatives mis en œuvre par des organismes ou des services et conformément aux engagements internationaux mentionnés au précédent alinéa.

Article 9

Des textes réglementaires déterminent en tant que de besoin les conditions d'application de la présente ordonnance.

Article 10

Dans les ordonnances souveraines, les arrêtés ministériels et règlements actuellement en vigueur, les termes : « Ordonnance Souveraine n° 5.664 du 23 décembre 2015 créant l'Agence Monégasque de Sécurité Numérique, modifiée » sont remplacés par le titre de la présente ordonnance.

Les références aux dispositions de l'Ordonnance Souveraine n° 5.664 du 23 décembre 2015 créant l'Agence Monégasque de Sécurité Numérique, modifiée, sont remplacées, s'il y a lieu, par des références à des dispositions de la présente ordonnance.

Article 11

Notre Secrétaire d'État, Notre Secrétaire d'État à la Justice, Directeur des Services Judiciaires et Notre Ministre d'État sont chargés, chacun en ce qui le concerne, de l'exécution de la présente ordonnance.

Notes

Liens

1. Journal de Monaco du 26 février 2021
   ^ [p.1] https://journaldemonaco.gouv.mc/Journaux/2021/Journal-8527