ARTICLE

JURIDIQUE

L'ESSENTIEL

- L'évolution des outils numériques et l'émergence de l'IA augmentent les vulnérabilités des associations face aux violations de données et aux cyberattaques.
- La directive NIS 2 et le RIA imposent de nouvelles obligations de sécurité et de transparence susceptibles de s'appliquer aux structures associatives.

NUMÉRIQUE

CYBERSÉCURITÉ ET INTELLIGENCE ARTIFICIELLE : LES ENJEUX DE DEMAIN

À l'ère du numérique, les structures associatives ne sont pas épargnées par l'augmentation des risques cyber, auxquels s'ajoutent les nouveaux enjeux liés à l'intelligence artificielle (IA). Retour sur ces risques et sur les outils de conformité à disposition des associations aujourd'hui.

AUTEUR Gabrielle Lambert
TITRE Avocate à la Cour, cabinet Seban avocats

AUTEUR Louise Flament
TITRE Stagiaire, cabinet Seban avocats

AUTEUR Audrey Lefèvre
TITRE Avocate associée, cabinet Seban avocats

Avec la généralisation des outils numériques, les associations doivent aujourd'hui composer avec des enjeux de cybersécurité de plus en plus importants et parfois transformés, notamment par l'émergence de l'intelligence artificielle (IA)[1]. Si près de 90 % des cyberattaques trouvent encore leur origine dans une erreur humaine, les nouveaux risques liés à l'IA rappellent combien la mise en place de bonnes pratiques internes et de mesures de sécurité et de conformité respectueuses des nouveaux textes réglementaires est essentielle.

LA GESTION DES RISQUES CYBER DANS LES STRUCTURES ASSOCIATIVES

Dans un contexte numérique en constant développement, les associations doivent se responsabiliser face aux risques cyber. La protection des données devient un impératif stratégique, nécessitant la mise en conformité avec la réglementation en la matière et, plus généralement, une culture de la sécurité numérique au sein des organisations.

Panorama des risques cyber dans le monde associatif

Les risques cyber désignent l'atteinte des systèmes d'information et de l'ensemble des données informatisées, de quelque nature que ce soit. Au sein des associations, les données peuvent être personnelles – la Commission nationale de l'informatique et des libertés (CNIL) les définissant comme « toute information se rapportant à une personne physique identifiée ou identifiable » –, non personnelles (mais stratégiques) et peuvent dans certains cas être des données sensibles – notamment pour les associations qui interviennent dans les secteurs social et médico-social. Une violation de

1. V. *JA* 2025, n° 713, p. 16 et s., dossier « Intelligence artificielle – Big Bang théorie ».
2. Dir. (UE) 2022/2555 du 14 déc. 2022.
3. Dir. (UE) 2016/1148 du 6 juill. 2016.
4. L. n° 2018-133 du 26 févr. 2018, *JO* du 27.
5. Sur la définition d'entité : dir. (UE) 2022/2555, préc., art. 6, point 38 ; sur la qualification d'entité essentielle et importante : dir. (UE) 2022/2555, préc., art. 3. Les entités essentielles sont les grandes entreprises (plus de 250 salariés et/ou plus de 50 millions d'euros de chiffre d'affaires annuel) qui font partie des « secteurs hautement critiques » (santé, énergie, transport, etc.) ainsi que les deux cas particuliers des infrastructures numériques et des administrations publiques. Les entités importantes sont les moyennes entreprises (plus de 50 salariés et/ou plus de 10 millions d'euros de chiffre d'affaires annuel total) qui font partie des « secteurs hautement critiques » ainsi que les moyennes et grandes entreprises qui font partie des

■ Les associations sont encouragées à se responsabiliser en adoptant des chartes, codes de conduite et normes volontaires.

ces données peut être définie comme tout incident de sécurité ayant comme conséquence de compromettre leur intégrité, leur confidentialité ou leur disponibilité (ou les trois), résultant tant d'une erreur humaine involontaire que d'une cyberattaque.
La violation de la confidentialité des données se traduit par la divulgation de celles-ci à des personnes non autorisées. Elle peut résulter d'actes malveillants (communication volontaire des données des adhérents) ou d'erreurs (partage accidentel via un Wi-Fi public, par exemple).
L'atteinte à l'intégrité des données se traduit quant à elle par l'altération de la fiabilité des données et de leur exactitude – par exemple, l'altération des informations médicales des résidents d'un établissement d'hébergement pour personnes âgées dépendantes (Ehpad) – et a le plus souvent pour conséquence l'atteinte à la disponibilité – lorsque les données sont rendues inaccessibles. Cette double atteinte peut survenir lors d'une suppression accidentelle par un prestataire informatique ou lors d'une attaque externe surchargeant le système d'information.
À noter qu'avec l'utilisation de l'IA, les cyberattaques sont de plus en plus fréquentes et puissantes.

Un cadre juridique en évolution

Les risques cyber présentent donc un enjeu majeur pour les associations, qui nécessitent, pour être maîtrisés, de se mettre en conformité avec les différents textes en vigueur, mais aussi d'adopter des bonnes pratiques au sein de leur organisation.
En matière de cybersécurité, la directive NIS 2[2] (pour *Network and Information Security Directive*) est venue mettre à jour la directive NIS 1[3] transposée en droit français par la loi du 26 février 2018[4]. Face à l'augmentation et à la sophistication des cyberattaques, cette directive, adoptée en décembre 2022, élargit son champ d'application aux « entités essentielles » et « importantes », pouvant inclure les associations loi 1901 ayant une activité économique si elles remplissent les critères définis[5].
Afin d'aider les acteurs concernés dans la compréhension de la directive, l'Agence nationale de la sécurité des systèmes d'information (Anssi) a mis à disposition, sur son site Internet « MonEspaceNIS2 »[6], un simulateur permettant aux organisations – d'ores et déjà et même si le texte de transposition de la directive n'a pas encore été adopté[7] – de déterminer si elles relèveront ou non de cette réglementation. Les associations concernées devront mettre en place des mesures de sécurité appropriées (notamment la rédaction de politiques relatives à l'analyse des risques et à la sécurité des systèmes d'information), procéder au signalement rapide des incidents graves de cybersécurité (dans les 24 heures, auprès de l'Anssi[8]), procéder à l'évaluation régulière des risques ou encore sensibiliser leurs collaborateurs[9].
Si une entité associative n'est pas assujettie à la directive NIS 2, elle n'en reste toutefois pas moins exposée aux risques cyber. Il est donc indispensable qu'elle mette en œuvre des mesures adaptées et, pour ce faire, utilise les dispositions prévues pour les entités dites « importantes » de la directive NIS 2 comme lignes directrices à suivre pour la protection de son système d'information et de ses données – les deux types d'entités ont les mêmes obligations en matière de sécurité, mais la supervision est plus légère pour les entités importantes que pour les entités essentielles[10].
De surcroît, l'Anssi encourage la responsabilisation en fournissant des guides de bonnes pratiques. Les associations sont ainsi invitées à sensibiliser leurs membres, renforcer leurs mesures techniques et élaborer un plan de réponse aux incidents.
Enfin, en cas de violation de données, des obligations de notification s'imposent. La loi dite « Lopmi »[11] oblige toute organisation victime d'une cyberattaque à porter plainte dans les 72 heures pour être indemnisée par son assureur. Pour les violations de données à caractère personnel, un signalement à la CNIL est obligatoire, ainsi qu'une information aux personnes concernées si nécessaire[12]. En fonction du secteur d'activité, les associations pourront en outre être amenées à notifier la violation à d'autres autorités. C'est le cas notamment des établissements et services sociaux et médico-sociaux (ESSMS) qui devront informer leurs autorités de tutelle (agences régionales de santé, départements, préfectures, etc.). À titre d'illustration, les ESSMS et lieux de vie et d'accueil (LVA) ont l'obligation d'informer « de tout dysfonctionnement grave dans leur gestion ou leur organisation susceptible d'affecter la prise en charge des usagers, leur accompagnement ou le respect de leurs droits et de tout événement ayant pour effet de menacer ou de compromettre la santé, la sécurité ou le bien-être physique ou moral des personnes prises en charge ou accompagnées »[13]. ●●●

« autres secteurs critiques » (recherche, production, transformation et distribution des denrées alimentaires, etc.).
6. monespacenis2.cyber.gouv.fr.
7. Le projet de loi de transposition est arrivé le 11 mars 2025 sur le bureau du Sénat en première lecture, avant d'être transféré à l'Assemblée nationale, qui l'examinera en mai-juin.
8. Dir. (UE) 2022/2555, préc., art. 23.
9. *Ibid.*, art. 21 (un référentiel d'exigences en matière de cybersécurité sera publié par l'Anssi pour préciser la mise en œuvre opérationnelle de ces mesures).
10. *Ibid.*, cons. 122 : « les entités importantes ne devraient [...] pas être tenues de documenter systématiquement le respect des exigences en matière de gestion des risques de cybersécurité [...] ».
11. L. n° 2023-22 du 24 janv. 2023, *JO* du 25.
12. Règl. (UE) n° 2016/679 du 27 avr. 2016, art. 33.
13. CASF, art. L. 331-8-1, art. R. 331-8 à R. 331-10 ; pour les ESSMS : CSP, art. R. 1413-67 à R. 1413-78.

●●● LA NÉCESSITÉ D'ENCADRER L'INNOVATION APPORTÉE PAR LE DÉVELOPPEMENT DE L'IA

L'arrivée de l'IA offre de nouvelles perspectives pour les associations, transformant leurs modes de fonctionnement traditionnels en assistant les organisations dans des tâches variées et parfois complexes.
Dans le secteur médico-social, l'IA propose des applications promettant l'amélioration de la qualité des plannings hospitaliers et leur automatisation, ou encore l'assistance à la rédaction dans le cadre de la transformation numérique des dossiers d'usagers informatisés (DUI). Les projets de recherche (partenariats et consortiums) bénéficient également de ces avancées en développant des outils performants grâce aux algorithmes et à la fouille de données. Ces nouvelles utilisations de l'IA impliquent également des enjeux et risques, notamment en matière de cybersécurité.

Les nouveaux risques introduits par l'IA

L'émergence de l'IA ouvre de nouvelles perspectives en cybersécurité, mais révèle aussi des vulnérabilités critiques. Les attaques peuvent désormais cibler directement les systèmes d'IA, en manipulant des algorithmes ou en introduisant des données malveillantes dans les données d'entraînement, compromettant la fiabilité des systèmes et obligeant les organisations à repenser leurs stratégies de protection.
La gestion des données représente un autre défi majeur. Les associations doivent naviguer entre plusieurs normes juridiques : données personnelles – soumises au règlement général sur la protection des données (RGPD)[14] –, données non personnelles stratégiques et secret des affaires. Tout fichier traité par une IA nécessite une vigilance accrue pour éviter les fuites.
Au-delà des enjeux cyber, l'IA questionne sur d'autres sujets divers. Ainsi, la propriété intellectuelle devient un terrain complexe avec les IA génératives. Qui est propriétaire des contenus produits : l'association, le développeur de l'IA ou l'outil lui-même ? Les données utilisées en entrée comme en sortie soulèvent également des questions juridiques inédites. Une organisation produisant un rapport ou un document stratégique via une IA générative peut-elle revendiquer un droit d'auteur ? Les conditions d'utilisation des différentes plateformes d'IA devraient être vérifiées avant toute souscription par l'organisation.
Enfin, les biais éthiques des systèmes d'IA – qui reproduisent, par exemple, des stéréotypes et génèrent des informations erronées ou proposent des analyses biaisées – constituent, dans le milieu associatif, et plus particulièrement les secteurs sensibles du social et du médico-social ou dans l'accompagnement de publics vulnérables, des enjeux qui nécessitent un encadrement strict.

Intégrer dans les organisations une utilisation conforme de l'IA

L'utilisation de l'IA s'inscrit dans un écosystème juridique préexistant (RGPD, Data Act[15], droit de la propriété intellectuelle et droit commun de la responsabilité) complété par le règlement IA (RIA)[16] entré en application le 1er août 2024, qui encadre spécifiquement ces nouveaux outils. Il propose une approche graduée basée sur l'évaluation des risques, classant les systèmes d'IA (SIA) en différentes catégories de risque (risque inacceptable dont les SIA sont interdits, haut risque, risque limité, risque minimal) et imposant des obligations proportionnées. L'objectif est de garantir la sécurité, la transparence et la protection des droits fondamentaux tout en favorisant l'innovation technologique européenne. Les associations doivent porter une attention particulière aux systèmes d'IA à haut risque[17], notamment dans les domaines de la justice, la défense, la santé, l'éducation et la finance, qui sont soumis à des exigences renforcées : autoévaluation de conformité, documentation technique sur la gestion des risques et des obligations de transparence, ce qui implique un contrôle humain indispensable[18].
Une obligation générale de transparence est également requise pour les systèmes d'IA à risque limité, ce qui inclut l'identification du contenu généré par IA.
Pour les IA à risque minimal, le RIA encourage les organisations à développer leurs propres chartes et codes de conduite, approche qui est d'ailleurs pertinente pour l'ensemble des systèmes d'IA utilisés.
Cette responsabilisation volontaire est également encouragée par la mise en place de normes internationales, notamment l'ISO/IEC 42001:2023, première norme dédiée à la gestion de la sécurité des systèmes d'IA. Visant à établir des systèmes sécurisés et éthiques, elle pourrait devenir un standard de référence malgré son caractère encore non contraignant.
Au regard des mesures citées ci-dessus, l'Union européenne se distingue dans le panorama mondial des régimes juridiques applicables aux technologies numériques par une approche réglementaire unique. Là où les États-Unis privilégient la déréglementation et où la Chine impose un contrôle strict, l'Europe fait le pari de la responsabilisation des acteurs. Sa stratégie vise à concilier innovation et protection des droits individuels, en plaçant l'éthique et la transparence – deux valeurs cardinales pour les associations – au cœur de la transformation numérique. ■

14. Règl. (UE) n° 2016/679, préc. ; v. *JA* 2018, n° 571, p. 16 et s., dossier « Gestion et administration – Règlement général pour données personnelles ».
15. Règl. (UE) n° 2023/2854 du 13 déc. 2023.
16. Règl. (UE) n° 2024/1689 du 13 juin 2024.
17. *Ibid.*, art. 6.
18. Pour les SIA à haut risque : règl. (UE) n° 2024/1689, préc., art. 14 et 26 ; pour les SIA avec obligation de transparence : règl. (UE) n° 2024/1689, préc., art. 50.