Cyberattaques en série : le sport français face à l'obligation de passer à la sécurité numérique renforcée

---

Deux mois après une première attaque ayant visé les données de 3,5 millions de foyers, le ministère des Sports vient de reconnaître une nouvelle « exfiltration de données » touchant cette fois la plateforme Forômes, dédiée à la gestion des formations, candidats et diplômes de l'animation et du sport. Près de 450 000 candidats voient ainsi exposer leurs informations personnelles (identité, adresses, dates de naissance, numéros de téléphone) en raison du piratage d'un compte légitime d'un organisme de formation, dont les accès ont été immédiatement désactivés.

Au-delà du fait divers technico-administratif, cet incident marque un tournant : le ministère reconnaît désormais « le caractère systémique des cyberattaques » dans le champ sportif et annonce le renforcement de ses dispositifs de cybersécurité, ainsi qu'un accompagnement des fédérations avec l'appui de l'ANSSI. Le signal est clair : la sécurité numérique devient une composante structurante de la gouvernance sportive, au même titre que l'intégrité des compétitions ou la lutte contre le dopage.

Du piratage isolé au risque systémique

Le ciblage répété du ministère des Sports illustre une évolution : le sport n'est plus seulement un « client » secondaire des menaces cyber, mais un secteur prioritaire pour les attaquants. Après les systèmes de l'État, ce sont les fédérations – voile, natation, golf, tennis – et leurs bases de données qui sont directement visées. La volumétrie des données (licenciés, encadrants, officiels, candidats aux diplômes), leur caractère sensible et les interconnexions croissantes entre systèmes (plateformes de formation, de billetterie, de résultats, de suivi médical ou disciplinaire) en font des cibles attractives.

Le cas Forômes est emblématique : une plateforme centrale, à la croisée des politiques publiques de formation et de l'écosystème sportif marchand, compromise via le piratage d'un compte autorisé. Juridiquement, cela renvoie à la question du contrôle effectif des accès, des habilitations, de la traçabilité et du partage de responsabilité entre l'État, les organismes de formation et, en bout de chaîne, les structures sportives bénéficiaires.

Responsabilité publique et devoir de sécurisation

En annonçant qu'il « prend pleinement ses responsabilités » et qu'il renforcera ses dispositifs, le ministère acte implicitement que les obligations de sécurité ne peuvent plus être appréhendées comme de simples clauses techniques, mais comme un pilier de la politique sportive. La référence explicite à l'ANSSI ouvre la voie à une normalisation accrue des pratiques : audits, référentiels de sécurité, segmentation des systèmes d'information, gestion des identités et des habilitations, procédures de réponse à incident.

Plusieurs axes de vigilance se dessinent :

- l'articulation entre les obligations de sécurité pesant sur l'État responsable de traitements et celles pesant sur les opérateurs et prestataires (fédérations, ligues, clubs, organismes de formation) ;

- la qualification des incidents (violation de données à caractère personnel, atteinte à un service essentiel, impact sur la continuité de missions de service public sportif) et les notifications afférentes ;

- la mise à niveau contractuelle des relations entre ministère, fédérations et prestataires numériques (hébergement, SaaS, infogérance) pour intégrer des exigences de cybersécurité vérifiables et sanctionnables.

Fédérations et écosystème sportif : de la prise de conscience à la conformité

Le ministère rappelle que plusieurs fédérations ont déjà été confrontées à des cyberattaques et annonce sa volonté de les accompagner dans une démarche de sécurisation. Pour l'économie du sport, cette évolution est structurante : le coût de la non-sécurisation (interruption de compétitions, indisponibilité de systèmes de gestion des licences, fuite de données de licenciés ou de partenaires) devient potentiellement supérieur à celui de l'investissement préventif.

Dans un environnement où la donnée est au cœur des modèles économiques (billetterie dynamique, CRM fans, sponsoring et data marketing, paris sportifs, contenus OTT), la cybersécurité devient un élément de valorisation – ou de dévalorisation – des droits sportifs. Les acteurs les plus exposés (ligues professionnelles, grands événements, plateformes numériques sportives) seront évalués non seulement sur leurs audiences, mais aussi sur la robustesse de leurs infrastructures numériques et la qualité de leur gestion des incidents.

Vers une culture de la « compliance cyber » dans le sport

L'affaire Forômes pourrait ainsi servir de catalyseur à l'émergence d'une véritable « compliance cyber » dans le sport français : cartographie des risques numériques, politiques de sécurité unifiées, formation des personnels, clauses contractuelles standardisées, mutualisation de certains outils et expertises sous l'égide de l'État ou d'instances fédérales.

Cette mutation ouvre un besoin nouveau de conseil et de structuration : revue des conventions entre ministère et fédérations, accompagnement des grands évènements et des clubs dans l'élaboration de leurs politiques de cybersécurité, intégration des exigences cyber dans les cahiers des charges d'organisation, dans les appels d'offres technologiques et dans les contrats de sponsoring.

Le sport, longtemps en retard sur ces sujets, n'a plus le luxe de considérer les cyberattaques comme des épisodes exceptionnels. À l'heure où le ministère des Sports reconnaît leur caractère systémique et annonce un renforcement de ses défenses, la question n'est plus de savoir si le secteur doit se transformer, mais à quelle vitesse et avec quel niveau d'exigence juridique, technique et éthique.

François Lhospitalier (Of Counsel - Economie du sport) – BCTG Avocats