# Performance physique individuelle : les règles d'or pour protéger les données des athlètes

**Par Stéphanie SAULNIER**
Juriste, service de l'emploi, des solidarités, du sport et de l'habitat,
Direction de l'accompagnement juridique,
Commission nationale de l'informatique et des libertés (CNIL)

Améliorer et optimiser sa performance physique individuelle sont des exigences attendues d'un sportif professionnel ou d'un athlète de haut niveau.

Les acteurs de l'écosystème sportif français ont recours à des dispositifs de mesure de la performance physique individuelle de leurs athlètes. Ces dispositifs permettent de recueillir de multiples données, dont des données de santé, intégrées à des bases de données « performance ». La réglementation sur la protection des données personnelles (Règlement général sur la protection des données et loi « Informatique et Libertés ») encadre leur traitement.

## Introduction

Améliorer et optimiser sa performance physique individuelle[1] sont des exigences attendues d'un sportif professionnel ou d'un athlète de haut niveau.

C'est pourquoi les acteurs de l'écosystème sportif français (fédérations sportives, clubs sportifs professionnels, ligues professionnelles, CREPS[2], institutions[3]) ont recours à des dispositifs de mesure de la performance physique individuelle de leurs athlètes.

Ces dispositifs prennent la forme d'objets connectés commercialisés, parfois même expérimentaux (exemple : ceintures, montres, gilets, balances connectés). Ils permettent de recueillir de multiples données telles que la distance parcourue, la vitesse maximale, le contact au sol, la longueur de foulée, le suivi de la cadence. Selon les contextes, d'autres données en particulier de santé comme la fréquence cardiaque, le poids, la taille, les résultats de tests sanguins ou urinaires, l'examen des os, la répartition de la fibre musculaire, les blessures sont également collectées. Toutes sont intégrées à des bases de données « performance ».

[1] La mesure de la performance physique individuelle des sportifs se distingue des statistiques concernant l'activité sportive des joueurs (statistiques sur les données de jeux). Par exemple, dans le domaine du football, le nombre de buts marqués, le nombre de cartons rouges, le nombre de minutes jouées, le total de passes décisives, le nombre de matchs joués, le nombre de fautes, etc.).

[2] CREPS : Centre de Ressources d'Expertise et de Performance Sportive.

[3] Exemple : Agence nationale du Sport (ANS), INSEP (Institut national du sport, de l'expertise et de la performance), Maisons régionales de la Performance, etc.

Ces bases, *via* des statistiques, ont pour objet d'estimer la « médaillabilité » des athlètes, d'apprécier leur état de forme, d'adapter les programmes d'entraînement, d'identifier leurs points forts / leurs points faibles, s'il convient ou non de les faire participer à des compétitions ou tournois, etc. Ainsi, dans les faits, elles contiennent de multiples informations personnelles sur les athlètes, notamment des données sensibles.

La réglementation sur la protection des données personnelles (Règlement général sur la protection des données (RGPD) et loi « Informatique et Libertés ») encadre leur utilisation.

Alors, comment garantir une place sur le podium, dans la course de la mise en conformité ?

## Sélectionner le meilleur entraîneur : le délégué à la protection des données

Dans la plupart des cas, tout organisme de l'écosystème sportif français mettant en place une base de données « performance » doit disposer de l'expertise d'un délégué à la protection des données.

Son rôle ? Piloter la conformité de l'organisme au RGPD (même s'il n'en est pas responsable[4]), et ce pour l'ensemble des traitements mis en œuvre au sein de cet organisme.

Une attention toute particulière doit être accordée à sa désignation puisque le niveau d'expertise du délégué doit être proportionné à la sensibilité des données traitées. Rappelons que de nombreuses données de santé sont recensées dans les bases de données « performance » : le délégué doit donc contribuer à intégrer dans les projets les spécificités de la réglementation applicable sur ce sujet.

La première étape sera d'identifier la personne qui dispose des connaissances et des compétences nécessaires pour exercer cette fonction : connaissance de la législation en matière de protection des données personnelles, de la sécurité des systèmes d'information et de la réglementation sectorielle. Une bonne connaissance de l'écosystème sportif français est également indispensable puisque le délégué doit être en capacité d'interagir avec l'ensemble des métiers intervenant sur ce type de projet (exemple : entraîneur, préparateur physique, membres du staff médical, représentant des organismes).

Le délégué doit être particulièrement endurant. Il doit en principe être associé, d'une manière appropriée et en amont, à tous les projets impliquant des traitements de données.

Comme tout athlète, le délégué doit disposer d'un bon équipement ! Il doit bénéficier de moyens matériels et organisationnels, de ressources et du positionnement lui permettant d'assurer ses missions.

[4] Même si le délégué à la protection des données a un rôle majeur dans la mise en conformité d'un organisme, il n'en est pas responsable. Sur ce point, *cf. infra*.

# Respecter les règles du jeu : les dispositions du RGPD et de la loi « Informatique et Libertés »

## Lors de la collecte des données de performance des athlètes, le rôle des acteurs de l'écosystème doit être identifié

Pour chacune des bases de données « performance », il convient de déterminer l'organisme qui concrètement assume la responsabilité de la bonne application des règles en matière de protection des données (le responsable de traitement). Il s'agit, ici, d'identifier celui qui dispose d'un pouvoir décisionnel dans la création de ces bases c'est-à-dire celui qui a défini le « pourquoi » et le « comment » ? Il faut ainsi savoir si d'autres organismes ont par exemple contribué au choix d'un outil « sur étagère » acquis auprès d'un prestataire externe et, si tel est le cas, formaliser cette relation.

En pratique, la ligne de partage entre le statut de responsable de traitement et celui d'autres acteurs intervenant dans les projets « performance » (responsable conjoint de traitement, sous-traitant, fournisseur externe d'une solution) peut parfois être délicate à fixer. La qualification doit intervenir au terme d'une analyse concrète des modalités de mise en œuvre de la base de données « performance » par son créateur.

## La collecte des données doit être licite, loyale et transparente

Pour pouvoir être créée et mise en œuvre, une base de données « performance » doit reposer sur l'une des « bases légales » du RGPD (fondement juridique). Elle donne le droit à l'organisme de traiter les données. Son choix est une étape clé ; elle prend en compte la nature de l'organisme responsable du traitement, le secteur d'activité, l'objectif général poursuivi, etc. Par exemple, les fédérations sportives délégataires peuvent s'appuyer sur la mission d'intérêt public pour fonder leurs bases de données « performance »[5].

Par ailleurs, les athlètes doivent recevoir une information concise, claire et accessible concernant la constitution de ces bases. L'information délivrée doit notamment leur permettre de savoir pour quelles raisons les données recueillies lors des entraînements et compétitions sont collectées, de comprendre l'usage qui en est fait, de faciliter l'exercice de leurs droits. Par exemple, il n'est pas possible de faire porter un capteur à un athlète sans lui délivrer une information conforme au RGPD[6].

## Les données sont collectées pour des finalités déterminées, explicites et légitimes

Les motifs de la collecte des données, c'est-à-dire l'objectif poursuivi, doivent être portés à la connaissance des athlètes, avant que les données ne soient intégrées à une base. Ces derniers doivent être en mesure de comprendre l'utilisation qui sera faite de leurs

[5] Les bases de données « performance » des fédérations délégataires sont constituées en application, d'une part, des contrats de performance passés avec l'Agence nationale du Sport en soutien de leur projet de performance fédérale et, d'autre part, des contrats de délégation passés avec le ministère chargé des Sports (actuel ministère des Sports et des Jeux Olympiques et Paralympiques).

[6] Sur ce point, voir les articles 12 et 13 du RGPD.

données. Exemple : estimer les chances de médailles, adapter la charge d'entraînement, prévenir les risques de blessure, etc.

Les données ne peuvent être réutilisées à d'autres fins, comme par exemple la lutte contre le dopage.

## Seules les données strictement nécessaires peuvent être collectées (principe de minimisation)

De nombreuses données individuelles, dont des données de santé, sont recueillies en pratique.

Par exemple, étudier la motricité des articulations de l'épaule d'un nageur permettra à l'entraîneur de savoir s'il doit compenser une « moindre performance » par un meilleur palmage au niveau des jambes. À ce titre, les résultats de cette étude sont bien nécessaires. En revanche, savoir si une athlète est sous contraceptif, le type de contraception ou encore la marque du contraceptif est à exclure.

Selon la CNIL, la collecte des données de santé des sportifs professionnels ou de haut niveau, dans un but d'amélioration ou d'optimisation de leur performance physique individuelle, se justifie par la notion d'intérêt public important[7]. L'adoption d'un texte encadrant les bases de données « performance » apporterait les garanties exigées par le RGPD[8].

## Les données doivent être conservées pour une durée strictement nécessaire

Selon les cas d'usage, des durées différentes de conservation peuvent être retenues. La durée de carrière de l'athlète pourra notamment être prise en compte.

## Des mesures de sécurité appropriées doivent être mises en place

Par exemple, il convient de limiter les accès aux bases de données « performance ». C'est ainsi que des personnels administratifs exerçant au sein des maisons régionales de la performance ne sont pas autorisés, au titre des dispositifs d'aide à la reconversion professionnelle, à accéder aux données de santé des athlètes.

## Suivre un entraînement intensif

Les acteurs de l'écosystème sportif français doivent être en mesure de démontrer, à tout moment, la conformité de leurs bases de données « performance » aux exigences du RGPD.

[7] L'intérêt public important (art. 9-2-g) du RGPD) est la seule exception de l'article 9 du RGPD qui pourrait fonder la collecte de données de santé dans ce contexte. Le code du sport attribue un rôle particulier à certains acteurs dans le domaine du sport de haut niveau et le développement de la performance, comme les fédérations sportives délégataires et les CREPS. Même si le consentement du sportif est utilisé en pratique, il ne semble pas adapté au cas particulier du sport professionnel ou de haut niveau (le consentement du sportif n'étant pas libre, spécifique, éclairé et univoque).

[8] L'article 9-2-g) du RGPD fonde le traitement des données de santé si ce « traitement est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée ».

Ils doivent tracer toutes les démarches entreprises et conserver tous les documents supports attestant de cette conformité.

Cette documentation repose notamment sur l'inscription de cette base dans le registre recensant les traitements. Elle doit comporter l'analyse d'impact relative à la protection des données menées (AIPD), les procédures d'encadrement de l'information des athlètes ainsi que les contrats définissant les rôles et responsabilités de la chaîne des acteurs traitant des données (sous-traitants, responsables conjoints).

La démarche de documentation des traitements est essentielle (cartographie de la base de données, identification des points de difficultés potentiels, priorisation des actions à mener, etc.). Chacun doit s'y exercer ardemment !

Et l'esprit d'équipe sera de rigueur… En effet, selon les modalités de mise en œuvre des bases de données « performance », il conviendra de définir et de formaliser l'ensemble des obligations respectives incombant à chaque acteur pour assurer la conformité au RGPD. Par exemple, dans l'hypothèse où des analyses telles que des séquençages pour étudier les faiblesses posturales seraient réalisées par un organisme extérieur au donneur d'ordre, les relations entre ces deux organismes devront être définies dans une convention.

## Éviter les blessures : le risque élevé pour les droits et libertés des athlètes concernés

Le RGPD impose la réalisation d'une AIPD pour tout traitement susceptible d'engendrer « un risque élevé » pour les droits et libertés des personnes concernées.

En pratique, il sera bien difficile de ne pas considérer qu'une base de données « performance » ne soit pas concernée par cette obligation. En effet, de telles bases réunissent au moins deux des critères pour lesquels l'AIPD[9] est obligatoire : collecte de données de santé ou hautement personnelles, collecte de données à large échelle, personnes vulnérables[10], profilage, usage de nouvelles technologies.

[9] Afin de faciliter la conduite et la formalisation d'analyses d'impact relatives à la protection des données, la CNIL propose un logiciel *open source* PIA et une méthodologie, *cf*. https://www.cnil.fr/fr/RGPD-analyse-impact-protection-des-donnees-aipd

[10] Tant les sportifs de haut niveau que les sportifs professionnels peuvent être assimilés à des personnes vulnérables :

- les premiers parce qu'il existe toute une procédure d'inscription sur une liste nationale qui prend « en compte la corrélation performances / "médaillabilité" » (source site web du ministère des Sports et des Jeux Olympiques et Paralympiques) ;
- les seconds parce qu'ils sont dans un lien de subordination avec leur employeur.

Par ailleurs, l'on peut facilement imaginer que le refus de remplir un formulaire de collecte des données d'entraînement pourrait conditionner la participation à la sélection opérée par un entraîneur, son inscription sur la liste des sportifs de haut niveau, etc.

## Ne pas oublier qu'il existe un arbitre : la CNIL

En France, la CNIL est l'autorité supervisant le bon déroulement du match (la réglementation) : elle peut contrôler les organismes. Si un manquement est constaté, elle peut les mettre en demeure ou même distribuer des cartons rouges (les sanctions[11]).

## Conclusion : et pour quelle récompense à l'arrivée ?

Une vie des athlètes bien plus protégée…

On le voit bien, le RGPD permet de construire des bases de données « performance » plus respectueuses de la vie privée, dès leur conception, et surtout d'être en capacité de le démontrer.

Mais pas seulement…

Dans un contexte grandissant de cyberattaques, les exigences du RGPD limitent les violations de données susceptibles de concerner des athlètes de renommée internationale ou du moins amoindrissent leurs effets potentiels. Une divulgation intempestive d'informations personnelles pourrait avoir des répercussions fort dommageables sur les résultats d'une compétition et, plus largement, sur la carrière d'un athlète. Et, le respect du RGPD sera toujours un atout…

Alors, prêt à franchir la ligne d'arrivée ?

[11] Différentes sanctions peuvent être prononcées par la CNIL : rappel à l'ordre, injonction de se mettre en conformité, assortie le cas échéant d'une astreinte, limitation temporaire ou définitive du traitement ou son interdiction, retrait d'une autorisation, retrait d'une certification, etc. Pour plus d'informations sur ces sanctions, *cf.* https://www.cnil.fr/fr/cnil-direct/question/sanctions-quelles-sanctions-peuvent-etre-prononcees-par-la-cnil