Comment les startups femtechs gèrent-elles les données de santé des utilisatrices ?

DÉCRYPTAGE - Alors que les femtechs s'efforcent de combler les lacunes médicales concernant la santé des femmes, la question de la confidentialité des données émerge comme un élément crucial. Les startups du secteur adoptent des stratégies rigoureuses pour sécuriser les données sensibles de leurs utilisatrices.

Temps de lecture : minute

27 mai 2024

La recherche médicale a longtemps été axée sur le corps masculin, considéré comme la norme. De fait, il existe encore aujourd'hui une importante lacune scientifique en ce qui concerne la santé des femmes, et de nombreuses maladies qui les affectent principalement, voire exclusivement, demeurent méconnues. Pour combler cette dette scientifique, sensibiliser les femmes aux problèmes qui les concernent, prévenir les maladies et parfois les guérir, l'écosystème a vu émerger de nombreuses femtechs.

Au cœur de leur proposition de valeur et de leur développement se trouve généralement la donnée. *« Tous les rapports convergent : il existe un manque criant de données sur la santé des femmes. La collecte de données est cruciale pour comprendre l'incidence de certaines pathologies et l'efficacité des traitements. Les femtechs représentent une réponse essentielle à cette problématique, offrant une perspective sans surmédicalisation »*, estime Juliette Mauro, présidente et membre fondatrice de Femtech France. Delphine Moulu, directrice générale de l'association, complète : *« Elles contribuent à la recherche sur la santé*

féminine en participant à de multiples études publiées dans des revues scientifiques et en collaborant étroitement avec des universités de renom. Femtech France a d'ailleurs établi un partenariat stratégique avec l'APHP pour stimuler l'innovation en matière de santé féminine au sein des hôpitaux. »

Les données d’une femtech canadienne spécialisée dans les sextoys connectés piratées

Néanmoins, si l’émergence de ces startups provoquent l’enthousiasme, elle suscite aussi des inquiétudes quant à la collecte des données de santé. *« La préoccupation de certaines utilisatrices découle selon moi de l’adage “si un service est gratuit, alors tu es le produit” »*, explique Emeline Hahn, CEO de Fizimed, une entreprise femtech qui adresse, entre autres, la problématique des fuites urinaires en proposant une sonde connectée. Pour l’entrepreneuse, la protection des données des femmes est cruciale : *« C’est un sujet dont j’ai pris conscience dès les débuts de Fizimed. Et pour cause, alors que nous démarrions l’activité, une femtech canadienne qui commercialisait des sextoys connectés avait vu ses données piratés, permettant aux cyber attaquants de savoir qui utilisait quoi et à quelle fréquence. »*

Vigilantes, les startups du secteur doivent donc l’être. Généralement dirigées par des femmes, elles-mêmes utilisatrices d’applications ou de dispositifs médicaux connectées, les femtechs françaises semblent particulièrement bonnes élèves, mais soulignent que se mettre en conformité représente un coût non négligeable.

Avoir les reins solides dès le début pour

gérer les données

« Chez Fizimed, nous avons, en interne, un expert IT et gestion des données. C'est nécessaire dès le démarrage où il y a un gros travail de qualification des données au regard de la CNIL et du RGPD. Il n'est pas évident au début de distinguer celles qui sont considérées comme sensibles, celles qui relèvent de la santé. Ça coûte cher. Il faut avoir les reins solides », affirme Emeline Hahn.

Une vision partagée par Chloé Bonnet, CEO de Lyv, une solution web d'autogestion des symptômes de l'endométriose, qui a évolué vers une application mobile en novembre dernier. *« Nous travaillons avec une société de conseil, Data Need Advice. La protection des données n'était pas notre première expertise à l'origine de Lyv, il faut savoir dès le départ ce qu'on ne sait pas et tout de suite s'entourer. Elle a cette connaissance de la santé et de la recherche qu'il nous fallait*, explique l'entrepreneuse avant de poursuivre. *En opposition à d'autres secteurs, nous préférons prendre le temps et faire de la protection des données notre cœur de mission. En l'intégrant by design, c'est structurant pour tous les sujets. »*

A la tête d'une startup en early stage, Chloé Bonnet reconnaît les défis inhérents à des ressources potentiellement limitées : *« Ce n'est pas toujours évident. Il faut prévoir ce poste de dépense dès le premier business plan. »*

Héberger local et bannir les interconnexions

Parmi les premières préoccupations qui surgissent figure celle de l'hébergement. *« La différence majeure à souligner lorsqu'il s'agit de données de santé est que, selon la loi américaine, la donnée appartient à celui qui la produit, tandis que selon le RGPD, appliqué en Europe, les données appartiennent à l'émetteur, donc à l'utilisatrice. Les utilisatrices doivent avant tout regarder la politique de confidentialité des applications*

femtechs qu'elles souhaitent utiliser, pour savoir où sont hébergées les données et ce à quoi elles vont servir », explique Juliette Mauro, présidente de Femtech France.

Cette réalité nécessite donc pour les entrepreneurs un benchmark rigoureux. «*Pour notre toute première preuve de concept, nous voulions une plateforme d'apprentissage pour pouvoir tester notre méthode et notre arbre de création de contenus qui soit à la fois ergonomique, bien faite, stable, tout en veillant à garder la main sur nos données. Nous voulions à minima un hébergement européen - c'était d'ailleurs une recommandation CNIL. Ça n'a pas été une mince affaire : nous avons fait un benchmark de plus de 50 solutions et avons opté pour un hébergeur Européen HDS. Depuis le passage à l'app, nous avons fait le choix de Scalingo, un hébergeur strasbourgeois et HDS, nous en sommes très heureux. Nos données sont sensibles et il s'agit là aussi de souveraineté !* », explique la CEO de Lyv.

Malo - appli femtech référencée sur Mon Espace Santé -, qui redonne à chaque parent le pouvoir d'agir sur sa santé et celle de son enfant et adresse des sujets comme la dépression post-partum a, elle aussi, jeté son dévolu sur Scalingo. *« Ils sont français, et nous avons à cœur de défendre une souveraineté dans la protection de la donnée. Nous avons toujours eu un bon niveau de relation avec eux »*, explique Madhu Desbois, COO chez Malo.

L'interconnexion avec d'autres solutions ou appareils connectés est aussi, et pour toutes, à bannir. *« C'est du bon sens que de ne pas mettre du Facebook Connect partout »*, estime Chloé Bonnet. Et pour cause, une enquête de l'ONG Privacy International révélait en 2020 que de nombreuses applications transféraient automatiquement les données de ses usagers à Facebook au travers du Software Development Kit, un outil fourni par la société aux développeurs pour faciliter l'intégration de fonctionnalités Facebook dans leurs applications. Juliette Mauro souligne

qu'*« aujourd'hui, les mises à dispositions de données dans les États interdisant l'avortement aux États-Unis ont été le fait en grande majorité des Gafam, ou des sites pharmaceutiques de ventes de médicaments en ligne. Le risque vient en priorité de ses grands acteurs de données et moins des femtechs. »*

Pour une sécurité accrue et une confidentialité renforcée et parce que son produit le permet, Fizimed a fait le choix de stocker les données utilisateurs directement sur l'appareil, plutôt que sur des serveurs distants. *« On ne récupère que des données anonymisées. On ne peut donc pas faire le lien entre une personne et l'usage fait de la sonde. Par ailleurs, aucune donnée ne remonte dans le cloud. C'est, de fait, plus sécurisé, mais les données ne sont accessibles que sur l'appareil où elles sont stockées. »* Une option de stockage bienvenue pour Fizimed qui a percé le marché allemand, où les consommateurs sont plus regardant sur la gestion de leurs données que les Français : *« Certaines cultures sont plus sensibles que d'autres. L'internationalisation nous permet de le constater. Une communication claire et transparente est encore plus nécessaire en Allemagne »*, analyse Emeline Hahn.

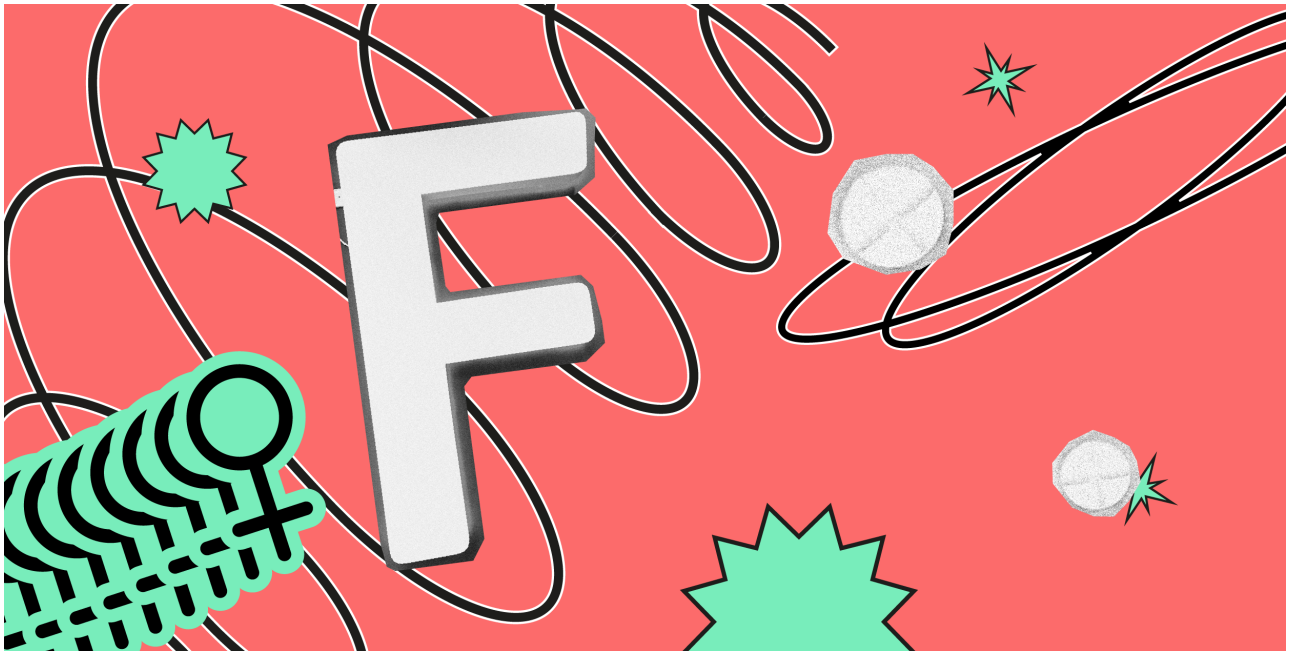
Décentraliser le sujet

Pour Madhu Desbois, l'acculturation de l'équipe d'une startup peut devenir un levier de sensibilisation et il est nécessaire de décentraliser le sujet de la sécurisation des données sensibles dans l'organisation. *« Dans notre process d'onboarding, sans exception, dans les deux mois après leur arrivés, les collaborateurs doivent suivre une formation de sensibilisation RGPD chez Malo. On ne peut pas construire une stratégie marketing, produit ou tech sans avoir une acculturation. On se doit d'être exigeant avec nous même pour construire une relation de confiance avec les parents qui utilisent Malo. »*

Même son de cloche chez Lyv : *« Quand notre responsable R&D lance une*

étude, le sujet de la protection des données est abordé dès le départ. Ça doit être décliné par tout le monde et sur tous les champs. C'est le cœur de la mission. On travaille pour des personnes potentiellement vulnérables, le cadre réglementaire est là pour protéger, il ne s'agit pas de cocher des cases. »

Elle espère que tous les nouveaux arrivants dans le secteur de la femtech prendront la mesure de la responsabilité qui leur incombe. *« Quand tu fais partie des pionniers sur un sujet, tu dois faire les choses proprement pour ne pas jeter l'opprobre sur toute une filière, c'est une grande responsabilité. »* Pour se mettre en conformité et dans la perspective d'un contrôle de la CNIL, elles peuvent compter sur l'aide de Femtech France : *« Notre rôle est, entre autres, de les accompagner sur ces questionnements là. Nous invitons régulièrement des représentants du ministère de la Santé, comme la délégation du numérique en santé, pour les y sensibiliser »*, conclut Juliette Mauro.



À lire aussi
10 startups de la FemTech à suivre en 2023

MADDYNEWS

La newsletter qu'il vous faut pour ne rien rater de l'actualité des startups françaises !

JE M’INSCRIS

Article écrit par Astrid Briant