

Quelle réponse des FinTech face à la réglementation générale sur la protection des données ?

Par Julien ROCHET, R&D Manager, bureau de Luxembourg, Jivway S.A. et Loris BERGERON, C.O.O. de D.CONSULTING

En réponse à une longue série de scandales financiers, des mesures réglementaires dont les préceptes ont été définis par le GAFI (Groupe d'action financière), régissent l'ensemble de la place. Au-delà des exigences de fonds propres qui sont désormais imposées aux établissements financiers, la législation a fortement évolué ces 20 à 30 dernières années et les professionnels du secteur sont aujourd'hui plus que jamais confrontés à une vigilance accrue des autorités de surveillance et de contrôle.

Des réglementations visant à protéger les investisseurs et les individus d'une manière générale sont venues compléter ces législations. L'une des dernières en date est le GDPR «General Data Protection Regulation». Ce règlement européen protège les données personnelles des individus et concerne tous les secteurs d'activités. Il est question de placer le client final au cœur de toutes les préoccupations. Ainsi, la sphère financière n'y échappe pas et ses institutions ont dû s'adapter à ce nouvel environnement réglementaire : elles ont changé leurs habitudes de travail et ont adapté leur gestion de la relation client.

En parallèle, l'émergence des FinTech – ces start-ups taxées de chanceler les business models traditionnels des institutions financières en place – a très vite été associée à la mise sur le marché d'une toute nouvelle forme de concurrence pour les banques. Ces entreprises technologiques n'en sont pourtant pas moins devenues des partenaires de choix pour les professionnels de la place en se positionnant comme une réponse technologique à ces obligations légales auxquelles ils doivent faire face. L'environnement réglementaire s'est ainsi offert aux FinTech comme une



opportunité d'étendre leur champ d'intervention. Il est vrai que jusqu'alors, l'innovation financière portait davantage sur l'élaboration de produits financiers complexes que sur la gestion des risques et la préservation de l'intégrité du système financier. L'exploitation et la gestion analytique des données financières sont depuis devenues le propre des FinTech. Ce faisant, elles ont élargi leur offre de services et se sont exprimées au-delà de l'élaboration de produits financiers. Elles offrent des services personnalisés traitant des volumes importants de données provenant de sources diverses et variées (données personnelles, bancaires, composition de portefeuille boursier, gestion de la relation client...)

A l'ère du big data et de l'échange automatique d'informations (FATCA, CRS), la mise en place de workflows d'activités et documentaires ainsi que la définition d'algorithmes de calcul pour une meilleure optimisation de la gestion des risques sont autant de sujets sur lesquels les FinTech ont su se positionner et sans



lesquels les institutions financières ne peuvent évoluer. A ce titre, les FinTech sont soumises aux réglementations internationales concernant la protection et le traitement des données personnelles de leurs utilisateurs.

Une forte capacité d'adaptation

Les réglementations comme le GDPR peuvent effectivement avoir des conséquences structurelles importantes sur l'organisation et le fonctionnement des FinTech. Elles peuvent avoir des conséquences financières lourdes en cas de non-respect de la loi, les sanctions pouvant aller de 2% à 4% du chiffre d'affaires mondial de la société. Cette appréhension des peines encourues pousse les FinTech à s'adapter rapidement à ces réglementations. Malgré une croissance exponentielle sur l'ensemble des marchés, les entreprises technologiques font preuve d'une capacité accrue à proposer des services à fortes valeurs ajoutées tout en restant des entreprises à taille humaine. Elles réduisent ainsi considé-

rament l'inertie au changement et conservent une approche orientée «clients». Cette structuration de l'environnement interne (niveau microéconomique) permet une gestion complète et rapide dans la prise de décisions des opérations envers les employés, la vente, l'administration... mais également une diminution des risques stratégiques, tactiques et opérationnels (niveau macroéconomique) envers les fournisseurs, les partenaires et clients de la FinTech.

Ce sont ces choix organisationnels et économiques qui permettent à ces entreprises technologiques de réagir aux mutations légales tout en faisant preuve d'un degré élevé de perméabilité et de flexibilité au changement. Elles s'adaptent efficacement aux nouvelles réglementations et garantissent un service de qualité, conforme à la législation.

Quelle est l'influence de la réglementation dans la conception des produits des FinTech ?

Les FinTech, qu'elles soient éditrices de solutions de type Software as a Service (SaaS) ou de solutions clients lourds installées localement sur les ordinateurs des utilisateurs finaux, sont directement concernées par la réglementation GDPR. Au vu de la réglementation, elles doivent offrir aux utilisateurs une visibilité et un contrôle total sur les données personnelles tout en maîtrisant leur cycle de vie, cela afin de pouvoir les transmettre sur simple demande à l'individu concerné. Cela implique aux FinTech d'avoir une connaissance précise des données détenues, de leurs localisations, de l'objet de la collecte, de leur mode de gestion, de stockage, de transfert et d'effacement.

Dès la mise en place ou la conception d'un produit, la protection de la vie privée est au cœur de la réflexion. Cette logique de «Privacy by design» est introduite dans les spécifications initiales, dans la conception et l'architecture des systèmes technologiques d'information afin de faciliter les principes de protec-

tion des données (droit à la portabilité, destruction de l'intégralité des données sur simple demande, sécurité de l'information...).

Que ce soit dans le cas d'un produit hébergé dans le Cloud ou d'un client lourd, la notion de protection et de mise en sécurité des données est primordiale. L'accès aux systèmes peut être sécurisé par des méthodes d'authentification fortes grâce à la génération d'un mot de passe complexe à usage unique, l'utilisation d'une carte à puce, la mise en place d'une identification biométrique ou digitale...

Les bases de données qui stockent les informations relatives aux utilisateurs peuvent être hébergées dans des data centers appartenant à des acteurs locaux ou internationaux importants du secteur (Amazon AWS, Microsoft Azure, Alibaba Cloud Computing Service...). Outre la disponibilité de ces bases de données grâce à leur stockage simultané en différents endroits, elles doivent être protégées et peuvent être cloisonnées ou mutualisées à l'ensemble des clients. A titre d'exemple, les fonctionnalités telles que Transparent Data Encryption (TDE) ou Always Encrypted (AE) permettent de chiffrer les données pour les protéger contre les menaces d'activités malveillantes.

C'est face à ces problématiques et dans le contexte d'un monde en perpétuelle évolution aussi bien technologique que légale, mais aussi dans une démarche constante d'amélioration, que nous voyons naître de nouvelles synergies. En effet, si d'importants partenariats entre FinTech sont nés, leur collaboration avec des acteurs historiques implantés sur le marché financier depuis de nombreuses années est devenue nécessaire.

Ces associations ont pour objectif de créer de nouveaux pôles de compétences et d'expertises. Cela permet à l'ensemble des acteurs d'être en adéquation avec la législation et garantit un niveau maximal de protection des données sensibles.