Alors qu'Apple a accepté de stocker en Chine les données de ses utilisateurs chinois, Microsoft s'est opposé au Département américain de la justice qui souhaitait l'accès aux courriels d'un utilisateur dont le compte était hébergé en Irlande. Microsoft s'érige ainsi en militant de la protection, même si le Cloud Act américain a depuis entériné la possibilité des saisies de courriels à l'étranger. La Commission européenne suit la même voie.

Avec le scandale Cambridge Analytica, la question des données personnelles est revenue au premier plan, son importance étant signalée à intervalles réguliers quand des abus majeurs sont découverts, telle la précédente alerte planétaire en 2013 avec les révélations d'Edward Snowden sur les écoutes de la NSA. Il s'agit pourtant d'un enjeu quotidien pour les entreprises, confrontées aux pressions des pouvoirs politiques ou judiciaires comme à la nécessité d'entretenir la confiance de leurs utilisateurs grâce à un niveau élevé de protection de leurs données personnelles. Les relations compliquées de Microsoft et d'Apple avec respectivement les administrations américaine et chinoise désignent ces enjeux.

Apple est dépendant de la Chine qui constitue son deuxième marché au monde derrière les États-Unis. Et le groupe américain paye cher cette dépendance parce qu'il prend le risque d'abîmer en Chine l'image qu'il entend donner au monde. Ainsi, dans l'affaire Cambridge Analytica, Apple a critiqué Facebook et son choix en faveur de la gratuité, porte ouverte à l'exploitation des données personnelles. À l'inverse, en vendant très cher ses terminaux, Apple garantirait à ses utilisateurs que leurs données ne soient jamais revendues ou communiquées à autrui. Mais cette image de coffre-fort est trompeuse, Apple ayant dû céder à la Chine à plusieurs reprises.

Après que ses services iTunes Movie et iBooks ont été interdits sur le marché chinois en 2016, Apple a retiré en janvier 2017 l'application du *New York Times* de la version chinoise de l'AppStore, le quotidien new-yorkais violant la réglementation locale selon le porte-parole d'Apple en Chine. En tout, ce sont 670 applications qui ont été retirées de l'AppStore chinois en 2017. Mais il ne s'agit là que d'atteinte à la liberté d'expression. Un an plus tard, en janvier 2018, le quotidien économique japonais, le *Nikkei*, annonçait qu'Apple avait entamé des négociations exclusives avec Yangtze Memory, une filiale du groupe chinois Tsingua Unigroup, dont le capital est contrôlé par l'État chinois. Il s'agit pour Apple de remplacer Samsung et Toshiba par un fabriquant chinois de semi-conducteurs, un secteur stratégique pour le pouvoir politique chinois qui a fait de la maîtrise de ces technologies avancées une priorité.

Les iPhone pourront donc être contraints de fonctionner avec des composants chinois. Au moins alimenteront-ils à coup sûr les nouveaux centres de stockage d'Apple en Chine. La chose est entendue depuis le 1er juin 2017 et l'entrée en application de la nouvelle loi chinoise sur la cybersécurité, laquelle oblige les prestataires de services à stocker sur le territoire national les données des internautes chinois. Apple s'y est résolu et, depuis le 28 février 2018, transfère les données *iCloud* de ses utilisateurs chinois auprès d'un prestataire, Guizhou-Cloud Big Data, que contrôle le gouvernement de la province de

Ghizhou. Mais Apple a promis qu'*« aucune porte dérobée ne sera créée »* pour récupérer les données de ses utilisateurs, réitérant des positions déjà tenues aux États-Unis face aux demandes du FBI (voir *La rem* n°38-39, p.82). L'autre moyen d'accéder à un compte est d'en connaître la clé de sécurité. C'est ce que pourront plus facilement obtenir les autorités chinoises quand elles solliciteront le *data center* du Ghizhou en actionnant les possibilités juridiques offertes par la réglementation chinoise, quand jusqu'ici les autorités chinoises devaient se confronter au système juridique américain pour espérer accéder à un compte *iCloud.*

À l'évidence, les positions d'Apple à l'attention de ses utilisateurs chinois ne sont pas comparables à la ligne stratégique de Microsoft. L'entreprise s'est en effet engagée dans une croisade pour la protection des données personnelles des individus contre toute forme d'ingérence étatique. De ce point de vue, les ingérences russes dans la campagne présidentielle américaine ont rappelé à tous que l'internet est un nouveau champ de bataille traversé par des enjeux géopolitiques majeurs.

Depuis 2017, Microsoft milite ainsi pour une « Convention de Genève » du numérique qui obligerait les États à épargner les ordinateurs des « civils » en cas d'attaque informatique, qui inciterait également les entreprises technologiques à collaborer entre elles pour lutter contre les cyberattaques, qui initierait enfin la création d'une organisation non gouvernementale de coopération pour identifier l'origine des attaques informatiques. Ces origines, souvent difficiles à identifier, remontent la plupart du temps à des États, comme la Corée du Nord pour le virus WannaCry en mai 2017, ou encore la Russie pour le logiciel de *ransomware* NotPetya en juin 2017 (voir *La rem* n°44, p.50). Cet engagement de Microsoft en direction des utilisateurs individuels s'est traduit autrement aux États-Unis. En 2013, la justice américaine a demandé à Microsoft de lui autoriser un accès à la boîte Hotmail d'un trafiquant de drogues, demande à laquelle Microsoft s'est opposé, le compte Hotmail étant hébergé en Irlande. Pour Microsoft, donner suite à une demande de la justice américaine dans un territoire sous une autre juridiction aurait été ouvrir la boîte de Pandore qui allait conduire des États peu scrupuleux à solliciter l'accès aux boîtes *mails* localisées à l'étranger de leurs ressortissants ou opposants.

Le juge new-yorkais avait dès 2016 donné raison à Microsoft dans le contentieux l'opposant à la justice américaine. Depuis l'arrivée au pouvoir de Donald Trump, l'administration a relancé l'affaire devant la Cour suprême qui a entendu les arguments de Microsoft le 27 février 2018. Mais la Cour n'aura probablement pas à se prononcer, parce que la loi américaine encadre désormais ce type de requête des autorités policières. En effet, le 23 mars 2018, le Cloud Act a été signé, qui autorise le Département de la justice à passer des accords avec des pays partenaires afin de procéder à la récupération *d'e-mails,* mettant fin à l'incertitude juridique sur laquelle reposait le conflit avec Microsoft. Il reste que la loi américaine permet désormais la récupération des *e-mails* à l'étranger, certes dans le cas d'accords de partenariats qui peuvent toujours être fragiles, ce qu'a révélé la remise en cause du *« Safe Harbor »* par l'Europe en 2016 (voir *La rem* n°36, p.5), un accord qui portait justement sur les conditions de transfert des données personnelles entre l'Europe et les États-Unis.

La même logique prévaut en Europe afin de renforcer la lutte contre le crime organisé et le terrorisme. Le 17 avril 2018, la Commission européenne a présenté un projet de règlement sur les preuves électroniques autorisant les autorités judiciaires à demander à tout éditeur de services opérant en Europe des informations relatives aux données de connexion d'un suspect, l'éditeur ayant dix jours pour répondre et six heures en cas d'extrême gravité des faits. Si les données « d'utilisation », celles qui sont liées à la liste des services visités ou les durées de connexion ne nécessitent pas l'intervention du juge, les données de « contenus », comme les *e-mails* ou les vidéos postées, doivent faire l'objet préalable d'une requête d'un juge pour être transmises aux enquêteurs. Et le juge ne l'accordera qu'à la condition que le crime présumé soit passible d'au moins trois ans de prison. Ce type de mesures, en Europe comme aux États-Unis, vise à mettre fin tout à la fois à l'instabilité juridique en la matière et aux délais que cette dernière générait dans les enquêtes.

Sources :

- « En Chine, Apple censure l'application du New York Times », lemonde.fr avec AFP, 5 janvier 2017.
- « Apple pourrait commander ses mémoires à un groupe chinois », Yann Rousseau, *Les Echos*, 16 février 2018.
- « Microsoft se pose en champion de la cybersécurité », Lucie Ronfaut, *Le Figaro*, 20 février 2018.
- « Données : Apple se plie aux exigences de la Chine », Elsa Braun, *Le Figaro*, 27 février 2018.
- « États-Unis : Gafam et défenseurs de la vie privée devant la Cour suprême », Florian Dèbes, Nicolas Rauline, *Les Echos*, 28 février 2018.
- « Microsoft refuse de livrer les mails de ses clients aux autorités », Elsa Braun, *Le Figaro*, 1er mars 2018.
- « Justice Department asks Supreme Court to moot Microsoft email case, citing new law », Ellen Nakashima, washingtonpost.com, 31 mars 2018.
- « Bruxelles force les preuves électroniques », Derek Perrotte, *Les Echos*, 17 avril 2018.
- « L'Europe veut faciliter l'accès aux preuves en ligne », Lucie Ronfaut, *Le Figaro*, 18 avril 2018.