RÈGLEMENTATION EUROPÉENNE

Dora : quelles conséquences pour les prestataires de services informatiques ?

Afin de gérer les risques liés à l'utilisation des technologies de l'information dans le secteur financier, le règlement européen Dora va imposer aux prestataires informatiques qui travaillent avec des entités financières un nouvel environnement réglementaire et une collaboration avec les autorités financières.

Le règlement UE 2022/2554 du Parlement Européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier (Dora) entrera en vigueur le 17 janvier prochain. De la même façon que la réglementation bancaire cherche à gérer les risques liés à la solvabilité du secteur financier en imposant des ratios prudentiels et des « *stress tests* » réguliers, Dora cherche à gérer les risques liés à l'utilisation des technologies de l'information dans le secteur financier, en imposant aux divers acteurs de ce secteur de nouvelles obligations en matière de gouvernance, de prévention, de notification et de contractualisation. Ce dernier aspect concerne tout particulièrement les prestataires de services informatiques, qui vont devoir intégrer dans leurs contrats certaines clauses obligatoires et s'engager à participer aux tests de résilience opérationnelle organisés par leurs clients.

Le secteur financier est l'un des plus gros consommateurs de services informatiques, qui, comme le relève le deuxième considérant du préambule de Dora, a « *désormais acquis une importance cruciale dans l'exécution des fonctions quotidiennes typiques de toutes les entités financières* ». Ces services informatiques assurent de plus en plus souvent une interconnexion entre les 22 000 entités financières présentes dans l'Union Européenne et une défaillance localisée peut rapidement dégénérer en un incident systémique. Faisant le constat que le droit de l'Union européenne prend insuffisamment en compte ce risque systémique malgré les règles générales sur l'externalisation déjà prévues par le droit européen des services financiers, les autorités européennes ont donc décidé d'adopter un règlement avec un champ d'application très large (couvrant 20 types d'entités financières dont les établissements de crédit et de paiement, les entreprises d'investissement, les sociétés de gestion, les prestataires de services sur crypto-actifs, les entreprises d'assurance et de réassurance et les institutions de retraite professionnelle) afin de prévenir, gérer et réduire les risques liés à l'emploi des services de Technologies de l'Information et de la Communication (services TIC). Ce règlement touche donc tous les prestataires informatiques fournissant des services aux entités financières, mais de manière inégale selon le caractère critique ou non des services fournis et la part de marché du prestataire.

Obligations s'appliquant à tous les prestataires de services informatiques

Dora fait tout d'abord du contrat informatique un contrat formel, qui doit être conclu par écrit, sur papier ou de manière électronique. La sanction de l'absence de conclusion formelle d'un contrat est probablement la nullité, même si le texte du règlement ne le précise pas. Le texte de Dora semble également indiquer que tout contrat de services TIC doit inclure des niveaux de services, alors que leur intérêt pour tous les services TIC ne semble pas évident.

Selon Dora, tout contrat entre un prestataire de services informatique et une entité financière doit désormais comporter (i) une description claire des services fournis (avec l'indication, lorsque la sous-traitance d'un service TIC qui soutient une fonction critique ou importante est envisagée, des conditions applicables à une telle sous-traitance), (ii) des informations sur les lieux d'où les services seront fournis, y compris les lieux de stockage, (iii) une description des mesures concernant la disponibilité, l'authenticité, l'intégrité et la confidentialité des données, (iv) les conditions

de réversibilité en cas de résiliation du contrat ou cessation d'activité du prestataire, (v) la description des niveaux de service, y compris leurs conditions de mise à jour et révision, (vi) une obligation pour le prestataire de fournir une assistance en cas d'incident de service, gratuitement ou à un cout prédéterminé, (vii) une obligation de coopérer avec les autorités de tutelle de l'entité financière, (viii) une description des droits de résiliation et des délais de préavis minimaux pour la résiliation des accords contractuels, conformément aux attentes des autorités compétentes et (ix) les conditions de participation des prestataires aux programmes de sensibilisation à la sécurité et aux formations à la résilience opérationnelle élaborées par les entités financières. Ces clauses obligatoires imposent aux prestataires des obligations de transparence accrues. Elles ne préjugent pas des conditions commerciales qui seront négociées entre les parties, mais permettront aux entités financières d'avoir une meilleure visibilité concernant leurs niveaux de risques. Cependant, on peut s'interroger sur l'intérêt pour les autorités de tutelle de pouvoir définir des durées de préavis pour des services qui ne sont ni importants ni majeurs et sur celui de la sensibilisation de ces prestataires à la résilience opérationnelle de leurs clients.

Les contrats de services informatiques avec les entités financières font donc l'objet d'une véritable standardisation, qui sera renforcée par les clauses contractuelles types que les autorités sectorielles pourront adopter et auxquelles il sera très difficile aux prestataires informatiques de déroger. Les prestataires informatiques vont également devoir faire un réel effort avec leurs sous-traitants. En effet, les prestataires informatiques font généralement appel à une chaine complexe de sous-traitants pour l'hébergement et la maintenance de leurs services, avec lesquels ils ont souvent peu ou aucune marge de manœuvre de négociation, du fait de la taille de sous-traitants tels qu'AWS ou Azure. Cependant, puisque le règlement Dora affecte tous les prestataires informatiques d'un secteur intensément consommateur de ressources informatiques, il est à espérer que l'effet de masse qu'il induit fasse également évoluer les positions de ces géants de l'informatique vers plus de transparence.

Obligations s'appliquant aux prestataires de services critiques ou importants

Dora impose un niveau d'obligations plus élevé aux prestataires supportant des fonctions critiques ou importantes que sur les autres prestataires, ce qui est logique au vu de son objet.

Certains prestataires de services informatiques fournissant des services génériques, qui n'ont pas été spécialement développés pour l'industrie financière mais qui supportent, du fait de l'utilisation qui en est faite par le client, des services critiques ou importants, peuvent ainsi se retrouver soumis à des obligations plus importantes que ce qu'ils avaient initialement envisagé et devront soit cesser de contracter avec ces clients, soit se soumettre à ces obligations. De plus, il semble probable qu'au vu de la difficulté à définir concrètement ce qui est une fonction critique ou importante, les entités financières vont approcher une interprétation la plus large possible de cette définition, afin de se prémunir contre tout risque de non-conformité et d'utiliser l'avantage que les clauses obligatoires additionnelles leur donnent dans la négociation contractuelle.

Une fonction est définie dans Dora comme critique ou importante si sa « *perturbation est susceptible de nuire sérieusement à la performance financière d'une entité financière, ou à la solidité ou à la continuité de ses services et activités, ou une interruption, une anomalie ou une défaillance de l'exécution de cette fonction est susceptible de nuire sérieusement à la capacité d'une entité financière de respecter en permanence les conditions et obligations de son agrément, ou ses autres obligations découlant des dispositions applicables du droit relatif aux services financiers* ». Le caractère critique ou important d'une fonction dépend donc des conséquences de sa perturbation soit sur les activités de l'entité financière, soit sur son respect de la réglementation applicable. Si le respect ou non d'une disposition de la réglementation financière semble relativement facile à évaluer, la premi-ère partie de la définition semble très subjective (perturbation de la performance financière d'une entité financière, ou de la solidité ou continuité de ses services et activités) et, en l'absence de jurisprudence, difficile à qualifier dans les faits. Cependant, il semble probable que le prestataire pourra difficilement contester la qualification des fonctions qu'il soutient et retenue par l'entité financière cocontractante.

Si le prestataire soutient des fonctions critiques ou importantes, le contrat doit obligatoirement inclure, en plus des clauses visées ci-dessus, des clauses imposant au prestataire notamment (i) d'assortir ses niveaux de services d'objectifs quantitatifs et qualitatifs, ainsi que les mesures correctrices qui devront être mises en œuvre quand ces derniers ne sont pas atteints (qui ne sont donc pas obligatoirement des pénalités), (ii) de notifier à l'entité financière tout incident qui pourrait avoir des conséquences sur sa capacité à fournir les services, selon des délais prédéfinis, (iii) de mettre en œuvre et de tester des plans d'urgence fournissant un niveau approprié de sécurité, (iv) d'accepter des droits d'audit très étendus au bénéfice de l'entité financière et des autorités réglementaires et (v) de prévoir une période de réversibilité adéquate pendant laquelle il continuera à fournir les services afin de permettre au prestataire de recourir à un prestataire tiers ou de réinternaliser le service. Dora ne prévoit pas explicitement que des niveaux de services minimums peuvent être imposés par les autorités réglementaires. Cependant, il semble probable que ces dernières deviendront prescriptrices de niveaux de services minimums pour certains services critiques, dans le cadre des sanctions ou recommandations qu'elles émettront envers les entités financières.

Une dernière clause obligatoire impose aux prestataires de participer pleinement aux tests de pénétration mis en œuvre par l'entité financière conformément à ses obligations. En effet, l'article 26 de Dora impose aux entités financières de réaliser au moins tous les trois ans des tests avancés de pénétration fondés sur la menace couvrant plusieurs, voire la totalité des fonctions critiques ou importantes qui ont été externalisées. Le prestataire doit donc s'engager contractuellement à participer à ces tests, mais il demeure libre de les encadrer et de facturer ses clients pour cette participation. Si ces tests pourraient avoir une incidence négative sur la qualité ou la confidentialité des services que le prestataire fournit à d'autres clients ne relevant pas de Dora, le prestataire peut engager un testeur externe pour réaliser des tests groupés sous la direction d'une

entité financière désignée associant plusieurs entités financières, afin d'éviter une multiplication de tests de pénétration. Cette solution sera cependant compliquée à mettre en œuvre contractuellement, puisque le prestataire devra choisir parmi ses clients lequel sera l'entité financière en charge d'organiser le test et faire accepter contractuellement à ses clients de se fier aux résultats de ce test.

Dora oblige donc les prestataires informatiques, s'ils veulent continuer de travailler pour des entités financières, à réécrire leurs contrats types afin qu'ils incluent les informations requises.

Les prestataires tiers critiques de services TIC

Dora prévoit finalement que les Autorités Européennes de Surveillance ou AES (qui sont l'Autorité Bancaire Européenne, l'Autorité Européenne des Assurances et des Pensions Professionnelles et l'Autorité Européenne des Marchés Financiers) peuvent conjointement désigner certains prestataires de services TIC comme étant critiques pour les entités financières sur la base de 4 critères : (i) l'existence d'un risque systémique pour les services financiers en cas de défaillance opérationnelle à grande échelle des services du prestataire (ii) l'utilisation des services de ces prestataires par des établissement d'importance systémique mondiale ou autre (iii) la dépendance d'entités financières envers les services fournis par le prestataire pour des fonctions critiques ou importantes et (iv) le degré de substituabilité du prestataire, aussi bien en terme d'existence sur le marché d'alternatives aux services proposés par le prestataire que de difficultés liées à la migration des données. La Commission Européenne a précisé[1] les modalités d'application de ces critères et introduit pour 3 de ces quatre critères des seuils quantitatifs permettant d'écarter les prestataires trop petits avant de procéder à une analyse qualitative.

La procédure de désignation est très rapide, le prestataire n'ayant qu'un délai de 6 semaines à compter de la notification pour faire part de ses commentaires sur cette désignation. Il est ensuite inscrit sur une liste publique et soumis à de lourdes obligations, sous la supervision d'une AES désignée comme superviseur principal. Tout d'abord, un prestataire critique établi dans un pays tiers doit disposer d'une filiale dans l'Union Européenne et il est interdit aux entités financières de contracter avec lui en l'absence d'une telle filiale.

Le prestataire critique de services TIC est ensuite soumis à un audit approfondi par son superviseur, afin de s'assurer qu'il a bien mis en place des règles, procédures, mécanismes et dispositifs complets, solides et efficaces pour gérer le risque qu'il est susceptible de faire peser sur les entités financières. Sur la base de cette évaluation, le superviseur établit un plan de supervision individuel clair, détaillé et motivé décrivant les objectifs annuels de supervision et les principales actions prévues pour le prestataire. Ce plan est révisé tous les ans.

Les prestataires critiques sont donc soumis à une tutelle forte de leur superviseur, qui contrôle et formule des « *recommandations* » touchant le cœur de leurs activités, et en particulier les mesures de sécurité qu'ils adoptent et leurs recours à la sous-traitance. Si le prestataire critique ne suit pas les « *recommandations* » de son superviseur, il doit fournir des explications circonstanciées justifiant ce refus. Le superviseur doit alors, s'il n'est pas convaincu par ces explications, effectuer une communication publique de ce refus et en informer les autorités compétentes sur les entités financières clientes du prestataire. Ces autorités peuvent alors informer les clients du prestataire du refus de respecter les recommandations de son superviseur et prendre toutes mesures en conséquence, qui vont jusqu'à exiger des clients du prestataire qu'ils résilient les contrats conclus avec le prestataire critique. Le superviseur dispose donc de moyens de pression très forts pour contraindre le prestataire critique soumis à son autorité à respecter ses recommandations.

Si ces arguments ne suffisaient pas, le superviseur dispose également de la possibilité d'adopter des mesures coercitives à l'encontre du prestataire, directement ou indirectement.

Le superviseur désigné dispose en effet du pouvoir d'imposer une astreinte pour obliger le prestataire tiers critiques de services TIC à respecter ses recommandations. Cette astreinte journalière est particulièrement lourde, puisqu'elle peut atteindre jusqu'à 1% du chiffre d'affaires quotidien moyen réalisé au niveau mondial par le prestataire au cours de l'exercice précédent, et parce que le superviseur désigné peut rendre publique toute astreinte infligée.

En dernier recours, les autorités compétentes peuvent exercer un pouvoir de coercition indirect sur les prestataires, en exigeant que les entités financières cocontractantes résilient, en partie ou en totalité, les accords contractuels concernés.

Le prestataire critique doit finalement s'acquitter auprès de son superviseur d'une redevance couvrant intégralement les dépenses encourues par ce dernier pour sa supervision.

Les prestataires informatiques vont donc devoir s'adapter à ce nouvel environnement réglementaire et collaborer avec les autorités financières s'ils veulent continuer à travailler avec les entités financières. Le gouvernement a introduit le 15 octobre dernier un projet de loi adaptant le code monétaire et financier et le code des assurances à Dora. Ce projet de loi comporte en particulier des dispositions d'adaptation du code monétaire et financier s'agissant des prérogatives de l'Autorité de contrôle prudentiel (ACPR) en matière de contrôle des entités financières qu'elle supervise. Le droit positif prévoit que l'ACPR peut exiger de tout tiers auprès de qui lesdites entités financières ont externalisé des fonctions ou activités opérationnelles la communication de tous renseignements ou documents nécessaires à l'accomplissement des missions de supervision de l'ACPR. Le projet de loi prévoit que les prestataires de services TIC compteront désormais parmi les personnes auxquelles le secrétaire général de l'ACPR peut demander tous renseignements et documents.

Marc LEMPÉRIÈRE
Avocat aux barreaux de Paris et New York
Associé Almain

Arnaud PINCE
Avocat au barreau de Paris
Associé Almain

Notes

(1) Règlement délégué (UE) 2024/1502 de la Commission du 22 février 2024 complétant le règlement (UE) 2022/2554 du Parlement européen et du Conseil par la définition des critères de désignation de prestataires tiers de services TIC comme critiques pour les entités financières