CENTRE DE DROIT
BANCAIRE ET FINANCIER

Union européenne

Le Digital Finance Package, partie 2 : Résilience numérique

Par Jeremy Bacharach le 25 novembre 2020

Il y a quelques jours, nous commentions le premier bloc du *Digital Finance Package* de la Commission européenne : le projet de règlement sur les marchés de crypto-actifs ou P-MiCAR (Bacharach, cdbf.ch/1163/). Nous continuons notre lecture de ce train de mesures en nous penchant aujourd'hui sur le projet de règlement concernant la « résilience numérique » des institutions financières : le *Proposal for a Regulation on digital operational resilience for the financial sector* (P-RDOR). Par ce projet, la Commission souhaite introduire des mécanismes réglementaires visant à couvrir les risques liés aux infrastructures informatiques utilisées par les acteurs de l'industrie financière.

Les problèmes concrets qui ont présidé à la création de ce projet ne sont pas entièrement clairs (et ce en dépit des impressionnants graphiques fournis par la Commission). A notre sens, deux principaux thèmes se détachent. Premièrement, il y a la crainte qu'une défaillance informatique au sein d'une institution financière ne se propage aux autres institutions et, par conséquent, affecte la stabilité financière de l'Union. Deuxièmement, ce que nous interprétons comme une sorte d'anxiété informe face aux incertitudes générées par la digitalisation grandissante de la finance, et qui s'exprime dans un « besoin de réguler » : il nous semble en effet que le ton quasi-alarmiste adopté par la Commission ne fait au final pas l'objet d'une explication très détaillée.

Le projet de RDOR réglementerait la résilience digitale des institutions financières sous quatre angles (1(1)(a) P-RDOR) :

- La création d'une réglementation relative aux cinq sous-domaines suivants : la gestion des risques numériques, le signalement (*reporting*) des incidents informatiques, le contrôle (*testing*) de la « résilience numérique », le partage de l'information en matière de risques numériques, et la gestion des risques relatifs aux prestataires de services externes ;
- La définition de règles applicables aux relations contractuelles entre institutions financières et prestataires de services externes ;
- La supervision des prestataires de services fournissant des prestations « critiques » (*critical*) ;
- Le cadre institutionnel y relatif.

Le champ d'application du règlement s'étendrait – en bref – à *tout le monde*, c'est-à-dire toutes les entités assujetties à une surveillance en vertu de la réglementation financière européenne,

des banques aux entreprises d'investissements, en passant par les réassurances et les référentiels de titrisation (2(1) P-RDOR).

L'art. 4(1) P-RDOR exprime le principe général de la réglementation : « *Financial entities shall have in place internal governance and control frameworks that ensure an effective and prudent management of all ICT risks* ». La suite du règlement entre plus en détail dans les divers devoirs des institutions financières. Il met en place un système relativement complexe de documentation et de contrôle interne concernant les systèmes informatiques des assujettis et les risques qui en découlent. Les thèmes suivants, en particulier, sont évoqués :

- La qualité des outils informatiques (art. 6)
- La confidentialité des données (art. 8(4))
- La détection des anomalies (art. 9)
- La continuité des affaires (*business continuity*, art. 10) ainsi que les mécanismes de *backup* et de *recovery* (art. 11)
- Les incidents informatiques (*ICT-related incidents*), ces incidents devant être prévenus, détectés, évalués, classifiés, et communiqués (art. 13 et 15 ss)
- Le contrôle (*testing*) des systèmes informatiques et de leurs vulnérabilités (art. 21 ss)
- L'échange d'informations entre assujettis (art. 40).

Le Chapitre V est titré « *Managing of ICT Third-Party Risk* » et porte sur l'externalisation de certaines tâches à des prestataires externes. Certaines problématiques classiques de l'*outsourcing* sont abordées, telles que la responsabilité ultime des assujettis (25(1) P-RDOR) ou le droit de regard de l'assujetti (27(2)(h) P-RDOR) et de ses autorités de surveillance (27(2)(i) P-RDOR). Mentionnons cependant trois éléments dignes d'être soulignés :

- Le RDOR réglementerait de manière particulièrement dense et détaillée les contrats d'*outsourcing*. L'art. 27(2) P-RDOR, par exemple, mentionne pas moins de 11 sujets devant être couverts par le contrat liant l'assujetti au prestataire externe.
- Parmi ces 11 sujets figure un élément intéressant : l'*exit*. Le P-RDOR exige en effet que l'institution soit également en mesure de se départir du contrat d'*outsourcing* (voir notamment 25(8), (9) et 27(2)(k) P-RDOR).
- *Last but not least*, le P-RDOR instaurerait un régime de surveillance des « *critical ICT third-party service providers* », c'est-à-dire des prestataires ayant une importance systémique – « critique » – pour le système financier européen (28ss P-RDOR, et notamment l'art. 30(2)).

Il est intéressant de comparer le projet RDOR avec la situation qui prévaut en droit suisse. A l'heure actuelle, les risques liés aux infrastructures informatiques sont essentiellement réglementés par les circulaires de la FINMA 2018/13 « Externalisation » et 2008/21 « Risques opérationnels – banques » (§§ 135-135.12). Ces circulaires consacrent une réglementation axée sur des principes généraux ainsi que des buts devant être atteints par les assujettis (*principles-based regulation*). Par contraste, le projet européen s'articule autour d'un nombre important de règles de comportement précises et détaillées, courant le risque d'accroître la charge réglementaire – « bureaucratique » diront certains – pesant déjà sur les institutions financières. En cas d'adoption du P-RDOR, il n'est pas exclu que la « mode européenne » finisse par s'imposer en Suisse par le jeu subtil de l'équivalence, inscrite dans plusieurs textes susceptibles d'être modifiés par le projet RDOR.