L'UNION EUROPÉENNE SE RENFORCE CONTRE LES MENACES

Le nouveau règlement européen sur la cybersécurité [1] a pour ambition de muscler la protection des utilisateurs, professionnels ou non, et celle des outils numériques face au cybercrime.

Par Frédéric Forster, directeur du pôle Télécoms du cabinet Alain Bensoussan Avocats Lexing

La cybermenace se développe à la vitesse éclair. Protéiforme et insidieuse, elle est portée par la multiplication des failles potentielles de sécurité. Elle se nourrit de la croissance sans égale du nombre et de la nature des objets connectés. Elle fait son miel du développement des projets de transition numérique tendant à dématérialiser tout ce qui peut l'être, et à utiliser le cloud et les accès distants à Internet. Car si le numérique est mondial, la menace l'est donc également. Elle ne s'arrêtera pas aux frontières, et seules des mesures internationales contreront les effets, planétaires eux aussi, des menaces et des actions menées contre la sécurité des SI. Le règlement européen adopté succède, avec seulement trois ans de décalage, à une directive européenne[2], dite Directive NIS (ou SRI en français), dont l'objectif affiché était déjà de prévoir l'adoption, par les États membres, de mesures destinées à assurer un niveau élevé et commun de sécurité des réseaux et des SI. Pour protéger l'économie de l'Union, ce texte a créé une nouvelle catégorie d'acteurs – les opérateurs de services essentiels (OSE) – dont l'interruption de l'activité aurait un impact significatif sur l'économie ou de la société.

APPLICATION PLUS GÉNÉRALE DU « SECURITY BY DEFAULT »

La France s'était déjà dotée, dès 2013, d'un dispositif législatif national, ayant conduit à l'identification de sociétés, qualifiées d'opérateurs d'importance vitale (OIV). Ces derniers étaient donc naturellement concernés par les dispositions de la directive européenne, et leur liste a été complétée par quelques organismes supplémentaires, pour constituer le nouvel ensemble des OSE. L'objectif d'harmonisation et de coopération interétatique par la mise en place d'échanges d'informations sur le cyberrisque, prôné par la directive, n'a cependant pas été atteint à cause de la non-transposition, ou la transposition incomplète, de ses dispositions dans le droit interne d'une majorité d'États membres (dont la France). Face à cet échec d'harmonisation, il est apparu nécessaire de passer par la voie du règlement européen, qui constitue l'instrument législatif communautaire le plus brutal – il contourne les parlements nationaux – et, partant, le plus directif qui soit. Ce règlement est effectif depuis le 28 juin 2019 (seuls six de ses articles voient leur entrée en vigueur repoussée de deux années supplémentaires, soit au 28 juin 2021). Reconnaissons que l'urgence, constatée en 2016, n'a fait que croître, et que le délai joue en défaveur des particuliers, des entreprises, des administrations et des États. Les entreprises du numérique sont donc particulièrement concernées par les objectifs énoncés par le règlement européen, par la contribution qu'elles apporteront à la construction d'un espace digital davantage sécurisé, autour du concept du *security by default*, déjà connu en matière de protection des données à caractère personnel, mais appliqué ici de façon plus générale, et de la certification de leurs produits ou de leurs services (gérée, en France, par l'Anssi [5]).

[1] Règlement (UE) 2019/881 du 17 avril 2019 relatif à l'Enisa [4] et à la certification cybersécurité des technologies de l'information et des communications et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité). Lien : bit.ly/2LTaW1O
[2] Directive (UE) 2016 :1148 du Parlement européen et du Conseil du 6 juillet 2016.
[3] Lien : bit.ly/2oThSTn
[4] Enisa : Agence européenne chargée de la sécurité des réseaux et de l'information
[5] Anssi : Agence nationale de la sécurité des systèmes d'information

LE RÈGLEMENT ARTICULÉ EN DEUX VOLETS ET SIX OBJECTIFS

A. Mise en place d'une certification de la cybersécurité à l'échelle européenne pour les produits, les services et les processus IT.

B. Extension du rôle de l'Enisa[4], dans le sens d'une assistance par l'agence aux États membres dans les processus d'élaboration et de mise en œuvre de leurs politiques nationales de sécurité et dans le rôle de consolidation de la coopération entre États membres sur les incidents de sécurité afin de mieux identifier et localiser les responsables des cyberattaques.

Ces volets principaux se déclinent ainsi [3] :

1. **Poursuite du renforcement des capacités et de l'état de préparation** des États membres et des entreprises, ainsi qu'une amélioration de la coopération, du partage d'informations et de la coordination des parties prenantes.
2. **Hausse au niveau de l'Union des capacités** susceptibles de compléter l'action des États membres, notamment dans les cas d'incidents et de crises transfrontières majeurs, tout en prenant en compte l'importance de préserver et de renforcer les capacités nationales de réaction en cas de cybermenaces de tous types.
3. **Sensibilisation des citoyens, des organisations et des sociétés** aux questions de cybersécurité.
4. **Renforcement de la confiance des consommateurs** par le recours à la certification à l'échelle de l'Union prévoyant des exigences et des critères d'évaluation communs en matière de cybersécurité dans l'ensemble des marchés nationaux et des secteurs.
5. **Encouragement des organisations, fabricants et fournisseurs** à mettre en œuvre la sécurité des produits et services TIC dès les phases de conception et de développement et durant tout le cycle de vie du produit ou service ;
6. **La généralisation de la sécurité par défaut et de la sécurité dès la conception** pour les produits, services ou processus TIC sans que cette sécurité ne nécessite une compréhension des détails techniques spécifique ou un comportement non intuitif de l'utilisateur.

Suite du dossier p. 118