Contributions à l'atelier : Convergences du Droit et du Numérique

L’évaluation de la conformité réglementaire d'un système d'information

Antoine Sacré[1]
Doctorant à la Faculté d'Informatique de l'Université de Namur, dans le cadre d'un doctorat en entreprise au sein de Comexis
Promoteur de thèse : Prof. Jean-Noël Colin[2]
Co-promoteur : Benoît Hosselet

1. Communauté d’appartenance

Étant doctorant en informatique, ma communauté d’appartenance est l’informatique. Je suis cependant sensibilisé aux applications du droit dans l’informatique car j’ai également en ma possession un master de spécialisation en droit des technologies de l’information et de la communication.

2. Contexte

La pression des contraintes réglementaires sur les systèmes d’informations est en croissance ces dernières années. À l’échelle communautaire, plusieurs actes législatifs introduisent des exigences ciblant spécifiquement les systèmes d’informations. Nous pouvons penser notamment à la directive 2000/31/CE sur le commerce électronique, le règlement 910/2014 sur l’identification électronique et les services de confiance pour les transactions électroniques, le règlement 2016/679 sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel (appelé “RGPD”) ou encore la directive 2016/1148 sur les mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (appelé “directive NIS”). Les ratio legis de ces actes législatifs étant différents, ils imposent des contraintes sur toutes les dimensions d’un système d’information (matérielle, logicielle, réseau, données, humaine). Ainsi, les contraintes réglementaires font aujourd’hui partie intégrante des contraintes à considérer lors de la conception, le développement ou la maintenance des systèmes d’informations.

Plusieurs défis découlent de cette pression réglementaire. Tout d’abord, les actes juridiques, la doctrine et même les guides formulés par des autorités publiques[3], sont trop peu lisibles et précis pour que les informaticiens puissent aisément les appliquer dans leur

[1] antoine.sacre@unamur.be
[2] jean-noel.colin@unamur.be
[3] Nous pensons par exemple au guide RGPD du développeur développé par la CNIL dans le cadre de la mise en place du RGPD dans les systèmes informatif, voir https://www.cnil.fr/fr/guide-rgpd-du-developpeur

travail sans devoir effectuer des interprétations alors qu'ils n'en ont pas nécessairement les compétences. Les petites équipes de développement informatique manquent ainsi de ressources pour intégrer correctement les exigences des normes.

Ensuite, plusieurs normes étant simultanément applicables à un même système informatique, l'insécurité juridique liée à la complexité des normes en est augmentée. En effet, il peut être complexe pour une équipe de développement informatique d'identifier les normes applicables et l'enchevêtrement qui peut exister entre ces normes peut conduire à des contradictions dans leurs exigences, augmentant la difficulté d'implémentation de celles-ci.

Des solution existent, notamment sous la forme de méthodologies visant à évaluer la conformité réglementaires des systèmes d'informations. Cependant, celles-ci sont trop chères, trop lourdes (ISO 27005, EBIOS, Octave, Mehari) ou ne sont pas accessibles publiquement (par exemple développées en interne dans une entreprise de consultance).

3. Contribution

Notre contribution propose le développement d'une méthodologie relativement simple et légère visant à aider principalement les petites équipes de développement informatique à évaluer et renforcer la conformité réglementaire des systèmes d'informations qu'elles développent ou maintiennent.

Notre objectif est d'évaluer si une modélisation d'un système d'information (graphique et/ou textuelle) peut servir de base de raisonnement pour en évaluer la conformité réglementaire. Cette évaluation de la conformité réglementaire se ferait sur base d'une description du système à analyser contenant toutes les informations nécessaires pour en évaluer la conformité. Un travail préliminaire sur les exigences réglementaires devra être effectué pour définir le méta-modèle des informations devant être présentes dans la description du système. Enfin, nous espérons pouvoir automatiser le processus d'évaluation de la conformité et, lorsque le système d'information est identifié comme non-conforme aux contraintes réglementaires, pouvoir proposer de manière intelligente et automatisée un ensemble de mesures correctrices.

Dans cette optique, nous avons déjà commencé le développement de la méthodologie par la définition d'une représentation graphique et textuelle d'un système d'information. Désormais, nous estimons qu'il est nécessaire de parcourir différents textes réglementaires dans le but d'en identifier les contraintes sur les systèmes d'informations, les conditions d'application de ces contraintes ainsi que les éléments des systèmes d'informations qui y sont soumis. Ce travail devrait permettre de mettre en lumière les oppositions pouvant apparaître entre des exigences d'actes législatifs différents. La liste de contraintes réglementaires ainsi créée devrait in fine permettre d'évaluer par la suite la conformité d'un système d'information, sur base de la modélisation de celui-ci. Nous sommes cependant toujours en phase de réflexion concernant le processus d'évaluation de la conformité réglementaire en tant que tel.