ARRCIS

Sacre, Antoine; COLIN, Jean-Noel; Hosselet, Benoît

Published in:
Time to reshape the digital society

Publication date:
2021

Document Version
le PDF de l'éditeur

Chapitre 5
ARRCIS : Évaluation et renforcement de la conformité réglementaire d'un système d'information

Antoine Sacré[1]

Jean-Noël Colin[2]

et

Benoît Hosselet[3]

Introduction

La pression des normes juridiques sur les systèmes d'information est en croissance ces dernières années. À l'échelle nationale, le Code de droit économique régit le commerce en ligne. À l'échelle européenne, plusieurs actes législatifs introduisent des exigences ciblant spécifiquement les systèmes d'information. Nous pouvons penser notamment au Règlement Général sur la Protection des Données (ci-après dénommé « RGPD »). Enfin, le projet de règlement européen de l'intelligence artificielle (Artificial Intelligence Act) augmentera certainement dans le futur la pression sur les fournisseurs de système d'intelligence artificielle.

L'impact d'une non-conformité à ces normes juridiques formulant des règles s'appliquant aux systèmes d'information peut être de plusieurs ordres. L'impact peut être d'ordre financier avec des amendes administratives pouvant aller jusqu'à plusieurs millions d'euros dans le cas du RGPD notamment. En 2020, l'Autorité de Protection des Données belge a

[1] Comexis, antoine.sacre@comexis.net.
[2] Namur Digital Institute, Université de Namur, jean-noel.colin@unamur.be.
[3] Comexis, benoit.hosselet@comexis.net.

d'ailleurs imposé des amendes de 50.000 € à un réseau social[4] et 600.000 € à Google[5] pour non-respect de certaines dispositions du RGPD. L'impact peut également prendre des formes plus diverses et toucher les activités mêmes d'une entreprise, par exemple par des sanctions civiles allongeant le délai de rétractation de douze mois, au lieu de 14 jours, en l'absence d'information sur ce droit de rétractation au moment requis. Voire encore d'autres sanctions, comme des rappels à l'ordre[6] ou encore des limitations temporaires ou définitives de traitement[7].

Les *ratio legis* de ces normes juridiques étant différentes, ils imposent des contraintes sur plusieurs dimensions d'un système d'information (matérielle, logicielle, humaine, réseau, données). Dès lors, les contraintes légales font aujourd'hui partie intégrante des contraintes à considérer lors de la conception, le développement ou la maintenance des systèmes d'information : elles sont donc incontournables lorsque l'on conçoit des systèmes d'information.

Bien que les normes juridiques soient aujourd'hui incontournables, l'aspect normatif dans les systèmes d'information n'est bien souvent envisagé qu'a posteriori du développement du système, par exemple dans le cadre d'une procédure d'audit, et non pas « by design ». Par « développement de système d'information », nous entendons le développement de nouveaux systèmes conçus de toutes pièces ainsi que les refontes de systèmes existants. Ces derniers sont particulièrement touchés lorsqu'une nouvelle norme juridique entre en application étant donné la complexité inhérente à la mise à jour de tels systèmes en phase d'utilisation. L'apparition de nouvelles normes n'est pas la seule cause du besoin de (re) mise en conformité. En effet, l'intégration des normes juridiques est également complexifiée par l'évolution constante des systèmes d'information et de leur environnement. La tendance actuelle vers le *cloud computing*, malgré tous ses avantages, engendre une perte de contrôle sur certains aspects du système d'information tels que le lieu d'exécution ou le matériel sur lequel est exécuté le système. La puissance des fournisseurs de

[4] Autorité de Protection des Données, « L'Autorité de protection des données impose 50.000 euros d'amende à un réseau social », 19 mai 2020 [en ligne].

[5] Voyez toutefois la décision de la Cour des marchés du 30 juin 2021.

[6] Art. 58, § 2 al. b, du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

[7] Art. 58, § 2, al. f, du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

services *cloud* engendre également une perte de contrôle dans le contenu des contrats de sous-traitance, qui sont bien souvent à prendre tels quels ou à laisser.

Des solutions existent. Nous pouvons penser notamment à des solutions liées à la gestion des risques des systèmes d'information telles que l'ISO 27005, portant sur la gestion des risques[8] ou à la méthode EBIOS, portant sur l'identification des risques des systèmes d'informations. D'autres méthodes dont la portée dépasse la sécurité informatique existent également, bien que plus rares, telles que l'ISO 19600 portant sur la gestion de la conformité des entreprises[9]. Ces solutions, bien que répandues, ne sont pas réellement satisfaisantes car elles ne couvrent pas toutes les étapes d'un processus de mise en conformité d'un système informatique. Une solution qui décrirait un processus d'évaluation de la conformité des systèmes d'information, utilisable aussi bien pour un système en phase d'exploitation qu'en phase de conception, permettrait d'éviter une potentielle refonte coûteuse des systèmes et permettrait de respecter les exigences légales demandant une prise en considération dès la conception des systèmes[10]. Enfin, une telle solution qui équiperait les développeurs de logiciels pour développer leur système de manière conforme aux lois serait extrêmement utile dans notre société actuelle où l'utilisation des logiciels devient inévitable dans la vie courante, l'e-gouvernement et les services essentiels (distribution d'eau, d'électricité, etc.).

I. Une solution : faciliter l'évaluation de la conformité des systèmes

Notre étude vise à faciliter la mise en conformité des systèmes d'information aux normes par la réalisation d'une méthodologie permettant l'évaluation aisée de la conformité des systèmes d'information, utilisable entre autres par des profanes en droit.

Le terme « système d'information » est considéré dans un sens large, dès sa phase de conception, et concerne aussi bien le système d'information d'un hôpital dans sa globalité qu'une application mobile, le site web d'un

[8] ISO/IEC, Technologies de l'information – Techniques de sécurité – Gestion des risques liés à la sécurité de l'information, 27005, 2018.

[9] ISO/IEC, Systèmes de management de la compliance – Lignes directrices, 19600, 2014.

[10] Nous pouvons par exemple penser à l'exigence de « protection des données dès la conception » formulée à l'article 25 du RGPD, dont la version anglaise « privacy by design » est plus couramment utilisée.

petit commerce. Nous nous concentrons principalement sur la dimension logicielle des systèmes d'information, bien que nous considérions que les éléments qui composent l'infrastructure physique d'un système d'information doivent être pris en compte lorsque cela est pertinent pour la mise en conformité à une norme juridique. Les documents contractuels exigés par une norme sont considérés comme tout autre élément du système d'information car ceux-ci sont indispensables à examiner lors de l'évaluation de la conformité d'un système.

Les normes prises en compte dans ce projet sont de deux ordres : (i) les normes juridiques dont, entre autres, les dispositions légales qui impactent le développement, l'exploitation et la maintenance des systèmes d'information, directement, en contenant des dispositions dont les exigences ciblent directement le processus de conception[11] ou indirectement par des exigences ciblant la finalité du système d'information, par exemple lorsque le système développé est un site de commerce en ligne ; (ii) les normes techniques, telles que les normes définies par l'organisation internationale de normalisation (ISO), dont les exigences impactent également le développement, l'exploitation et la maintenance des systèmes d'information. À ce stade nous n'avons abordé que les normes juridiques dans nos recherches et nous ne développerons que ces dernières dans la suite de l'article.

II. Travaux connexes

Nous ne sommes pas les premiers à nous intéresser à la conformité des systèmes d'information. D'autres auteurs s'y sont également attardés avec des champs d'applications divers.

Palmér (2017) a conçu une technique de modélisation d'architecture d'entreprise permettant aux entreprises d'améliorer leur conformité au RGPD. Concrètement, l'auteur a créé une série de méta-modèles dont l'objectif est de représenter graphiquement l'architecture d'une entreprise respectant les exigences du RGPD. Les exigences des normes sont dans ce cas représentées implicitement à travers les éléments et les relations entre éléments composants ces représentations graphiques

D'autres recherches se sont concentrées sur certains aspects de l'évaluation de la conformité, notamment l'aspect juridique, comme Amariles, Troussel et Hamdani (2019), qui se sont intéressés à l'automatisation des tâches réalisées par des juristes lors de l'évaluation de la conformité

[11] Nous pensons de nouveau à l'exigence de « protection des données dès la conception » formulée à l'article 25 du RGPD.

d'un système d'information. Les auteurs ont débuté en 2019 le développement d'une méthodologie permettant d'automatiser l'évaluation de la conformité sur la base de documents à caractère juridique (privacy policy, contrats…) en lien avec le système d'information.

L'évaluation de la conformité de la dimension matérielle des systèmes d'information a aussi fait l'objet de développements, notamment du côté des brevets où Graves et al. (2008) ont eu pour but d'automatiser le travail effectué par un auditeur lors de l'évaluation de la conformité de l'infrastructure des systèmes d'information à des normes techniques, avec pour originalité la génération de questionnaires afin de collecter les informations manquantes pour réaliser l'évaluation et l'envoi automatique de ces questionnaires aux personnes susceptibles de posséder ces informations.

Le type de modélisation utilisé par Palmér (2017) a pour vocation d'être traité comme un modèle « to-be », grâce auquel une mise en conformité peut être déduite. Ainsi, le travail effectué ne permet pas d'évaluer une conformité mais de tendre directement vers celle-ci. Indépendamment de l'efficacité d'une telle approche sur l'entièreté d'une norme, sa nature ne la rend pas aisément extensible à plusieurs normes simultanément, ni plus compréhensible que la norme elle-même, car les exigences des normes ne sont pas clairement explicitées à travers les éléments et les relations entre éléments des méta-modèles, ce qui ne permet pas de connaître les raisons d'une non-conformité. La problématique du rassemblement des informations concernant le système évalué pourrait être évitée en basant l'évaluation de la conformité sur des documents juridiques si cela n'avait pas pour conséquence de restreindre la vision du système d'information, bien que les similitudes courantes entre ces documents ont l'avantage de permettre d'envisager une automatisation de l'évaluation de la conformité, comme l'ont réalisé Amariles, Troussel et Hamdani (2019). Enfin, le type de solution technique telle qu'imaginée par Graves et al. (2008) est optimisé pour évaluer la conformité à un niveau technique mais est difficilement envisageable pour évaluer la conformité à des normes juridiques ou à d'autres dimensions d'un système d'information moins concrètes, notamment la dimension organisationnelle.

Compte tenu des solutions proposées dans la littérature, nous estimons qu'il existe une place pour l'étude d'une méthode d'évaluation de la conformité des systèmes d'information traitant de toutes les dimensions d'un système d'information et fonctionnant sur une multitude de normes simultanément, à partir de laquelle il serait possible, pour l'utilisateur de la méthodologie, de réaliser un plan d'action lui permettant d'améliorer la conformité de son système d'information par rapport aux normes évaluées.

III. Modélisation des normes

Un modèle de normes est indispensable pour rendre la méthodologie fonctionnelle car il permet à l'utilisateur de la méthodologie d'identifier aisément les dispositions qui s'appliquent à son système d'information et d'évaluer la conformité de son système. Ainsi, notre but avec cette modélisation est de normaliser les informations pertinentes, présentes dans des normes de natures différentes, afin de définir un processus d'identification des exigences pertinentes et d'évaluation de la conformité identique entre toutes les normes.

A. Normes prises en compte

Comme dit précédemment, les normes juridiques considérées dans ce projet sont les normes dont les dispositions impactent le développement, l'exploitation et la maintenance des systèmes d'information. Nous concevons que du strict point de vue de la conformité à une norme, il n'est pas intuitif de ne considérer qu'un sous-ensemble des dispositions d'une norme. Cependant, notre but est ici d'évaluer la conformité des systèmes d'information, il n'est donc pas pertinent d'effectuer un travail d'extraction et de modélisation d'exigences normatives qui n'ont pas d'implications sur les systèmes d'information et qui, dès lors, ne verront pas leur conformité influencée par le système d'information.

B. Caractéristiques de la modélisation

Pour réaliser la modélisation, nous avons fait le choix de procéder par une approche « top-down », c'est-à-dire qu'au lieu d'étudier dans un premier temps les méthodes d'extraction des contraintes normatives et, dans un second temps, les méthodes de modélisation de ces contraintes, nous avons effectué le chemin inverse, dans le but de garantir que la modélisation obtenue correspond tout à fait aux besoins de notre étude et n'est pas influencée par la méthode d'extraction des exigences. La modélisation a ensuite été affinée par l'essai de la modélisation de plusieurs normes juridiques, à savoir certaines dispositions du Code de droit économique[12], du RGPD[13] et du Règlement européen sur les Dispositifs Médicaux (ci-après dénommé « RDM »)[14].

[12] Les articles VI.41, VI.45, § 1, VI.46, § 2 et § 3, XII.6 et XII.7 du Code de droit économique.

[13] Les articles 25, § 1 et § 2, et 32, § 1, du RGPD.

[14] Les articles 1 à 123 ainsi que l'annexe I du RDM.

Les caractéristiques que doit idéalement posséder la modélisation sont en partie tirées de Jureta *et al.* (2013) : les auteurs ont identifié et décrit une série de critères d'évaluation de la qualité des formalismes de modélisation des contraintes légales dans le domaine de l'ingénierie des exigences logicielles. Les critères principaux tirés de cette étude sont notamment que la modélisation devrait permettre de ne représenter que les exigences qui s'appliquent à une situation particulière, c'est-à-dire les exigences qui s'appliquent aux systèmes d'information dans le cas présent. Ainsi, selon les auteurs, aussi bien le champ d'application que les exigences de la loi devraient être intégrés à la modélisation. De plus, une représentation utilisant la modélisation devrait permettre au lecteur du modèle d'identifier rapidement (i) les personnes concernées par la loi (et les relations entre elles), (ii) les personnes concernées par une exigence particulière et (iii) toutes les exigences se rapportant à une personne concernée particulière. En outre, une représentation utilisant la modélisation ne devrait pas contenir plus d'informations que la norme n'en contient. Cela signifie que si des déductions sont possibles à partir de la loi, ces mêmes déductions et seulement celles-ci devraient être possibles à partir de la représentation. Enfin, toujours selon les auteurs, la modélisation devrait permettre un traçage des références normatives de chaque information représentée.

Nous avons, par l'essai de la modélisation de plusieurs normes juridiques, également identifié d'autres critères importants. Tout d'abord, et non des moindres, le modèle créé suivant la modélisation devrait permettre de vérifier la conformité aux normes représentées en incluant toutes les informations nécessaires à l'évaluation de la conformité, sous une forme permettant à une personne ne maîtrisant pas les normes modélisées de comprendre ces informations et de réaliser l'évaluation de son système d'information. Enfin, la technique de modélisation devrait être suffisamment générique afin de pouvoir s'appliquer à plusieurs normes simultanément.

Malheureusement, aucun formalisme ou modèle ayant ces caractéristiques n'a été trouvé dans la littérature scientifique. Nous avons donc choisi de créer cette modélisation.

C. Extractions des informations

La phase d'extraction des exigences des normes regroupe les activités d'identification et d'extraction des exigences, et des informations, pertinentes pour l'évaluation de la conformité des systèmes d'informations. Bien que nous ne considérions en soi pas cette phase comme une étape de la méthodologie, il nous a semblé nécessaire d'en formaliser la

réalisation car cette tâche est indispensable à réaliser pour développer la méthodologie.

Nous avons choisi de classer les informations extraites des normes en plusieurs catégories. Ces catégories sont les définitions, la description d'une action à réaliser, la condition pour réaliser une action, le caractère événementiel de la condition, l'entité responsable de l'action, le délai pour réaliser l'action et la dépendance à la conformité d'au moins une autre disposition. Ces catégories sont inspirées du travail d'Anish *et al.* (2019) sur la formalisation des obligations des parties prenantes dans le contexte du développement de système d'information soumis au Health Insurance Portability and Accountability Act (HIPAA), à l'exception de la dernière catégorie que nous avons ajoutée suite à nos essais de modélisation. Différentes catégories d'informations pouvant être extraites suivant le but poursuivi par l'extraction des exigences[15], ces catégories sont amenées à évoluer avec le développement de notre méthodologie.

La procédure suivie pour extraire les informations des normes est la lecture d'un paragraphe et le classement de ce paragraphe dans une des catégories prédéterminées dans le modèle. Chaque paragraphe de la norme peut donc correspondre à une entrée dans le modèle sauf s'il n'est pas pertinent, dans ce cas il n'est pas intégré au modèle, ou si le paragraphe définit plusieurs actions dont les conditions diffèrent, dans ce cas autant d'entrées sont créées que de paires [conditions, actions]. En guise d'exemple, après le parcours des 123 articles du RDM et de sa première annexe, nous avons identifié 98 paragraphes contenant au moins une action ayant un impact sur le système d'information. Notons que pour 4 paragraphes parmi ces 98, 2 actions distinctes ont été identifiées.

D. Modélisation des informations

Une fois extraites des normes, les informations sont ajoutées au modèle sous une forme particulière, propre à chaque information. Nous présentons ci-après les formes les plus intéressantes que nous avons réalisées.

Les conditions d'application et les actions sont intégrées au modèle en reformulant le paragraphe sous la forme suivante : « Si *condition* (*c.-à.-d.*

[15] Par exemple, Breaux *et al.* (2006) se sont limités aux obligations et aux conditions d'application de celles-ci car leur modèle visait avant tout à formuler des exigences logicielles. Waltl *et al.* (2014) ont eux choisi de diviser le contenu de normes juridiques exigeant la réalisation d'analyse de risque des systèmes d'information dans le milieu financier en 3 catégories : (i) les buts (les idées générales des exigences dans les lois), (ii) les principes (les intentions des exigences) et (iii) les exigences. Ces trois concepts devant permettre, selon les auteurs, de faciliter la compréhension de ces normes pour les informaticiens.

un évènement, un contexte ou une situation) alors *action requise* (*c.-à.-d. une exigence formulée par rapport à un agent*) ». Au sein du modèle, la condition de réalisation de l'action est reformulée pour toujours avoir la forme « Si *condition* ». L'action, elle, est reformulée pour toujours commencer par l'agent ciblé par l'exigence (sauf s'il n'est pas déterminable), suivie d'un verbe modal (peut, doit, devrait…) (sauf s'il n'est pas déterminable). Les références vers le paragraphe d'où est tirée chaque action et condition sont ajoutées directement dans le texte des actions et conditions afin de maintenir la traçabilité de chaque élément composant l'action ou la condition.

Les conditions d'application peuvent être de deux sortes : soit être des conditions simples, soit des conditions événementielles dont la valeur de vérité dépend d'un événement, d'un « trigger », et change donc dans le temps indépendamment du système d'information, selon Anish *et al.* (2019). Les conditions classiques peuvent être évaluées dès le début de la conception, contrairement aux conditions événementielles, qui sont ponctuelles car elles dépendent d'événements. Nous avons effectué cette séparation car nous souhaitons laisser le choix aux utilisateurs de la méthodologie d'évaluer la conformité de leur système au temps « t » avec ou sans prise en compte des contraintes qui pourraient s'appliquer sur leur cas dans le futur. Ainsi, grâce à la séparation entre condition et condition événementielle, il est possible de n'évaluer la conformité qu'aux exigences s'appliquant dès la phase de conception, c'est-à-dire aux conditions qui ne sont pas dépendantes d'événements. Les deux dispositions suivantes, l'annexe I.17.1 du RDM[16] et l'article 10.4 du RDM[17], ont pour but d'illustrer la différence entre les conditions classiques et les conditions événementielles. Dans la première, la condition apparaît dans la première partie du paragraphe : « Les dispositifs comportant des systèmes électroniques

[16] « Les dispositifs comportant des systèmes électroniques programmables, notamment des logiciels, ou les logiciels qui sont des dispositifs à part entière sont conçus de manière à garantir la répétabilité, la fiabilité et les performances eu égard à leur utilisation prévue. En condition de premier défaut, des moyens adéquats sont adoptés pour éliminer ou réduire autant que possible les risques qui en résultent ou la dégradation des performances ». Annexe I.17.1 RDM.

[17] « À la demande d'une autorité compétente, les fabricants lui communiquent toutes les informations et tous les documents nécessaires pour démontrer la conformité du dispositif, dans une langue officielle de l'Union définie par l'État membre concerné. L'autorité compétente de l'État membre dans lequel le fabricant a son siège social peut demander que le fabricant fournisse des échantillons du dispositif gratuitement ou, si c'est impossible, donne accès au dispositif. Les fabricants coopèrent avec une autorité compétente, à sa demande, à toute mesure corrective prise en vue d'éliminer ou, si ce n'est pas possible, d'atténuer les risques présentés par des dispositifs qu'ils ont mis sur le marché ou mis en service. […] », art. 10.4 RDM.

programmables, notamment des logiciels, ou les logiciels qui sont des dispositifs à part entière […] » (annexe I.17.1 du RDM). Cette condition porte sur les composants du dispositif et est évaluable dès la conception de celui-ci, cette condition n'est donc pas une condition événementielle. Dans la seconde, la condition possède une dimension événementielle car ce n'est que si l'autorité compétente demande toutes les informations et tous les documents nécessaires pour démontrer la conformité du dispositif que celle-ci s'applique. Pour gérer les exceptions qui apparaissent régulièrement dans les normes, nous effectuons autant d'entrées dans notre modèle que de cas créés par l'exception et nous ajoutons la condition de l'exception dans toutes les exigences ciblées par l'exception.

Le délai pour réaliser l'action et la durée de réalisation de l'action sont extraits de l'action en répondant à la question « quand et pendant combien de temps l'action doit-elle être réalisée ? ». Nous avons pu observer que pour beaucoup d'actions, le délai et la durée de réalisation ne sont pas explicitement précisés dans la norme. Dès lors, nous considérons par défaut que l'action doit être réalisée dès que sa ou ses conditions d'application sont rencontrées. Ces deux catégories d'information sont importantes car elles permettent de modéliser les contraintes temporelles qui apparaissent dans les normes, qui seraient autrement difficilement transmises dans le modèle[18].

IV. Méthode d'évaluation de la conformité des systèmes d'information

L'objectif de notre recherche est de développer et d'évaluer une méthodologie permettant l'analyse de la conformité des systèmes d'information. Cette méthodologie se divise actuellement en trois étapes à réaliser par l'utilisateur de la méthodologie. En premier lieu, l'utilisateur sélectionne les exigences d'une norme sur la base de laquelle il souhaite vérifier la conformité de son système d'information (par exemple, l'utilisateur peut sélectionner les exigences portant sur les sites de e-commerce). En second lieu, l'utilisateur modélise son système d'information (par exemple, un

[18] Nous pensons notamment aux dispositions du Code de droit économique (CDE) qui formulent des contraintes temporelles telles que « avant que », par exemple dans l'art. XII. 7 CDE : « […] avant que le destinataire du service ne passe une commande par voie électronique […] », « durant », par exemple dans l'art. VI. 45, § 1 CDE : « […] durant toute la procédure d'achat ou de réservation […] » ou encore « à tout moment ».

site de e-commerce). Enfin, l'utilisateur analyse la conformité de son système d'information sur la base d'un processus d'évaluation.

Pour des raisons de pertinences et d'espace, seules les première et dernière étapes sont décrites dans cet article.

A. Sélection des exigences pertinentes

Le but de cette étape, pour l'utilisateur de la méthodologie, est d'identifier l'ensemble des dispositions qu'il souhaite analyser parmi la ou les normes pertinentes pour son système d'information, afin de (i) connaître l'ensemble des informations devant figurer dans le modèle du système d'information qu'il devra réaliser et de (ii) connaître l'ensemble des dispositions qui devront être vérifiées lors de l'étape d'évaluation de la conformité.

Concernant les normes dont sont tirées les dispositions, la méthodologie permet pour l'utilisateur, sur la base d'informations génériques sur le système d'information à évaluer, de sélectionner les normes qui pourraient être pertinentes pour son système d'information parmi un nombre restreint de normes. Nous considérons que l'identification des normes juridiques applicables à un système d'information particulier est actuellement difficilement réalisable par un profane en droit seul car identifier les normes applicables lorsque l'on ignore que celles-ci existent ou lorsque l'on ne maîtrise pas leur terminologie est une tâche ardue. De plus, la nature actuelle des systèmes d'information, dont les pays d'exécution et d'utilisation peuvent différer du pays du responsable du système, fait surgir la question de la détermination du droit applicable et plus précisément sa dimension territoriale. Bien que pertinente, cette problématique ne sera pas abordée dans cet article de par sa complexité, aussi faisons-nous l'hypothèse que chaque utilisateur de la méthodologie réglera lui-même cette problématique.

Questionnaire

Afin de développer cette première étape de la méthodologie, nous avons développé un outil permettant à l'utilisateur de la méthodologie d'obtenir un ensemble de références de dispositions légales pertinentes pour son cas, sur la base desquelles son système d'information devrait se conformer. Cet outil prend la forme d'un questionnaire généré automatiquement sur la base des conditions d'application des normes dont les réponses possibles aux questions sont pour l'instant limitées à « oui » ou « non ».

Concrètement, les questions sont générées à partir de trois concepts.

Le premier correspond aux conditions d'application singulières, qui correspondent aux sections de conditions d'application qui se répètent dans plusieurs conditions d'application composant le modèle. Ces conditions d'applications singulières portent un identifiant construit sur la base de la référence à l'article exprimant en premier la condition. Ces conditions étant toutes formulées de la même façon et commençant donc toutes par « Si … », il a été possible de générer, de façon certes un peu brute, des phrases interrogatives en supprimant le « Si » et en ajoutant un « ? » à la fin de la phrase. L'utilisation des conditions d'application singulières, en plus de permettre la création de questions relativement courtes, a permis de garantir l'absence de répétitions dans les questions posées. Le tableau ci-dessous (tableau 1) représente deux conditions d'application singulières, telles qu'elles sont présentes dans le modèle. Les codes « 52.7.A » et « 85.A » correspondent aux références des dispositions dans lesquelles ces deux conditions ont été respectivement rencontrées pour la première fois lors du parcours de la norme.

Code	Description
52.7.A	Si le dispositif est de classe I (art. 52.7 RDM)
85.A	Si le dispositif est commercialisé (art. 85 RDM)

Tableau 1. Exemple d'expressions singulières

Le second concept correspond à une reformulation des conditions d'application pour chaque action en expressions logiques, sur la base de l'article Breaux *et al.* (2006). Ces expressions logiques étant réalisées en combinant les conditions d'applications singulières avec les opérateurs logiques « et », « ou », « (», «) » et « non ». Ces expressions logiques permettent d'estimer, à partir de la réponse fournie par l'utilisateur pour chaque question générée sur la base des conditions d'application singulière qui composent l'expression, si une condition d'application s'applique (lorsque l'évaluation de la valeur de l'expression logique renvoie vrai) ou non (lorsque l'évaluation de la valeur de l'expression logique renvoie faux) au système d'information de l'utilisateur. Le tableau ci-dessous (tableau 2) représente la condition tirée de l'article 85 du RDM. Nous pouvons observer que cette condition « Si le dispositif est un dispositif de classe I et si le dispositif est commercialisé (art. 85 RDM) » est en fait composée de deux conditions singulières « Si le dispositif est de classe I » et « Si le dispositif est commercialisé » qui correspondent aux deux conditions singulières du tableau 1. L'expression logique évaluée par le questionnaire pour l'article 85 est donc « 52.7.A & 85.A ».

Référence	Nom	Condition	Référence Parent	Expression logique
Art. 85 RDM	**Rapport sur la surveillance après commercialisation**	Si le dispositif est un dispositif de classe I et si le dispositif est commercialisé (art. 85 RDM)	Art. 84 RDM	52.7.A & 85.A

Tableau 2. Exemple d'expression logique

Enfin, le dernier concept est la relation hiérarchique entre les actions. Il correspond, pour une action donnée, à la référence à l'action parente, ou à plusieurs actions parentes le cas échéant, dont les conditions d'application doivent au moins être satisfaites pour appliquer l'action donnée. Dans l'exemple précédent (tableau 2), cela correspond aux dispositions de l'article 84 du RDM : « Plan de surveillance après commercialisation ». Cela signifie que pour une action donnée, si une action parente a été évaluée comme ne s'appliquant pas à un système d'information, les conditions d'applications de cette action n'ont pas besoin d'être évaluées pour savoir que cette action ne s'appliquera pas à ce système d'information. Ce concept a ainsi permis de limiter la quantité de questions posées.

B. Processus d'évaluation de la conformité

Une fois le modèle du système d'information réalisé, processus que nous n'abordons pas dans cet article, la troisième étape de la méthodologie à réaliser par l'utilisateur est l'évaluation de la conformité. Le but de cette étape est d'évaluer la conformité du système d'information et de générer une liste de dispositions non conformes qui pourra servir ensuite pour renforcer la conformité du système. Actuellement, l'évaluation de la conformité est réalisée manuellement mais nous espérons pouvoir l'automatiser dans le futur.

Le processus d'évaluation de la conformité est réalisé sur la base des informations suivantes : (i) la liste des actions auxquelles le système d'information devrait se conformer (tirée de l'étape de sélection des exigences), (ii) pour chaque action, le délai pour réaliser l'action, les agents concernés par l'action (afin de pouvoir se focaliser sur les actions à réaliser par l'équipe de développement par exemple) et le caractère événementiel ou non d'au moins une des conditions d'applications de l'action (afin de pouvoir estimer la gravité d'une non-conformité). Sur la base de ces informations, l'évaluation de la conformité est réalisée action par action, le but étant de rechercher dans le modèle du système d'information les éléments

pertinents permettant d'estimer avec un degré de confiance suffisant que l'action a bien été réalisée par l'agent responsable.

À partir de l'évaluation, trois états de conformité peuvent être formulés par action évaluée : (i) soit le modèle du système d'information permet d'observer que l'action est respectée ; (ii) soit le modèle du système d'information ne permet pas d'observer que l'action est respectée ; (iii) soit il ne peut être observé que le système d'information n'est pas conforme et des informations complémentaires sont nécessaires pour préciser la conformité du système. Une constatation est également formulée afin (i) de lister les éléments probants (les éléments qui permettent de vérifier une action ou une partie d'action), qu'ils aient permis de conclure à une conformité ou pas, et (ii) de détailler les causes d'une non-conformité.

Finalement, un classement des résultats par action est réalisé afin d'estimer l'adhérence du système à la norme évaluée. En effet, toutes les non-conformités aux actions n'ont pas la même gravité car elles n'engendrent pas les mêmes niveaux de risques pour l'organisation responsable du système d'information. Notamment, le caractère événementiel d'une condition, par exemple lorsqu'un événement n'a pas encore eu lieu, permet de diminuer la gravité d'une non-conformité aux actions dépendant de cet événement. Plus largement, les potentielles sanctions, par action, ont un rôle important dans l'estimation des risques et par conséquent, dans le plan de mise en conformité qui suit l'évaluation du système.

V. Application à un cas et discussion

À ce stade de la recherche, nous ne sommes pas capables de présenter des résultats significatifs. Cependant, nous avons pu valider la viabilité de l'approche sur la base d'un cas pratique, qui a consisté en la mise en place de toutes les étapes de notre méthodologie dans le but d'évaluer la conformité d'une application mobile médicale par rapport au Règlement européen sur les Dispositifs Médicaux (RDM)[19].

L'application mobile médicale en question est une application actuellement conçue et développée par un prestataire de service informatique dont l'objet est l'aide au suivi du traitement thérapeutique par les patients, afin d'améliorer l'adhérence thérapeutique. Pour réaliser cela, l'application se

[19] Règlement (UE) 2017/745 du Parlement européen du Conseil du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) n° 178/2002 et le règlement (CE) n° 1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE.

base sur le schéma de médication personnel du patient pour envoyer des rappels et des conseils afin de permettre une prise optimale des médicaments (la bonne dose au bon moment).

En tant que dispositif médical traitant des données de santé, beaucoup de normes juridiques régissent cette application mobile dont le RGPD, le CDE et le RDM. Nous nous sommes cependant concentrés uniquement sur le RDM pour ce cas d'étude.

Dans le but de sélectionner les exigences pertinentes pour l'application mobile, nous avons généré un questionnaire sur la base de notre modèle du RDM. Appliqué à cette norme, ce questionnaire permet en maximum 48 questions de fournir une sélection des exigences pertinentes pour un système d'information particulier parmi les 98 paragraphes du règlement déterminés comme ayant un impact pour les systèmes d'information. Dans le cas de l'application mobile médicale étudiée, les 48 questions ont été nécessaires pour générer une sélection des exigences pertinentes. Cette sélection contient 64 paragraphes du RDM auxquels l'application mobile devrait se conformer.

Une fois les exigences pertinentes sélectionnées, nous avons réalisé un modèle de l'application mobile contenant toutes les informations nécessaires pour évaluer la conformité au RDM. Pour la grande majorité des dispositions du RDM, les informations nécessaires concernent la réalisation de documentations contenant des informations techniques sur le système et justifiant entre autres la mise en place de système de gestion des risques, de gestion de la qualité ou de surveillance après commercialisation.

Enfin, nous avons appliqué notre processus d'évaluation de la conformité. Nous avons pu déterminer qu'au moment de son évaluation, l'application mobile n'était pas entièrement conforme au RDM. Ce résultat n'était pas étonnant dans la mesure où l'application mobile n'était pas encore fonctionnelle au moment de son évaluation. L'évaluation de la conformité de l'application mobile a néanmoins pu mettre en évidence les dispositions dont les exigences sont encore à intégrer dans l'application, principalement les exigences concernant les informations à fournir à l'utilisateur d'un dispositif médical.

Notre approche présente certaines limitations. Tout d'abord, l'identification des normes pertinentes est habituellement réalisée par une veille juridique qui n'est pas *de facto* intégrée à notre méthodologie étant donné que seules des normes impactant les systèmes d'information y seront modélisées, simplifiant ainsi, pour l'utilisateur de la méthodologie, le travail d'identification des normes impactant les systèmes d'informations. Cependant, afin de faire évoluer la méthodologie, une veille devra

néanmoins être réalisée dans le but d'identifier et d'y ajouter de nouvelles modélisations de normes.

Ensuite, bien que le cœur de notre recherche soit l'évaluation de la conformité des systèmes d'information, notre approche possède des limitations inhérentes à l'utilisation d'une modélisation du système d'information pour l'évaluation de la conformité, par rapport à un audit complet de celui-ci par exemple. Nous ne pouvons effectivement garantir que le système d'information est tout à fait équivalent à sa modélisation (l'un et l'autre peuvent évoluer à des rythmes différents, des erreurs peuvent apparaître lors de la modélisation, etc.). Nous estimons cependant que notre approche permet néanmoins de donner une indication sur l'adhérence d'un système à une norme.

Conclusion

Dans cet article, nous avons présenté une approche intuitive de l'évaluation de la conformité des systèmes d'information dont le travail effectué durant la première phase de notre recherche a consisté à effectuer une première itération de notre approche et débuter la validation de celle-ci. Nous avons pu, sur la base de l'étude d'une application mobile médicale, vérifier que notre approche permet la modélisation de manière suffisante du système d'information et d'une norme afin de pouvoir réaliser une évaluation de la conformité du système d'information par rapport à cette norme, dans ce cas, le Règlement 2017/745 relatif aux Dispositifs Médicaux.

Dans le futur, nous souhaitons valider les différentes étapes de notre méthodologie. Cette validation nous permettra de faire évoluer notre solution de manière itérative et de développer une instrumentation solide. Nous souhaitons également pouvoir laisser à l'utilisateur le soin d'estimer si certaines conditions d'application ne sont pas évaluables, par exemple en donnant la possibilité de répondre « je ne sais pas » à une question du questionnaire. Nous espérons ensuite faire évoluer notre méthodologie afin de permettre l'évaluation de la conformité de plusieurs normes simultanément. Cette prise en compte de plusieurs normes simultanément sera l'occasion de mettre en lumière les oppositions pouvant apparaître ou non entre des exigences d'actes législatifs différents. Nous souhaitons également consolider notre solution en l'appliquant à d'autres cas d'études, aussi bien en termes de systèmes à analyser que de normes à appliquer.

Bibliographie

Législations

Règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), *J.O.U.E.*, L 119, 4 mai 2016.

Règlement 2017/745 du Parlement européen du Conseil du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) n° 178/2002 et le règlement (CE) n° 1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE, *J.O.U.E.*, L 117, 5 mai 2017.

Littérature scientifique

Palmér, Charlie. 2017. « Modelling EU DIRECTIVE 2016/680 Using Enterprise Architecture ». Mémoires. *School of Electrical Engineering and Computer Science (KTH)*. Disponible sur http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-201631 (26 mars 2020).

Amariles, David Restrepo, Aurore Clement Troussel, et Rajaa El Hamdani. 2019. « Compliance Generation for Privacy Documents under GDPR: A Roadmap for Implementing Automation and Machine Learning ». *32nd International Conference on Legal Knowledge and Information Systems*, Madrid, 13. Disponible sur http://gdprjurix.cs.bath.ac.uk/programme/Compliance%20Generation%20for%20Privacy%20Documents.pdf (26 avril 2020).

Graves, David, Adrian John Baldwin, Yolanta Beresnevichiene, et Simon Kai-Ying Shiu. 2008. « Systems and Methods for Monitoring Compliance with Standards or Policies », 14. Disponible sur https://patents.google.com/patent/US20080271110 (28 mai 2020).

Jureta, Ivan, Travis Breaux, Alberto Siena, et David Gordon. 2013. « Toward Benchmarks to Assess Advancement in Legal Requirements Modeling ». *2013 6th International Workshop on Requirements Engineering and Law (RELAW)*, Rio de Janeiro, Brazil: IEEE, 25-33. Disponible sur http://ieeexplore.ieee.org/document/6671343/ (13 mai 2020).

Waltl, Bernhard, Alexander W. Schneider, et Florian Matthes. 2014. « Deriving and Modelling Compliance Requirements from Legal Audits ». *Sebis*, 21. Disponible sur https://wwwmatthes.in.tum.de/document/downloadFileVersion?changeSetId=1khd2dksum55d&type=after (6 mai 2020)

Breaux, Travis D., Matthew W. Vail, et Annie I. Anton. 2006. « Towards Regulatory Compliance: Extracting Rights and Obligations to Align Requirements with Regulations ». *14th IEEE International Requirements Engineering Conference (RE'06)*, 49-58. Disponible sur https://ieeexplore.ieee.org/document/1704048 (2 avril 2020).

Anish, Preethu Rose, Vivek Joshi, Abhishek Sainani, et Smita Ghaisas. 2019. « Towards Enhanced Accountability in Complying with Healthcare Regulations ». *2019 IEEE/ACM 1st International Workshop on Software Engineering for Healthcare (SEH)*, Montreal, QC, Canada: IEEE, 25-28. Disponible sur https://ieeexplore.ieee.org/document/8823886/ (6 janvier 2021).