https://profdoc.iddocs.fr/spip.php?article77

Le RGPD : une timide avancée pour la protection des données

- Numérique : analyses -

Date de mise en ligne : mercredi 22 novembre 2017

A ne pas confondre avec le GCPD, le RGPD n'est autre que le nouveau *règlement général européen sur la protection des données*, que chaque pays de l'UE est amené à appliquer sur son territoire à partir du 25 mai 2018 [1].

Adopté en 2016 après quatre années de discussions, il remplace la *Directive sur la protection des données personnelles* adoptée en 1995. L'objectif est double, « redonner aux citoyens le contrôle de leurs données personnelles, tout en simplifiant l'environnement réglementaire des entreprises ». Comme les entreprises traitant des données personnelles, les établissements publics sont logiquement concernés par ce règlement, avec la nécessité pour chaque État membre de l'UE de trouver les moyens d'une application cohérente, en France avec un travail développé en collaboration avec la CNIL.

Regardons les grandes lignes de ce règlement, avec ensuite quelques considérations précises sur les conséquences en matière de protection, en particulier pour les enfants, avec enfin des considérations et questions sur les usages et responsabilités en établissements scolaires.

Les grandes lignes du RGPD

Le double objectif du règlement est essentiel, il permet de comprendre que deux approches s'opposent à l'égard de son contenu et de son application. Certains estimeront que les données ne sont pas assez protégées, d'autres que les entreprises du numérique ne pourront pas développer de services concurrents à ceux des entreprises anglo-saxonnes comme *Alphabet*, *Facebook* ou *Microsoft*.

Le règlement s'applique à toute structure manipulant des données à caractère personnel, qui concerne donc une personne identifiée ou identifiable, avec un ensemble large de données susceptibles de permettre l'identification (un pseudonyme ou un numéro d'identifiant, ainsi qu'une localisation, en font partie). Par contre, il est estimé que le traitement de données anonymes produites par un individu ne pose pas la nécessité d'un cadrage, ce qui permet par exemple l'adaptation de services selon des données globales plutôt qu'une personnalisation du service. Dans l'entre deux, une notion importante est celle de « pseudonymisation », qui n'est pas une anonymisation des données, mais une séparation de bases, avec ainsi des données à caractère personnel dans une base, des données liées dans une autre base sans que la première soit accessible à celui ou celle qui va se charger du traitement des données. C'est une notion qui peut être particulièrement importante pour le contexte de l'Éducation nationale.

Le règlement insiste sur les principes de consentement, de loyauté, de transparence, à l'égard de l'individu concerné par le traitement des données. Le sujet est particulièrement sensible pour des mineurs, quand ce sont les titulaires de la responsabilité parentale qui sont décisionnaires du consentement et garants pour leur enfant du respect de loyauté et de transparence. Deux contextes sont différenciés à ce sujet, celui d'usages personnels du numérique par l'enfant, sous la responsabilité plus ou moins lâche des titulaires de la responsabilité parentale, celui d'usages administratifs et scolaires « contraints » par les services publics concernés. La distinction est importante car le choix de rejeter le traitement des données n'existe pas pour l'enfant mineur dans le deuxième contexte (art. 6, § 1).

L'affranchissement d'une tutelle au consentement est posée à 16 ans par le règlement, avec liberté donnée aux États de descendre à 13 ans. Quel que soit l'âge, l'article 9 précise que « le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou

philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits. » Toutefois, au-delà de conditions particulières qui permettent ce traitement, celui-ci est autorisé dès que les données sont rendues publiques par l'individu.

Le règlement assure le droit pour l'individu d'accéder aux informations le concernant, d'en avoir connaissance (art. 12). De même l'individu doit pouvoir connaître le responsable du traitement et le cas échéant le délégué à la protection des données (art. 13). Il a droit de rectification (art. 16), le droit à l'effacement, ou droit à l'oubli (art. 17). En l'état du règlement ce droit à l'oubli ne semble avoir grande valeur tant les exceptions sont importantes en qualité, en matière de droit à la liberté d'expression et d'information pour le contexte général, « pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement » en ce qui concerne le contexte administratif et scolaire au sens « contraints ».

Un ensemble de dispositions sont prises pour préciser les obligations des responsables du traitement, mais aussi de sous-traitants éventuels, qui peuvent ainsi être des entreprises qui fournissent des services avec des données à caractère personnel fournies et manipulées par un établissement scolaire, entre autres. La question se pose notamment de la conservation des données par le sous-traitant, ainsi avec obligation de suppression ou transfert au responsable du traitement des données (art.28). Obligation est faite de tenir un « registre des activités de traitement » (art. 29), avec des informations sur ces activités, leurs finalités, leur durée. Notons que la désignation d'un délégué à la protection des données, ou DPD, est obligatoire dans les organismes publics (art. 37), sans obligation telle pour les entreprises privées dans la plupart des circonstances. Ce point peut être problématique au sens où le DPD peut avoir un rôle important de conseil à l'égard du responsable du traitement, en l'occurrence auprès du chef d'entreprise.

Le règlement exige de chaque État la mise en place d'au moins une autorité publique indépendante de contrôle, ainsi comme la CNIL. On peut toujours discuter du degré d'indépendance de celle-ci, notamment à l'égard des organismes publics, elle n'en est pas moins *a priori* compétente pour ce type de contrôle, à condition de disposer de moyens qui lui manquent actuellement. L'ambition du règlement, en matière de contrôle, des articles 51 à 67, avec des autorités, commissions, comités, peut surprendre, tant il peut complexifier largement les procédures, sans lisibilité pour l'usager à ce niveau. Le recours de l'usager se fait auprès de l'autorité de contrôle, quand il est débouté par le responsable du traitement.

Il est demandé aux États de « [concilier], par la loi, le droit à la protection des données à caractère personnel au titre du présent règlement et le droit à la liberté d'expression et d'information, y compris le traitement à des fins journalistiques et à des fins d'expression universitaire, artistique ou littéraire » (art. 85).

Une protection fragile des données

Si le règlement apparaît à maintes égards comme un progrès vis-à-vis des réglementations existantes, tout du moins au niveau européen, il se base toutefois beaucoup sur le principe d'un consentement pour lequel il faut s'assurer l'importance et la conscience. Là où, de ce fait, on aurait pu espérer des garde-fous à l'égard d'individus qui sont poussés au partage de données, c'est sans doute le contraire qui apparaît, avec une libération du traitement des données.

Ainsi, on peut toujours définir des données sensibles interdites au traitement, le simple fait de permettre leur traitement quand elles sont rendues publiques limite largement ce type de protection [2]. Ainsi, tout site web réseau

social proposant aux internautes une fois inscrits de donner ces informations, de manière explicite ou non, il apparaît que la protection est caduque, notamment chez des enfants mineurs qui, s'ils ont obtenu dans le meilleur des cas l'assentiment tutélaire, n'en sont pas moins généralement seuls devant la décision de donner ou non ces informations. Si l'on peut penser qu'il est logique de tirer parti de données rendues publiques, on peut aussi faire la différence entre publication et autorisation de traitement.

Le « droit à l'oubli » peut être aisément respecté par des sites web, soit par des procédures autonomes et automatiques sur les réseaux sociaux numériques, soit par une prise en charge humaine sur des forums, blogs et autres sites. Il en va autrement pour les services publics, avec une dérogation à cette protection. Il faut ainsi comprendre que l'absence de traitement numérique est impossible, que le droit consacre la numérisation du traitement à des fins de service public. Cela concerne la politique de gestion fiscale, au niveau national, mais aussi la gestion déconcentrée de données, dans des services variés, avec des moyens de protection des données plus ou moins fiables. Cela concerne les personnels administratifs, les fonctionnaires, leur vie professionnelle est en ligne en très grande partie, mais aussi les administrés, tous les administrés, dont les élèves.

Si le transfert de données semble encadré, il paraît difficile de ne pas trouver les failles tant le texte est alambiqué à ce sujet. Finalement, l'usager ayant donné son consentement, il n'y a pas d'obstacle particulier au transfert des données par le responsable du traitement, comme rien n'empêche les clauses minuscules ou illisibles donnant lieu à un consentement pour des usages divers et variés des données personnelles. La règle, pour les sites web, peut alors rester celle d'une collecte de données à caractère personnel la plus large possible, avec transfert à des services secondaires, auxquels l'usager adhère ensuite en acceptant lui-même le transfert des données, ou à des services tiers, avec alors tout de même une sécurité à attendre par pseudonymisation, si tant est qu'un contrôle soit possible pour observer cette sécurité.

Enfin notons que toute navigation, une fois le consentement octroyé, avec une rareté de sites web qui permettent de refuser le traçage en navigant dessus, tout concourt à un traitement de données, et que l'utilisation d'Internet, en soi, pour l'essentiel, suppose d'adhérer politiquement au principe d'une algorithmie prédictive et invasive. Si les navigateurs sur les ordinateurs de bureau permettent les navigations anonymes, sans *cookies*, ou l'installation d'*add-ons* qui bloquent les sites mouchards, il en va différemment des ordiphones notamment, sans aucune obligation légale de permettre ce type de paramétrages ou d'installations par ailleurs, tandis que les *add-ons* et applications permettant de supprimer les messages d'avertissement et de demande de consentement sont amenés à se développer [3].

Il est important enfin de préciser que le préambule au règlement est essentiel pour comprendre l'esprit du texte, mais aussi pour les suites qui peuvent être données par la Commission européenne et le Comité européen à la protection des données, qui a quant à lui notamment un rôle de conseil, de publication de lignes directrices, de recommandations et de bonnes pratiques. L'essentiel des éléments du préambule se retrouvent dans les articles du règlement, avec toutefois quelques développements plus importants dans ces paragraphes introductifs au sujet des enfants, en particulier pour la question très sensible du consentement.

Le paragraphe 32 défend l'usage que l'on connaît maintenant bien depuis quelques mois selon lequel on coche une case ou clique pour manifester son consentement à l'utilisation des données à caractère personnel, notamment par l'enregistrement de *cookies*. Au-delà de l'information qu'il donne sur l'enregistrement de *cookies* par le site, ce message généralisé apparaît finalement davantage comme une gêne pour les internautes, qui s'habituent et cliquent, plutôt que comme une information donnant lieu à un consentement conscientisé. Il en va de même pour les autorisations données lors des installations d'applis sur ordiphones, d'autant plus qu'alors la volonté d'installation précède l'accès, avec une frustration plus ou moins grande à ne pas consentir. Cette considération peut pousser à croire qu'il existe un abus de traitement de données à caractère personnelle, sauf si l'on estime à juste titre que les applis n'existeraient pas sans la capacité pour leurs responsables d'en tirer un parti financier par la récupération de données personnelles. C'est entre ces deux pôles que doit se positionner la loi, et c'est de toute évidence en faveur

de l'économie numérique qu'elle penche. C'est l'assentiment pour un modèle économique qui peut être considéré comme pervers à certains égards, toujours avec l'octroi de services gratuits quand la monnaie d'échange est la donnée à caractère personnelle, avec une valeur toute relative, assujettie à la capacité du service à capter une publicité plus ou moins valorisée.

Le paragraphe 38, s'il insiste sur une protection spécifique pour les enfants [4], ne permet en rien de comprendre les moyens concrets de cette protection. Car finalement, à moins d'interdire l'enregistrement et le traitement de données personnelles, on peut douter qu'une quelconque information pour consentement permette de freiner l'enfant. Il sera au mieux prudent, mais d'autant moins que la « pression sociale » à l'utilisation d'un service sera forte.

Si le paragraphe 58 est intéressant, dans une certaine bienveillance, il n'est pas particulièrement convaincant, tant il paraît délicat voire impossible de légiférer précisément sur ce sujet : « Le principe de transparence exige que toute information adressée au public ou à la personne concernée soit concise, aisément accessible et facile à comprendre, et formulée en des termes clairs et simples et, en outre, lorsqu'il y a lieu, illustrée à l'aide d'éléments visuels. Ces informations pourraient être fournies sous forme électronique, par exemple via un site internet lorsqu'elles s'adressent au public. Ceci vaut tout particulièrement dans des situations où la multiplication des acteurs et la complexité des technologies utilisées font en sorte qu'il est difficile pour la personne concernée de savoir et de comprendre si des données à caractère personnel la concernant sont collectées, par qui et à quelle fin, comme dans le cas de la publicité en ligne. Les enfants méritant une protection spécifique, toute information et communication, lorsque le traitement les concerne, devraient être rédigées en des termes clairs et simples que l'enfant peut aisément comprendre. » S'il existe peut-être un juste milieu entre la phrase sibylline précisant l'utilisation de *cookies* et les interminables conditions générales d'utilisation (CGU), il n'y a aucune raison que le message puisse être claire et limpide quand on sait la complexité des procédés de traitement des données personnelles à des fins variées.

Il ne faut pas oublier la question des droits sur les données, sur les contenus, qui n'est pas vraiment traitée dans le règlement. Ainsi, ce qui est fait de la donnée personnelle, quand il y a service avec production de contenus, publication de contenus, qui peut varier, du respect strict du droit d'auteur jusqu'au principe bien connu avec le « modèle » de *Facebook* de licences et sous-licences sur les contenus qui reviennent à nier la propriété intellectuelle sur ces contenus, en passant par la définition de la licence par l'utilisateur lui-même, ainsi selon le modèle de *Flickr* pour les photographies et autres illustrations.

Responsabilités et règles dans le contexte scolaire

Rappelons que l'individu sujet d'un traitement de données, ainsi concernés l'élève et le titulaire de la responsabilité parentale si l'élève a plus de 16 ans, doivent avoir connaissance du responsable du traitement et le cas échéant du délégué à la protection des données (DPD). Dans les établissements scolaires, pour l'un comme pour l'autre, le sujet est problématique. Cela pose la question de la responsabilité véritable d'un service dont l'existence est contrainte par l'administration centrale ou académique, de la connaissance de la durée du traitement, de son transfert à des tiers par la suite, de son archivage éventuel, de son enregistrement dans des bases nationales qui ne sont plus du ressort de l'établissement public local.

C'est ainsi le problème de tenir un registre des activités de traitement sans responsabilité intrinsèque quant au choix ou non du traitement. On peut se demander alors en quoi la responsabilité ne relève pas de responsabilités institutionnelles nationales, pour les outils obligatoires, que ce soit pour la gestion des données administratives en ligne, la tenue de cahiers de texte, la gestion numérique des évaluations, la mise en place d'un catalogue documentaire. Logiquement relèveraient alors de l'établissement uniquement les outils choisis au niveau local, comme un outil de publication en ligne qui ne relève pas d'une plateforme académique ou quelque logiciel en ligne que ce soit avec utilisation de données à caractère personnel. Il paraît difficile de donner une responsabilité légale à

des individus qui ne sont pas à l'origine du choix des outils déployés pour le fonctionnement de l'établissement, notamment en ce qui concerne la garantie de sécurité, alors qu'il semble évident qu'ils doivent garantir cette sécurité, par exemple avec le sous-traitant, quand ils ont effectivement choisi un service eux-mêmes.

Globalement donc, le choix opéré de désigner le chef d'établissement comme responsable du traitement, quel que soit le service numérique, pose question. Une délégation sur ce sujet dans chaque établissement scolaire paraît tout autant difficile que la délégation se base sur un volontariat voire une désignation, sans recrutement effectué à partir de compétences reconnues, avec le risque d'une responsabilisation contrainte et donc dans un cadre, soit inopérant, soit déresponsabilisant.

Le règlement permet de résoudre cette difficulté avec une délégation nationale à la protection des données pour chaque Ministère, ainsi une délégation pour l'Éducation nationale, avec une sous-traitance par délégations académiques de plusieurs personnels chargées, avec les compétences requises, de relever les activités de traitement dans les différents établissements. C'est alors une manière responsable de surveiller la licité de ces activités, avec des moyens plus opérants que ceux actuels de la CNIL. Cette solution est d'autant plus intéressante qu'elle peut obliger chaque établissement à prendre la responsabilité de signaler dans un formulaire académique cohérent l'ensemble des services utilisés qui supposent le traitement de données à caractère personnel, avant l'utilisation d'un service. Le cadre de la commission numérique ou informatique peut être l'occasion, avec des personnels de différents services, ainsi que des élèves et parents, de faire le point sur les outils et services employés avec données à caractère personnel, une fois par an.

Exigeant une autorité de contrôle indépendante, le règlement conforte le rôle en France de la CNIL. Pour autant, en matière de responsabilités, il n'est pas évident que la CNIL puisse être d'un quelconque recours dans l'Éducation nationale, que ce soit pour les parents, enfants ou personnels. Sur le sujet du consentement, il n'est pas évident de savoir qui définit et comment définir les usages administratifs et scolaires « contraints », par les services publics concernés, comment les distinguer de ceux qui ne le sont pas. On pourrait presque imaginer, en regard du règlement, une autorité de contrôle indépendante spécifique aux organismes publiques, avec des compétences particulières qui lui donnent davantage d'autorités pour faire face à d'éventuels blocages administratifs devant les irrégularités et devant les contestations par les usagers. Il convient effectivement que le recours s'opère auprès d'une instance spécifique, tant les dérogations des organismes publics semblent importantes, vis-à-vis du droit général, avec l'exigence de spécialistes dès l'engagement du recours.

Le paragraphe 39 du préambule au règlement précise que la protection des données « exige de garantir que la durée de conservation des données soit limitée au strict minimum ». Cette question n'est pas une mince affaire dans l'Éducation nationale, d'autant plus qu'il peut y avoir des dérogations en matière d'archivage pour les organismes publics. Il faudrait sans doute envisager à cet égard une réglementation claire, voire une diminution de la durée de conservation des données, d'une part afin que l'enfant soit protégé, à comprendre qu'il ne subisse pas l'existence d'une masse de données qu'il ne maîtrise pas, d'autre part afin que son processus d'apprentissages soit respecté, par exemple autour d'un cycle de trois ou quatre ans, afin que des données sur ces compétences, sur ces capacités, ne puissent être utilisés au-delà de leur valeur intrinsèque, dans sa construction et son évolution personnelles. Si tant est que l'on estime que les données puissent être un vecteur de progrès, ce qui exigerait sans doute une décision politique d'ordre général, par référendum, encore faut-il que chaque citoyen soit sensible à la question, la pseudonymisation doit être rejetée pour l'anonymisation dès qu'il n'y a plus d'intérêt pour l'individu à ce que les données lui soient associées. La question est notamment à débattre de l'intérêt d'une conservation des données relatives aux apprentissages de l'élève, pour l'élève, via un identifiant national unique tel que préconisé par François Taddéi, Catherine Becchetti-Bizot et Guillaume Houzel dans un rapport publié en avril 2017 [5], également mentionné, pas nécessairement à cette fin, par la Commission européenne dans le RGPD.

On peut enfin questionner l'utilisation de services externes à l'Éducation nationale dans les établissements scolaires et le consentement des usagers à cet égard, principalement les élèves et les titulaires de la responsabilité parentale.

Car en l'état il existe de nombreuses pratiques problématiques, et surtout un flou juridique qui devrait être clarifié. Plusieurs questions méritent ainsi sans doute des clarifications législatives, au-delà de simples recommandations et d'adaptations fragiles d'autres textes. Un enseignant peut-il publier des documents d'élèves sur le Web, en matière de données personnelles identifiables ou de propriété intellectuelle ? Si oui, sur quels types de sites web peut-il publier ? Avec quel consentement ? Si la question ne se pose *a priori* pas pour les parents sur des photos de leurs enfants, quid de la publication, dans l'absolu, de photos d'élèves par les personnels de la communauté scolaire ? Est-il licite d'utiliser des services en ligne dans le cadre scolaire avec les élèves en demandant aux élèves de créer leur propre compte ou d'utiliser leur compte personnel ? Selon quels services, à quelles conditions ? En quoi peut-on considérer qu'il y a promotion d'un modèle économique, au-delà d'une certaine neutralité, quand on engage des élèves à créer un compte tel dans le cadre scolaire, ou encore à utiliser des services bureautiques qui seront amenés, dans des utilisations ultérieures, à récolter leurs données personnelles en contrepartie du service ?

Si l'on en revient aux objectifs de l'école, il faut bien sûr mettre ces questions en relation avec deux questions essentielles : en quoi se passer de ces services, si c'est un problème, revient à nier certains enjeux d'une éducation dans la société de l'information, et comment pallier ce refus de travailler sur des services qui peuvent être plébiscités par ailleurs ? Quelles sont les alternatives à ces services et quels moyens se donne-t-on pour les proposer aux équipes éducatives, en matière d'infrastructures et de moyens humains ? Les réponses supposent au préalable de ne pas considérer l'éducation comme une potentielle manne pour l'économie numérique, mais aussi de considérer qu'une réponse adéquate suppose des moyens budgétaires associés.

Conclusion

Par son insistance sur la nécessité de protéger les données à caractère personnelle, le règlement général européen sur la protection des données apparaît comme une avancée de principe pour l'individu et sa capacité à maîtriser les données qu'il est amené à donner ou que d'autres peuvent enregistrer à son sujet sur Internet. A maintes égards toutefois on peut douter de l'efficacité de telles règles. Les contraintes pour les responsables de traitement peuvent être techniques, en matière de sécurité, en matière d'information, mais elles sont surtout très formelles, à la recherche d'un consentement à l'utilisation plus ou moins importante des données collectées. Si la commission insiste sur la clarté et la transparence, dans ce consentement, on peut avoir l'impression d'une certaine naïveté à ce sujet, pour les enfants comme pour les adultes, tout simplement parce qu'il y a une économie numérique à soutenir, en parallèle, économie qui s'appuie sur la donnée personnelle comme monnaie d'échange contre les services proposés. De là les contraintes sur le fonds semblent rejetées, non par principe en théorie car le Parlement européen ne soutient pas cette monétisation des données personnelles, mais par principe de réalité, sans que les États membres soient amenés à s'opposer légalement à cette monétisation.

Dans le cas particulier des organismes publics et de l'Éducation nationale, la question se pose bien sûr du recours à des services en ligne extérieurs qui basent leur modèle économique sur la donnée à caractère personnelle. C'est un ensemble à clarifier. Il s'agit aussi de continuer de travailler sur l'utilisation de la donnée élève à l'intérieur de la structure, malgré les dérogations dérangeantes du RGPD à ce niveau spécifique de mineurs, parmi les dérogations relatives aux services publiques à l'égard du numérique. Des avancées peuvent être attendues pour des responsabilités logiques selon les outils et la contrainte imposée pour tel ou tel outil, pour des durées de conservation réduites des données personnelles, pour une meilleure information des enfants et parents au sujet de cette collecte de données, information quasiment inexistante aujourd'hui, voire pour un droit de regard et de retrait sur certaines informations.

En complément

Deux articles parus pendant l'écriture de cet article, en complément ou en parallèle :

- Pour le Parlement européen, nos données personnelles ne sont pas des marchandises ! *In* La Quadrature du net [en ligne], 21 nov. 2017. Disponible sur : https://www.laquadrature.net/fr/contenu_num_pe
- FAVIER Manon. Le RGPD : il n'est pas trop tard pour s'organiser ! *In* Medium [en ligne], 22 nov. 2017. Disponible sur : https://medium.com/@mfavier32/le-rgpd-il-nest-pas-trop-tard-pour-s-organiser-8756d0175c53

---

[1] Version française notamment disponible sur le site de la CNIL : https://www.cnil.fr/fr/reglement-europeen-protection-donnees

[2] Art.9, al.2, e)

[3] A noter que la commission européenne est favorable à un paramétrage du navigateur pour automatiser le consentement...

[4] « Les enfants méritent une protection spécifique en ce qui concerne leurs données à caractère personnel parce qu'ils peuvent être moins conscients des risques, des conséquences et des garanties concernées et de leurs droits liés au traitement des données à caractère personnel. Cette protection spécifique devrait, notamment, s'appliquer à l'utilisation de données à caractère personnel relatives aux enfants à des fins de marketing ou de création de profils de personnalité ou d'utilisateur et à la collecte de données à caractère personnel relatives aux enfants lors de l'utilisation de services proposés directement à un enfant. Le consentement du titulaire de la responsabilité parentale ne devrait pas être nécessaire dans le cadre de services de prévention ou de conseil proposés directement à un enfant. »

[5] Rapport disponible sur : http://www.education.gouv.fr/cid115649/vers-une-societe-apprenante-rapport-sur-la-recherche-et-developpement-de-l-education-tout-au-long-de-la-vie.html Lecture critique de ce rapport sur : https://profdoc.iddocs.fr/spip.php?article76