UNIVERSITE POLYTECHNIQUE DE BINGERVILLE (UPB)
COURS DE REGLEMENT GENERAL SUR LA PROTECTION DES DONNEES (RGPD) – MASTER -

INTRODUCTION

Le phénomène juridique entend encadrer toutes les activités humaines du moment où celles-ci ont des impacts sociaux. Cela est d'autant vrai que le droit se définit, au plan objectif, comme l'ensemble des règles qui régissent les rapports sociaux et dont la violation est sanctionnée par l'autorité publique. Dans cette dynamique, l'outil informatique, les activités qui s'y rattachent n'échappent pas à l'encadrement du droit. Les activités liées aux TIC sont nouvelles et se renouvellent sans cesse si bien qu'on a l'impression que le droit tente de les découvrir. En effet, si des domaines traditionnels du droit tels que le droit au respect à la vie privée, à l'honneur, à la dignité, à l'image permettent d'encadrer les activités des TIC, une part importante de ces activités échappent aux contenus traditionnels du droit. C'est au niveau de la protection des droits relatifs à la vie privée que l'on recourt à l'encadrement des données personnelles.

L'objet de ce cours renvoie d'ailleurs au Règlement général de la protection des données. Bien qu'intervenant en droit ivoirien, le RGPD a une origine européenne (Droit européen). Aussi l'historique de la matière nous invite à revisiter l'histoire de la RGPD en France (Chapitre I) avant d'examiner sa réception en droit communautaire de l'UEMOA (Chapitre II). Le but du règlement étant la protection des droits, il importe, enfin, de décliner certains de ceux-ci (Chapitre III).

CHAPITRE I : HISTORIQUE DU RGPD

Le RGPD a certes des traces dans la législation française qui demeure comme un instrument précurseur de la protection des données (Section 1). Mais, c'est au sein du droit européen que le RGPD s'est véritablement construit (Section 2).

SECTION 1 : DES PREMICES FRANÇAISES

Si denses soient-elles, les premières règles du RGPD peuvent être résumées en deux temps : la loi de 1978 (paragraphe 1) et la loi de 2004 (paragraphe 2).

Paragraphe 1 : La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, au fichier et aux libertés

Avant 1978, aucune loi ne régissait, en France, la conservation informatisée de données ; cela s'explique par l'ancien système destockage entièrement mécanique (mécanographie). Notons toutefois que des doutes sont émis dès 1970, année où un député, propose la création d'un «tribunal de l'informatique», mais cette idée sera temporairement abandonnée. C'est en 1974 que le journal *Le Monde* révèle un scandale détaillé : le projet SAFARI, initié par l'INSEE (Institut National de la Statistique et des Etudes Economiques, consistant à informatiser les fichiers régionaux d'état civil pour les rendre nationaux – ce qui pourrait, selon ses opposants, permettre le fichage des français – ainsi que de les interconnecter avec le fichier des cartes d'identités et d'assurance vieillesse–dans un premier temps, le projet sera modifié ensuite, et n'aboutira finalement pas.

Suite au scandale provoqué par l'article du *Monde* – qui jugea le projet trop vaste et permettant le fichage des français, le nouveau président Valéry Giscard d'Estaing décide la création d'un organisme de contrôle des données personnelles dans la société de l'information : la CNIL (Commission Nationale de l'Informatique et des Libertés), et avec elle est promulguée une loi majeure, la loi de 1978 dite « Informatique et libertés ». Cette loi précurseur présente des atouts certains. Ces atouts sont déclinés en termes d'objectifs poursuivis par ladite loi. En effet,

- L'informatique doit être au service de chaque citoyen

C'est en effet de cette phrase que découle le reste du texte, qui pose la définition de la donnée à caractère personnel – définition d'ailleurs sensiblement identique à celle du RGPD - . Le texte fonde également des principes concernant les données personnelles dont :

— le droit d'information : chacun peut être informé des traitements dont ses données font l'objet, cet article est applicable en toutes circonstances, même aux cas relevant de la sécurité nationale;
— le droit d'accès : plus complet que le droit d'information, il permet à chacun d'accéder aux informations qui sont conservées sur lui, il est toutefois interdit d'en faire usage dans certains cas;
— le droit de rectification : chacun peut demander à faire corriger les données stockées le concernant;
— le droit d'opposition : chacun peut s'opposer à faire l'objet d'un traitement, pour un motif légitime (le démarchage commercial est reconnu par la loi

comme motif légitime). Ces droits se retrouveront amplifiés et adjoints à d'autres, dans le RGPD.

Cette loi fut améliorée par une autre intervention législative en 2004.

Paragraphe 2 : La loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel

En 2004, deux facteurs, nommément le début de la marchandisation des données et la traçabilité (le fait que de plus en plus de traces informatiques sont laissées au quotidien), poussent le législateur à réviser la loi de 1978. En France, cette fois en retard sur l'Europe (qui pousse la directive correspondante en 1995), le contrôle *a priori* de la CNIL (contrôle avant l'utilisation des données), devenu trop encombrant, est transformé en un contrôle *a posteriori* (contrôle après l'utilisation des données), mais bien plus contraignant, en effet, celle est maintenant capable de prononcer des sanctions :

— injonction à cesser le traitement;
— retrait de l'autorisation de traitement ;
— suppression de certaines données ;
— sanction pécuniaire pouvant aller jusqu'à 150000 € pour les contrevenants.

La nouvelle loi met aussi en place un nouveau système relatif à la déclaration des fichiers et traitements ; toute structure souhaitant effectuer un traitement de données à caractère personnel oustocker ces données doit effectuer une déclaration à la CNIL, sauf dans certains cas (mais la déclaration devient la norme). On note toutefois que l'État devient soumis au même régime de déclaration simple, alors qu'il était auparavant soumis à une demande d'autorisation de par la nature très personnelle des données qu'il collecte.

Ces dispositions forts intéressantes soient elles présentaient des lacunes. Aussi, le RGPD fut-il créé en droit européen en les modifiant et les améliorant.

SECTION 2 : UNE CONSOLIDATION EUROPEENNE (Droit de l'UE)

En janvier 2012, la Commission européenne, consciente de l'absence de consensus sur la protection des données personnelles dans l'ensemble des pays de l'Union, et jugeant le sujet important, décide de rédiger un règlement. De nombreux pays membres sont consultés, et un premier jet du règlement est proposé par la Commission européenne en novembre 2013.

Le texte commence alors à être discuté le 11 mars 2014 par le Parlement européen, qui le modifie, et l'adopte le jour suivant en première lecture. Les négociations se poursuivent rapidement, entre la Commission européenne, le Parlement européen et le Conseil de l'UE, qui aboutiront au texte final le 15 décembre 2015.

Ainsi, la procédure d'adoption de ce texte s'est étalée sur une longue période durant laquelle les divers acteurs (États, entreprises et citoyens), ont pu participer au processus de création, le tout, afin d'essayer d'obtenir un texte équilibré, à la fois protecteur des personnes, et laissant une certaine liberté aux entreprises et administrations publiques.

La consolidation européenne est d'un atout indéniable à un double égard : elle permet une harmonisation des règles relatives aux données des Etats membres de l'UE (paragraphe 1) et protège davantage les droits et libertés fondamentaux (paragraphe 2).

Paragraphe 1 : L'harmonisation des règles européennes en matière de protection des données

Le droit de l'UE sur les données est construit à partir d'un cadre harmonisé. En d'autres termes, tous les Etats-membres de l'Union européenne sont soumis aux mêmes règles, ce qui facilite la circulation des données personnelles à travers l'UE. Pour les données en dehors de l'Union, le règlement est très strict également, puisque celles-ci sont soumises au règlement dans de très nombreux cas. Le droit communautaire sous régional africain auquel appartient la Cote d'Ivoire a épousé la même logique et dynamique.

Concrètement, toute donnée concernant un citoyen européen, même traitée hors union, est dans le champ d'application du règlement ; c'est un cadre très large et protecteur pour les Européens. Notons d'ailleurs que le règlement européen sur les données de 2012 concerne exclusivement les personnes physiques.

Paragraphe 2 : La protection des droits et libertés fondamentaux

Pour les structures y compris les administrations traitant de la donnée personnelle, le principe de déclaration obligatoire à la CNIL est transformé en principe de responsabilité, permettant bien plus de souplesse, mais augmentant les sanctions. L'idée est que la structure traitant les données personnelles doit être en mesure de démontrer que les principes de protections sont respectés, et la CNIL pourra contrôler la structure de manière inopinée ; le contrôle, déjà partiellement effectué *a posteriori*, l'est maintenant intégralement, puisque la CNIL ne vérifie rien avant contrôle. En cas de délit constaté lors du contrôle, les amendes sont désormais dissuasives, puisqu'elles peuvent aller jusqu'à 4% du chiffre d'affaire mondial de l'entreprise, une belle somme.

A titre de comparaison, cette règle des 4% de chiffre d'affaires appliquée au réseau social Facebook nous donne, pour l'année 2017, plus d'un milliard et 300 millions d'euros.

En ce qui concerne les utilisateurs, leurs droits sont renforcés, avec notamment l'arrivée du consentement « explicite » : le traitement des données personnelles est soumis à un consentement qui ne peut être forcé ; particulièrement, l'accès au service ne peut être conditionné à acceptation de traitement de données qui n'y seraient pas directement nécessaires.

Par ailleurs, le règlement consacre aux utilisateurs les droits mentionnés à la partie traitant du droit français, à savoir :

- le droit d'information, remplacé par un principe de « transparence de l'information », assez précisément défini, notamment en ce qui concerne les informations à communiquer ;
- Le droit d'accès, qui reste quasiment le même, à ceci près que la durée de conservation doit maintenant être précisée ;

- le droit de rectification, géré de manière identique: tout changement de la part de l'utilisateur doit être répercuté;

- le droit d'opposition, à la fois complété et fragilisé, pour former un « droit à l'effacement », qui reste finalement peut-être le point le moins protecteur de la nouvelle législation, en cela qu'il ne prévoit que six cas ouvrant droit à opposition.

A ces droits existants précédemment, le RGPD en créé deux nouveaux :

- le droit à la limitation du traitement, qui est une sorte de droit à l'effacement allégé, qui permet de laisser ses données à la structure responsable du traitement, mais de lui demander de les marquer pour limiter leur utilisation future ;

- le droit à la portabilité, fruit d'une longue bataille des associations de défense des droits des citoyens ; il permet à chacun de demander l'intégralité des données à caractère personnelles concernant. Ces données doivent être transmises « dans un format structuré, couramment utilisé et lisible par [une] machine », et il est autorisé d'aller mettre ces données dans un autre traitement, sans que le responsable du premier (celui à qui on demande la portabilité) ne puisse s'y opposer.

Imitant le droit de l'UE, l'UEMOA va reprendre l'essentiel des règles du RGPD telles qu'elles viennent d'être traitées.

CHAPITRE II : LE RGPD EN DROIT COMMUNAUTAIRE SOUS REGIONAL AFRICAIN (CEDEAO, UEMOA)

Le 16 février 2010, la Communauté Economique Des Etats de l'Afrique de l'Ouest (CEDEAO) prenait **l'Acte Additionnel A/SA.1/01/10 relatif à la protection des données à caractère personnel** ; lequel acte, est également applicable aux Etats membres de l'UEMOA. A ce jour, plus de la moitié des Etats signataires se sont inspirés de cet Acte pour asseoir une législation nationale de protection des données à caractère personnel (DCP).

Le Règlement Général sur la Protection des Données numéro 2016/679 du 27 avril 2016 (RGPD), en application depuis 2018 dans les Etats membres de l'Union Européenne, semble avoir fait le tour de la question sur la protection des données personnelles et apparaît plus adapté, selon les observateurs, aux défis actuels dictés par l'usage quotidien de l'outil numérique. La présente étude se propose de faire un comparatif de ces deux textes juridiques appelés à garantir, chacun de son côté, la protection des données personnelles dans des espaces communautaires différents, mais combien liés par des enjeux économiques importants.

Une lecture croisée de ces textes révèle les grands principes de traitement des données applicable en droit des Etats membres de la CEDEAO notamment la Côte d'Ivoire. Ces principes se rapportent au fondement même du traitement (Section 1) ainsi qu'aux obligations du responsable du traitement des données (Section 2).

Section 1 : Les grands principes du traitement

La notion de grands principes fait référence aux règles qui gouvernent le traitement des données à caractère personnel. A chaque traitement est assigné un but, un objectif, à ne pas outrepasser, au risque de tomber dans l'illégalité ou l'illégitimité par rapport au RGPD et à l'Acte Additionnel. Ces deux textes s'accordent pour définir le traitement, lequel doit être licite, c'est à dire être fait dans le cadre d'une activité professionnelle. Les informations collectées par une entreprise auprès de sa clientèle en vue d'effectuer par exemple une livraison, éditer une facture ou proposer une carte de fidélité, constituent dans leur ensemble, un traitement des données personnelles ayant pour objectif la gestion de sa clientèle. Le traitement de données à caractère personnel au regard du RGPD fait appel à plusieurs grands principes, notamment ceux de transparence, loyauté, limité dans la durée et les finalités, etc.

Les impacts sont de deux ordres : au plan interne (paragraphe 1) et externe (paragraphe 2)

Paragraphe 1 : Sur le plan interne

Les organismes devront pour certains :

- désigner un délégué à la protection des données, chargé de contrôler la conformité de l'entreprise à la règlementation sur la protection des données personnelles,

- pour les entreprises de plus de deux cent cinquante employés ou qui réalisent certains types de traitements, elles devront constituer et tenir à jour un registre des activités de traitement.

- et dans tous les cas, mettre en place des procédures internes permettant d'assurer la « protection des données dès la conception » des traitements (*Privacy by design*) et mener des analyses d'impact, préalables à la mise en œuvre de certains traitements.

Paragraphe 2 : Sur le plan externe

Les organisations concernées devront prendre des mesures :

- à l'égard des personnes concernées, en mettant à jour les mentions d'information ainsi que les modalités de recueil du consentement,

- à l'égard de l'autorité de contrôle, mettre en place un dispositif permettant de lui notifier la survenance d'une violation des données engendrant « un risque pour les droits et libertés des personnes physiques », notification qui devra être étendue à l'ensemble de ces personnes physiques, si ce risque est « élevé ».

- à l'égard des autres acteurs non institutionnels du traitement, établir des contrats écrits non seulement avec les sous-traitants, mais aussi avec les responsables conjoints de traitement, en énumérant et répartissant précisément les rôles et responsabilités de chacun.

Tous ces principes ont pour objectif de garantir les droits de l'individu sur son « or noir » et de mener les organisations à plus de responsabilité et de confidentialité dans le

traitement des DCP. Même si les principes mis en avant dans l'Acte Additionnel, à savoir les principes de consentement, légitimité, licéité, loyauté, finalité, pertinence, conservation, exactitude, transparence, confidentialité, de sécurité et du choix du soustraitant sont édictés, l'on peut relever que le RGPD a englobé des notions non prises en compte dans l'Acte Additionnel, notamment celle de la protection des données dès leur conception. Ultimement, ces grands principes servent à mesurer l'ampleur des obligations qui pèsent sur le responsable du traitement.

Section 2 : Les obligations du responsable du traitement

Le RGPD définit le responsable de traitement comme toute personne, entreprise, organisme, autorité publique « qui détermine les finalités et les moyens d'un traitement de données ».
Dans la pratique, le responsable de traitement est la personne morale (entreprise, collectivité, association, etc.) incarnée par son représentant légal (président, gérant, maire…) qui est à l'origine et qui réalise le traitement. Le traitement tel que défini dans les deux textes, consiste en diverses opérations. L'on pourrait citer à titre d'exemples :

- la collecte d'informations de clients pour l'achat et/ou la livraison de biens ou pour la confection de cartes de fidélité ;
- la conservation d'informations d'identification sur les salariés par les ressources humaines ;
- la mise en place d'un système de vidéosurveillance, etc.

Sur cette base, plus de la moitié de la population mondiale a eu une fois au moins ses données traitées, sans toutefois savoir que ce traitement obéissait à des principes, et que son consentement était nécessaire avant tout traitement.

Tout compte fait, le responsable de traitement est soumis à des obligations générales (paragraphe 1) dont l'inobservation ou le défaut de conformité, est susceptible d'engager sa responsabilité (paragraphe 2).

Paragraphe 1 : Les obligations générales du responsable du traitement

Le responsable du traitement est soumis à diverses obligations, au nombre desquelles :

- obligation de licéité du traitement : le responsable de traitement doit traiter les données en conformité avec le RGPD de manière loyale, licite, transparente. Par exemple, si le traitement repose sur le consentement d'une personne, le responsable de traitement doit être en mesure de rapporter la preuve de ce consentement ;

- obligation d'information : pour la réalisation d'un traitement, le responsable de traitement a l'obligation d'informer les personnes concernées de la catégorie de traitement des données, leurs utilisations, les finalités du traitement, etc ;

- obligation de sécurité : le responsable de traitement a l'obligation de mettre en place des dispositions permettant de sécuriser les données traitées. Et, en cas de violation des dispositions de protection des données, il est tenu d'en informer la CNIL et, dans les cas les plus graves, les personnes concernées ;

- obligation de prise en compte des droits des personnes : le responsable de traitement doit faciliter l'exercice de leurs droits pour les personnes concernées et prendre en compte les demandes liées à l'exercice de ces droits.

Dans l'Acte additionnel, il faut retenir, au titre des obligations du responsable de traitement :

- les obligations de confidentialité : le traitement des données à caractère personnel est confidentiel. Il est effectué exclusivement par des personnes qui agissent sous l'autorité du responsable du traitement et sur ses seules instructions.
- les obligations de sécurité : le responsable du traitement est tenu de prendre toute précaution utile au regard de la nature des données et notamment, pour empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès.

- les obligations de conservation : les données à caractère personnel doivent être conservées pendant une durée fixée par un texte réglementaire et uniquement pour les fins en vue desquelles elles ont été recueillies ;

- les obligations de pérennité : le responsable du traitement est tenu de prendre toute mesure utile pour assurer que les données à caractère personnel traitées pourront être exploitées quel que soit le support technique utilisé.

Le RGPD a une vocation extraterritoriale, puisqu'il impose des obligations aux responsables de traitement et aux sous-traitants établis hors de l'Union Européenne. Et par voie de conséquence, s'applique également en Afrique, dès lors que ces responsables traitent des données de personnes physiques résidentes européennes ou encore, lorsque le responsable de traitement est une filiale ou une entité d'une personne morale de droit européen ou lorsque les données traitées concernent des personnes morales de droit européen.

L’impact de cette réglementation est significatif, puisqu’avec le RGPD, le sous-traitant même situé hors UE est pleinement responsable en cas de manquement aux obligations du RGPD. Plusieurs personnes peuvent être responsables de traitement : le RGPD contrairement à l’Acte
additionnel prévoit les cas de co-responsabilité. Dans un tel cas, un accord doit définir précisément les obligations et le partage de responsabilités de chacune d'elles.

Quel que soit le texte, le responsable de traitement engage sa responsabilité en cas de non-respect de ses obligations.

Paragraphe 2 : La responsabilité du responsable du traitement

Le responsable de traitement est tenu d’assurer la conformité du traitement qu’il réalise. Cela implique la prise de toutes les mesures nécessaires pour assurer cette conformité et d’être en mesure de démontrer la conformité du traitement au RGPD. C’est la consécration du principe général d’accountability. Le responsable de traitement, en fonction du traitement envisagé, doit donc évaluer les risques potentiels qui peuvent survenir et prendre toutes les mesures adéquates. Par exemple, pour certains traitements, notamment les données à caractère sensibles, des mesures supplémentaires devront être prises, comme la réalisation d’une étude d’impact ou un hébergement spécifique de ces données.

Par ailleurs, si le responsable du traitement recourt à des sous-traitants, il devra s’assurer de ce que ces derniers opèrent en conformité avec le Règlement, sous peine de voir sa responsabilité engagée personnellement.

Les sanctions prévues à l’encontre du responsable, essentiellement administratives peuvent aller jusqu’à une amende de vingt millions (20 000 000) d’euros ou, pour les entreprises, jusqu’à 4% du chiffre d’affaires mondial. L’Acte additionnel fait référence à une sanction sous forme d’amende, sans en préciser le montant.

Outre cette amende, des sanctions administratives peuvent être prononcées, telles que le retrait provisoire de l’autorisation de traitement accordée. Le retrait définitif peut également être prononcé par l'Autorité de protection. Lorsque le traitement est mis en œuvre pour le compte du responsable du traitement, celui-ci a grand intérêt à choisir un sous-traitant offrant des garanties suffisantes de capacité et de compétence. Il incombera au responsable du traitement et à son sous-traitant de veiller au respect des mesures de sécurité définies par l'Acte additionnel.
Le traitement des données appelle donc à une extrême vigilance pour le responsable de traitement, au regard de ses implications et sanctions, en cas de violation.

Le contrôle et l'encadrement juridique du traitement sont spécifiquement garantis en Côte d'Ivoire par l'ARTCI.

CHAPITRE III : L'AUTORITE DE REGULATION ET LA MISE EN CONFORMITE DU TRAITEMENT EN COTE D'IVOIRE

Il ressort d'un état des lieux de la protection des données en date du 22 janvier 2022, qu'une autorité de protection des données à caractère personnel existe dans six (6) Etats de l'UEMOA sur un total de huit (8).

Le Togo dispose d'une loi dédiée à la protection des données et est sur le point de se doter d'une autorité de régulation.

La Guinée-Bissau pour sa part ne dispose d'aucune législation ni d'une autorité de protection des données à caractère personnel. Il faut espérer que les enjeux économiques liés à la protection des données personnelles décideront les autorités compétentes de ce pays à se doter d'un cadre normatif de protection des données.

En Côte d'Ivoire, la régulation est confiée à l'ARTCI

Section 1 : L'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire

L'Acte additionnel de la CEDEAO applicable dans l'espace UEMOA recommande que chaque Etat membre mette en place une Autorité de protection des données à caractère personnel.

En Côte d'Ivoire, l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI) a été créée par l'ordonnance numéro 2012-293 du 21 mars 2012 à l'issue de la fusion du Conseil des Télécommunications de Côte d'Ivoire (CTCI) et de l'Agence des Télécommunications de Côte d'Ivoire (ATCI).
C'est une autorité administrative indépendante qui a pour mission, en autres20, la protection des données personnelles. Elle exerce trois types d'attribution :

- informer et sensibiliser les populations et les responsables de traitement sur leurs droits et obligations ;

- réceptionner les demandes et l'octroi des récépissés de déclaration et la délivrance des autorisations pour le traitement des données à caractère personnel ;

- elle exerce un contrôle proactif du respect des dispositions légales en matière de protection des données à caractère personnel, la réception des réclamations et des plaintes des personnes concernées et la sanction le cas échéant, de la violation de la loi.

L'ARTCI exerce en la matière cinq (5) types de contrôle conformément à l'article 4 de la Décision n° 2021-0676 du 4 août 2021 portant procédure de contrôle en matière de protection des données à caractère personnel.

De Janvier 2019 à Décembre 201922, plus de cent cinquante (150) organismes ont saisi l'Autorité, soit par appels téléphoniques, courriels, lettres physiques, en vue d'obtenir des renseignements ou de se mettre en conformité avec la législation en vigueur. Cela dénote de l'intérêt croissant pour la problématique relative à la protection des données à caractère personnel. Plusieurs entreprises ont également été auditées dans le cadre de leur procédure de mise en conformité24. La loi du 19 juin 2013 relative à la protection des données à caractère personnel donne le cadre général des formalités à accomplir pour les entreprises engagées dans le traitement des DCP et informe sur le régime des autorisations.

Section 2 : Les droits protégés par la régulation en Côte d'Ivoire (la vie privée)

Plusieurs droits sont protégés par l'ARTCI à travers le RGPD. Ce sont les droits relatifs au nom, le domicile, l'adresse, le patrimoine… Cet ensemble de droits renvoie à ce que l'on qualifie de droit à la vie privée (paragraphe 1) et leurs violations entrainent des sanctions (paragraphe 2).

Paragraphe 1 : Sens et contenu du droit à la vie privée

La protection de la vie privée est affirmée par plusieurs textes internationaux et nationaux de valeurs juridiques différentes certes, mais presque toutes obligatoires. Exemple : article 12 de la Déclaration Universelle des droits de l'homme ; la loi n° 2013450 du 19 juin 2013 et la Constitution ivoirienne. La jouissance au droit à la vie privée permet au sujet de droit que ne soit point divulguer ou diffuser des informations qui porte sur un élément de la vie privée sans son consentement. Cela est un principe qui est faiblement assorti d'exceptions. Quelles sont donc les composantes de la vie privée ? On peut affirmer que les éléments de la vie privée se rapportent à l'identité de la personne, son intimité, la santé, les souvenirs et les convictions religieuses de la personne.

A- L'identité de la personne

L'identité est tout ce qui permet de distinguer l'individu parmi tant de personnes. Le juge français a ainsi sanctionné une revue qui avait consacré un article à l'artiste Jean Ferrat. L'article avait en effet dévoilé son véritable nom. La revue a été condamnée pour avoir porté atteinte à l'identité de la personne.

B- L'intimité de la personne

L'intimité de la personne recouvre divers éléments.

1- La nudité

L'exposition de la nudité au public d'une personne sans son consentement ou son contentement est constitutive d'une atteint à sa vie privée.

2- La vie conjugale

Elle concerne toutes les situations dans lesquelles la vie sentimentale de l'individu est exposée.
On situe ces situations à deux niveaux : les fiançailles et le mariage.

a- Les fiançailles

Faisant partie de la vie sentimentale de la personne, les fiançailles sont protégées ; et la divulgation de toutes informations y relatives est sanctionnée.

b- Le mariage

Le 16 février 1974, le Tribunal de Paris a rappelé que la diffusion du mariage de Jhonny Halliday et de Sylvie Vartan était une atteinte à leur vie privée. Pour le Tribunal, il revenait aux intéressés de fixer les limites des informations liées au mariage qu'ils souhaitaient partager avec le public.

c- Le divorce

Il est interdit de rendre compte ou de reproduire les pièces sur la procédure de divorce ou le divorce lui-même.

3- La maternité

Dévoiler l'état de grossesse ou la situation de nourrice d'une personne est qualifié de violation de la vie privée de la personne concernée.

4- L'esthétique

Révéler un défaut physique caché d'une personne est une atteinte à l'esthétique de la personne ainsi qu'une violation de son droit à la vie privée.

C- La santé de la personne

Toutes informations rendues publiques sans le consentement de la personne et qui concernent son état de santé ou des examens médicaux auxquels elle aurait été soumise sont constitutives de violation du droit à la vie privée.

D- Les souvenirs

Nul n'a le droit de publier les souvenirs d'une personne même de bonne foi, c'est-à-dire sans intention malveillante.

E- Les convictions religieuses, politiques et philosophiques

Toutes publications qui dévoilent les croyances sus-indiquées d'un groupe de personne ou d'une personne sont interdites.

F- Le patrimoine

Le patrimoine constitue, en partie, la richesse dont dispose une personne. L'on ne peut les exposer à l'insu du concerné. Cependant, en matière politique, ce principe peut être atténué. Ces éléments de la vie privée sont protégés de sorte que leurs violations emportent des sanctions.

Paragraphe 2 : Sanctions à la violation de la vie privée

Deux types de sanctions sont prévus en cas d'atteinte à la vie privée de la personne : sanction civile et sanction pénal.

A- Sanctions civiles

Ce sont : l'indemnisation financière du préjudice subi par la victime. Parfois, l'indemnisation peut être suivie d'autres ou d'une sanction non financière : la séquestre et la confiscation.

B- Sanctions pénales

Ce sont : l'emprisonnement ; l'amande ou les deux. L'application de l'amande suppose que le préjudice subi doit être suffisamment grave en raison de ses effets ou la nature de la personne coupable.

CONCLUSION

La problématique de la protection des données à caractère personnel, se pose avec plus d'acuité avec l'usage croissant de l'outil numérique, qui offre plus de souplesse et d'opportunités dans sa gestion quotidienne. Ces avantages qui comportent en eux leurs propres inconvénients, en raison de l'exposition de flux importants de données à un public indéterminé et inquantifiable, comporte des risques et enjeux importants que de nombreux textes sur divers continents, ont eu pour vocation de réduire ou juguler.

Ces textes, notamment l'Acte additionnel du 16 février 2010 et le RGPD du 27 avril 2016, ont l'avantage de répondre à ce besoin de sécurité des personnes dont les données personnelles sont au quotidien, l'objet de traitement, à des fins diverses. En cela, ils constituent une évolution qualitative.

Cet objectif fort louable peut se retrouver quelque peu distancé par la vitesse de transformation du vecteur de ces données que sont les télécommunications et les nouvelles technologies, devant donner lieu à une capacité d'adaptation permanente de la législation en la matière, voire à une législation prospective. Faute de quoi, les dispositions textuelles peuvent se trouver assez vite dépassées.

C'est déjà le cas pour l'Acte Additionnel de 2010, qui devra faire sa mue.

Conscients de ces faiblesses, la plupart des Etats membres de l'UEMOA ont adopté des législations récentes dont les dispositions pour certaines, dépassent le cadre du texte communautaire. C'est le cas en Côte d'Ivoire, avec la loi du 19 juin 2013 relative à la protection des données à caractère personnel.

L'intelligence artificielle, qui est de plus en plus prégnante, ouvrira à n'en point douter de nouveaux enjeux quant au traitement des données personnelles.

Enfin, ces données, traitées, conservées et contrôlées, par les autorités de contrôle de différents espaces, notamment l'UEMOA et l'Europe, qu'en est-il des rapports entre ces différentes autorités ? Coopèrent-elles, dans quel cadre ?

Tel pourrait être l'enjeu d'une véritable protection des données à caractère personnel, dans un monde virtuel, sans frontières.