NEWSLETTER E-SANTE

NUMÉRO 9 ● 2024

ÉQUIPE

Alexandre FIEVEE
Avocat associé

Alice ROBERT
Avocat counsel

SOMMAIRE

ACTUALITES

P. 2 • Demande de rétractation d'une ordonnance « 145 » contraire au RGPD

P. 3 • Certification HDS : un nouveau « nouveau projet de référentiel »

P. 4 • CJUE : on peut être responsable du traitement sans traiter de données personnelles

P. 6 • Informer de la fermeture d'une clinique, oui. Mais pas n'importe comment...

P. 7 • Etudes cliniques : l'existence d'un tableau de concordance empêche toute anonymisation ?

P. 9 • Droit d'accès : Peut-il être utilisé pour vérifier le bon déroulé du traitement... Médical ?

P. 10 • L'urgence médicale ne peut pas passer outre le RGPD

VU DANS LA PRESSE

P. 11 • Un organisme de contrôle médical peut-il traiter les données de santé de ses propres salariés ? *DSIH 29 janvier 2024*

DEMANDE DE RETRACTATION D'UNE ORDONNANCE « 145 » CONTRAIRE AU RGPD

ACTUALITES

La Cour d'appel de Nîmes a été saisie d'une demande de rétractation d'une ordonnance « 145 » (mesure d'instruction prévue par le Code de procédure civile, permettant de conserver ou d'établir, sur requête, des moyens de preuves), par laquelle une société a recueilli des éléments de preuves chez son concurrent, en faisant usage de données sensibles en guise de mots-clés.

Une ordonnance « 145 » basée sur des données de santé

Un prestataire de santé soupçonnait son concurrent direct d'avoir débauché ses salariés et détourné ses patients.

Sur requête de ce prestataire, le président du TC de Nîmes a rendu une ordonnance au visa de l'article 145 du Code de procédure civile, désignant un huissier afin de recueillir des éléments de preuve, chez le concurrent, permettant d'engager une action en indemnisation au fond.

Cette ordonnance prévoyait l'utilisation, au titre de « mots clés », des nom, prénom, NIR, lieu de domicile, diagnostic et traitement de 376 patients du prestataire de santé, dans le cadre de la recherche des éléments de preuve.

Une ordonnance contraire au RGPD

A l'issue de l'exécution de cette ordonnance, le concurrent a fait assigner le prestataire de santé devant le président du TC de Nîmes, afin d'obtenir sa rétractation. Le président du TC de Nîmes a considéré que les mesures d'instructions contenues dans cette ordonnance étaient proportionnées et justifiées par un motif légitime et a donc débouté le concurrent de sa demande en rétractation.

Pour le prestataire, le concurrent est irrecevable à agir sur le fondement du RGPD, seuls les patients pouvant l'invoquer. Par ailleurs, le traitement de donnée était justifié car indispensable à la constatation d'un droit en justice. Enfin, la prétendue violation de règles impératives n'entre pas dans le champ de compétence du juge de la rétractation.

La Cour d'appel de Nîmes, dans sa décision du 10 novembre 2023, relève qu'il y a bien eu des manquements au RGPD, à savoir le défaut d'information des patients quant à la transmission de leurs données à l'autorité judicaire et au concurrent, ainsi que le défaut de consentement des patients à l'utilisation de leurs données personnelles en vue d'une action en justice. L'ordonnance validée en l'absence d'atteinte excessive aux droits des personnes

Pour la Cour d'appel de Nîmes, la divulgation d'indications sur la santé des personnes concernées n'a pas porté une atteinte excessive aux droits de ces dernières, au regard du but poursuivi par le prestataire de santé de parvenir à la manifestation de la vérité.

Cette décision est motivée par les éléments suivants :

- le prestataire de santé dispose d'un motif légitime de recourir à une mesure d'instruction nécessaire à la protection de ses droits ;
- les investigations menées n'ont pas permis au prestataire de santé d'obtenir d'autres informations que celles dont il disposait déjà sur ses patients ;
- l'huissier est soumis au secret professionnel et le concurrent est un prestataire de santé soumis au secret médical.

L'ordonnance « 145 » n'a donc pas été rétractée.

Source : ici

CERTIFICATION HDS : UN NOUVEAU « NOUVEAU PROJET DE REFERENTIEL »

Le nouveau projet de référentiel HDS a fait l'objet de nouvelles modifications.

Pour rappel, conformément à l'article L.1111-8 du Code de la santé publique, l'hébergement externalisé de données de santé à caractère personnel requiert en particulier une certification.

La procédure de certification nécessite une conformité à des exigences figurant dans un référentiel de certification.

L'Agence numérique en santé (« l'ANS ») a proposé, en novembre 2022, un nouveau projet de référentiel consistant, en réalité, en une mise à jour du référentiel existant (voir notre précédent article sur le sujet).

A la suite d'une consultation publique achevée le 9 décembre 2022, ce nouveau projet de référentiel a fait l'objet de certains remaniements. Cette version modifiée a été validée par la CNIL dans le cadre d'un avis rendu le 13 juillet 2023.

Aussi, l'ANS a soumis, en décembre dernier, le projet d'arrêté approuvant ce nouveau « nouveau » projet de référentiel à la Commission européenne.

Si le contenu de cette dernière version n'a pas encore été dévoilé, les communications faites par l'ANS révèlent que les modifications portent notamment sur les points essentiels suivants :

- Les activités objet de la certification avec en particulier une clarification (attendue) de la définition de l'« activité d'administration et d'exploitation des systèmes de santé », à savoir l'épineuse activité d'hébergement dite « activité 5 »
- Une amélioration des garanties apportées par l'hébergeur vis-à-vis des prestataires faisant appel à ses services ;
- Une clarification des obligations contractuelles de l'hébergeur ;
- Une intégration de la dernière version de la norme ISO 27001 ;
- Un renforcement progressif de la souveraineté des données (avec notamment une exigence d'hébergement physique des données dans l'Espace Economique Européen) ;
- Des précisions sur l'articulation des exigences du référentiel avec les exigences de la certification SecNumCloud.

En termes de calendrier, l'arrêté approuvant cette nouvelle version devrait être publié au Journal Officiel à compter du 6 mars 2024 (après le statut quo de la Commission européenne).

Le délai de mise en conformité serait de 6 mois à compter de la publication de l'arrêté : c'est-à-dire que dès septembre 2024, les demandes de certifications, que ce soient des nouvelles demandes ou des demandes de renouvellement, devront alors être basées sur le nouveau référentiel.

Source : ici

CJUE : ON PEUT ETRE RESPONSABLE DU TRAITEMENT SANS TRAITER DE DONNEES PERSONNELLES

Par un arrêt du 5 décembre 2023, la Cour de justice de l'Union européenne (CJUE) a estimé que le Centre national de santé publique (CNSP) lituanien pouvait bien être qualifié de responsable du traitement, s'agissant des traitements de données personnelles réalisés au moyen d'une application mobile développée par un de ses prestataires, alors même que le CNSP ne traite lui-même aucune donnée personnelle.

Un traitement entièrement délégué

Dans le cadre de la pandémie provoquée par le virus de la COVID-19, le ministre de la Santé de Lituanie a ordonné au Centre national de santé publique (CNSP) de faire l'acquisition d'un système informatique permettant l'enregistrement et le suivi des données des personnes exposées à ce virus. Le CNSP a donc fait appel à un prestataire afin de développer une application mobile.

Par le biais de cette application, étaient notamment collectées les données suivantes des utilisateurs : le numéro d'identité, les coordonnées géographiques (latitude et longitude), le pays, la ville, le code postal, le nom de rue, le numéro de l'immeuble, le nom, le prénom, le code personnel et le numéro de téléphone. Alors que l'application était en phase d'essais sur des données réelles, le processus d'acquisition de l'application, par le CNSP, a avorté.

L'autorité de contrôle Lituanienne a néanmoins estimé que le CNSP est le responsable du traitement réalisé au moyen de l'application et l'a condamné à une amende administrative de 12.000 € pour divers manquements au RGPD.

Le CNSP, estimant ne pas être responsable du traitement, a formé un recours contre cette décision, ce qui a abouti à la saisine de la CJUE.

La qualification de responsable du traitement confirmée par la CJUE

La juridiction nationale compétente pour connaitre du recours du CNSP a posé, en substance, la question suivante à la CJUE :

Une entité prévoyant d'acquérir un outil de collecte de données, à savoir l'application mobile en cause, doit-elle être considérée comme responsable du traitement, s'agissant des données personnelles utilisées dans le cadre d'essais, alors qu'elle n'a aucun droit de propriété sur l'outil de collecte de données et ne procède pas elle-même au traitement de données ?

La CJUE a répondu : « *pour établir si une entité, telle que le CNSP, peut être considérée comme étant responsable du traitement au sens de l'article 4, point 7, du RGPD, il convient d'examiner si cette entité a effectivement influé, à des fins qui lui sont propres, sur la détermination des finalités et des moyens de ce traitement* ».

Dans la mesure où le CNSP (i) a commandé l'application en cause, (ii) a prévu que des données personnelles soient traitées aux fins de gestion de la pandémie de COVID-19 au moyen de ladite application et (iii) a joué un rôle actif dans la détermination des questions posées dans l'application, et de leur formulation, la CJUE a estimé que le CNSP a effectivement participé à la détermination des finalités et des moyens du traitement.

La CJUE considère comme indifférents : le fait que le CNSP n'ait pas lui-même traité de données personnelles, le fait qu'il n'y avait pas contrat entre le CNSP et le prestataire en charge du développement de l'application et le fait que le CNSP n'ait pas acquis l'application mobile en cause, ni autorisé la diffusion de l'application par la boutique en ligne.

Source : ici

INFORMER DE LA FERMETURE D'UNE CLINIQUE, OUI. MAIS PAS N'IMPORTE COMMENT…

L'autorité de contrôle italienne a rappelé que les panneaux d'information n'ont, en principe, pas à contenir de données personnelles, et encore moins de données sensibles (GPDP Italie 8 juin 2023)

Un médecin en charge d'un service spécialisé dans une clinique est tombé malade et n'a pas pu assurer les soins pendant une journée.

Afin d'informer les patients de la fermeture du service en question, le directeur de la clinique a demandé qu'un panneau d'information soit affiché à l'entrée de la clinique.

Ce panneau comportait la mention suivante : « *Les utilisateurs sont informés que le [date], les consultations de [spécialité] ne seront pas assurées pour des raisons de service (Maladie du docteur X)* ».

Le médecin, considérant qu'une telle information est contraire au RGPD, a déposé une plainte auprès de l'autorité de contrôle italienne.

Cette dernière a considéré que la clinique avait « diffusé » (c'est-à-dire porté à la connaissance de tiers) des données à caractère personnel et tout particulièrement des données sensibles en violation du RGPD, et notamment du principe de licéité (article 5§1 a. du RGPD), et du principe d'interdiction des traitements portant sur des catégories particulières de données à caractère personnel (article 9 du RGPD).

Compte tenu de ce qui précède, l'autorité de contrôle a infligé à la clinique une amende de 5.000 €.

Source : ici

ETUDES CLINIQUES : L'EXISTENCE D'UN TABLEAU DE CONCORDANCE EMPECHE TOUTE ANONYMISATION ?

L'autorité de contrôle italienne est venue préciser la notion d'anonymisation et a considéré que des données ne sont correctement anonymisées (i) qu'après avoir été agrégées et (ii) une fois le tableau de concordance entre le nom des patients et le code d'identification détruit (GPDP Italie, 18 juillet 2023).

L'hôpital universitaire de Careggi a sollicité de l'autorité de contrôle italienne l'autorisation de réaliser une étude clinique visant à « évaluer l'efficacité du médicament mobocertinib », médicament prescrit aux patients atteints de cancers du poumon. L'étude clinique visait une cinquantaine de patients.

Pour démontrer le respect de cette étude clinique au RGPD, l'hôpital a, entre autres, indiqué que : « *les noms des patients seront rendus anonymes par l'attribution à chaque patient d'un code d'identification alphanumérique* », et que le tableau de concordance entre le nom des patients et le code d'identification alphanumérique serait uniquement conservé par le coordinateur de l'étude, tandis que les chercheurs accédant à l'étude ne disposeront que du code d'identification.

Au cours de son enquête, l'autorité de contrôle a considéré que l'hôpital avait qualifié, à tort, les mesures précédemment décrites de « *mesures d'anonymisation* ».

Le rappel de l'autorité sur les critères de l'anonymisation

L'autorité a rappelé que « *les règles de protection des données ne s'appliquent pas aux données anonymes* », et que sont considérées comme anonymes « les informations qui ne se rapportent pas à une personne physique identifiée ou identifiable ou les données à caractère personnel qui ont été rendues suffisamment anonymes pour que la personne concernée ne soit plus identifiable ou ne puisse plus être identifiée ».

L'autorité a ajouté que le risque de réidentification de la personne concernée doit être soigneusement évalué en tenant compte de « *tous les moyens […] dont dispose raisonnablement le responsable du traitement ou un tiers aux fins d'identifier cette personne physique, directement ou indirectement* ».

Afin de vérifier *« la probabilité raisonnable de l'utilisation des moyens pour identifier la personne physique* », il convient de prendre en considération « *tous les facteurs objectifs, y compris les coûts et le temps nécessaires à l'identification, en tenant compte à la fois des technologies disponibles au moment du traitement et de l'évolution technologique* ».

L'application des critères en l'espèce

Compte tenu de ce rappel, l'autorité de contrôle a considéré que, dans le cas d'espèce, « *on ne peut considérer que l'anonymisation est obtenue par la simple suppression des données à caractère personnel de la personne concernée ou leur remplacement par un code*.

En effet, les données anonymisées ne le sont que si elles ne permettent en aucune manière d'identifier directement ou indirectement une personne, compte tenu de tous les moyens (ressources économiques, informationnelles, technologiques, compétences, temps) mis à disposition du responsable du traitement ou des tiers pour identifier une personne concernée ».

Toujours selon l'autorité, « *un processus d'anonymisation ne peut être qualifié comme tel s'il n'empêche pas une personne, qui utiliserait des moyens* « raisonnablement disponibles *»,* (i*) d'isoler une personne dans un groupe (individualisation), (ii) d'établir un lien entre une donnée anonymisée et des données relatives à une personne figurant dans un ensemble de données (corrélation) et (iii) de déduire de nouvelles informations relatives à une personne à partir de données* »

L'anonymisation par la destruction du tableau de concordance et l'agrégation des données

L'hôpital a également indiqué à l'autorité de contrôle italienne qu'à la fin de l'étude (à l'issue d'une durée de conservation de 7 ans), il détruirait le tableau de concordance permettant d'établir la corrélation entre les données et les patients et agrégerait les données.

L'autorité de contrôle a considéré que ces mesures (agrégation et destruction du tableau de concordance) pouvaient être considérées comme des mesures d'anonymisation acceptables mais que, compte tenu du nombre très limité de patients, le risque de réidentification de chacun d'eux était accru (ce que l'autorité appelle risque de « reconstruction »).

En conséquence, l'autorité de contrôle italienne a rendu un « avis favorable » à la réalisation de cette étude, à condition, notamment, que l'hôpital réduise le risque de reconstruction en :

- veillant à ce que l'agrégation des données (leur regroupement pour former des ensembles de données plus larges) soit effectif, c'est-à-dire qu'il y ait sensiblement moins de « variables » après l'agrégation, qu'avant ;

- effectuant des contrôles périodiques des mesures d'anonymisation prenant en compte l'évolution technologique et s'engageant à « supprimer toute singularité ».

Source : ici

DROIT D'ACCES : PEUT-IL ETRE UTILISE POUR VERIFIER LE BON DEROULE DU TRAITEMENT… MEDICAL ?

Dans un arrêt du 26 octobre 2023, la Cour de justice de l'Union européenne (CJUE) a répondu à la question suivante : le droit d'accès permet-il à la personne concernée d'obtenir gratuitement une copie de son dossier médical, y compris lorsque cette demande n'est pas motivée par un des objectifs visés par le RGPD, et lorsqu'une disposition de droit national prévoit le remboursement des coûts engendrés par cette communication ?

Un praticien refuse de fournir gratuitement une copie de son dossier médical à son patient

Un patient allemand a été soigné par un médecin-dentiste. Par la suite, le patient, suspectant des erreurs commises lors du traitement qui lui a été prodigué, a demandé au praticien de lui fournir, à titre gratuit, une copie de son dossier médical.

Le praticien a indiqué au patient qu'il ne répondrait favorablement à sa demande qu'à condition qu'il prenne en charge les frais liés à la fourniture de la copie du dossier médical, conformément au droit national allemand, qui prévoit que le praticien peut demander au patient de lui rembourser les coûts engendrés par la communication de la copie du dossier médical.

Pour le praticien, l'objectif poursuivi par le patient n'était pas, comme le prévoit le considérant 69 du RGPD, la prise de connaissance du traitement de ses données personnelles pour en vérifier la licéité, mais un but étranger au RGPD, à savoir la vérification du bon déroulé du traitement médical.

Une personne concernée peut-elle exercer son droit d'accès pour des buts étrangers à la vérification de la licéité du traitement de données personnelles ?

La Cour fédérale de justice allemande, saisie du litige, a posé, en substance, la question préjudicielle suivante à la CJUE :

Le responsable du traitement est-il tenu faire droit à une demande de droit d'accès exercée dans un but étranger à ceux cités par le RGPD, à savoir prendre connaissance du traitement de ses données à caractère personnel et en vérifier la licéité ?

La CJUE a répondu que l'obligation de fournir une copie des données personnelles à la personne concernée s'impose au responsable du traitement, « *même lorsque cette demande est motivée dans un but étranger* » à ceux visés par le considérant 63 du RGPD.

Le RGPD permet-il au patient d'obtenir gratuitement une copie de son dossier médical, malgré des dispositions de droit national prévoyant le paiement de frais ?

La Cour fédérale de justice allemande a également interrogé la CJUE quant au point de savoir si le patient était fondé à obtenir gratuitement une copie de son dossier médical, au titre du droit d'accès, nonobstant les dispositions de droit allemand prévoyant le paiement de frais.

La CJUE a reconnu que l'article 23 du RGPD permet aux Etats membres d'adopter, dans certaines circonstances, des mesures législatives limitant la portée des droits des personnes concernées. Toutefois, pour la CJUE, l'article 23 du RGPD exclut l'adoption de législations nationales qui, telle la législation allemande d'espèce, mettraient à la charge de la personne concernée les frais d'une première copie de ses données à caractère personnel, en vue de protéger les intérêts économiques du responsable du traitement.

Source : ici

L'URGENCE MEDICALE NE PEUT PAS PASSER OUTRE LE RGPD

L'autorité de contrôle italienne a sanctionné un pneumologue pour avoir, sous prétexte de l'urgence, transmis à un tiers des données de santé.

Un patient, après avoir réalisé un examen pneumologique, a constaté que le courrier électronique comportant ses résultats d'examen avait été transmis à un tiers sans son consentement. Le patient a donc déposé une plainte devant l'autorité de contrôle italienne.

Le médecin justifiait une telle transmission en indiquant que compte tenu « du degré de gravité de la maladie » et de « l'urgence à prévoir, dans les plus brefs délais, l'utilisation d'un respirateur », il n'avait pas eu d'autre choix que de « transmettre les résultats de l'examen médical à la seule société en Toscane qui pouvait fournir rapidement […] l'appareil au patient ».

Le médecin considérait :

- que le traitement était exempté de consentement, conformément à l'article 9(2)h du RGPD, car « essentiel aux soins du patient » et *« nécessaire aux fins de [..] diagnostics médicaux* » ;

- qu'en tout état de cause, le patient (i) avait donné son consentement puisque le médecin l'avait alerté sur la gravité de sa maladie, (ii) était informé de la nécessité urgente d'acheter un respirateur en passant par l'intermédiaire d'une société tierce et (iii) avait confirmé qu'il « *achèterait dès que possible la machine* ».

Au cours de son enquête, l'autorité de contrôle a :

- considéré que la transmission des données de santé du patient à un tiers, « bien que prétendument destiné à faciliter l'acquisition de la machine », « *ne peut être considérée comme essentielle pour le traitement, étant donné que le patient était en mesure d'acquérir la machine de manière autonome* » ;

- rejeté l'argument selon lequel le patient avait consenti à un tel traitement, le consentement n'étant pas suffisamment « explicite » ;

- estimé qu'en tout état de cause, conformément au principe de minimisation, le tiers « *avait uniquement besoin d'acquérir des éléments relatifs à la pathologie du patient, et non l'ensemble de ses résultats d'examen* ».

Compte tenu de ce qui précède, l'autorité de contrôle a infligé au pneumologue une amende de 5000 € pour avoir violé le principe de licéité, posé à l'article 5(1) a du RGPD et le principe d'interdiction de traitement des données sensibles, posé à l'article 9 du RGPD.

Source : ici

UN ORGANISME DE CONTROLE MEDICAL PEUT-IL TRAITER LES DONNEES DE SANTE DE SES PROPRES SALARIES ?

VU DANS LA PRESSE

« DSIH » 29 JANVIER 2024

Lorsqu'un organisme de contrôle médical traite des données de santé d'un de ses salariés afin d'évaluer les capacités de travail dudit salarié, la licéité d'un tel traitement au regard du RGPD interroge. Comment effectivement gérer cette double « casquette » de l'organisme, à la fois responsable de traitement agissant dans le cadre de sa mission de contrôle médical, et également employeur de la personne concernée par le traitement ? Un tel traitement peut-il être autorisé ? N'y-a-t-il pas conflit d'intérêts ? Le consentement du salarié concerné pour procéder à un tel traitement est-il requis ? Comment assurer le respect du secret médical au sein de l'organisme, en particulier vis-à-vis de l'équipe travaillant avec le salarié concerné ?

La Cour de Justice de l'Union européenne a récemment jugé (lien vers la décision) que ce type de traitement est parfaitement licite au regard du RGPD, sous réserve de respecter, effectivement, les conditions et garanties prévues par ce texte.

En l'occurrence, l'affaire concernait un service médical ayant notamment pour mission légale d'évaluer l'incapacité de personnes assurées auprès de certaines caisses d'assurance maladie. Cette mission, réalisée sous forme d'expertise médicale, permet aux caisses d'assurance maladie d'apprécier leur obligation ou non de verser des indemnités d'incapacité de travail.

A la demande d'une des caisses concernées, le service médical a réalisé une expertise relative à l'incapacité de travail d'un assuré de ladite caisse. La particularité de la situation résidait dans le fait que cet assuré était, par ailleurs, un employé du service médical.

Pour mémoire, le RGPD prévoit des exceptions à l'interdiction de principe du traitement de données de santé (article 9§1 du RGPD), parmi lesquelles figure le « *traitement nécessaire notamment à l'appréciation de la capacité de travail du travailleur* » (article 9§2 h)).

Si un tel traitement est possible, il doit, néanmoins, être exercé sous certaines réserves (même article), en particulier le respect d'un devoir de confidentialité dans les conditions indiquées à l'article 9§3 du RGPD (« *les données sont traitées par un professionnel de la santé soumis à une obligation de secret professionnel conformément au droit de l'Union, au droit d'un État membre ou aux règles arrêtées par les organismes nationaux compétents, ou sous sa responsabilité, ou par une autre personne également soumise à une obligation de secret conformément au droit de l'Union ou au droit d'un État membre ou aux règles arrêtées par les organismes nationaux compétents.* »).

Les juges européens ont considéré que cette exception (le traitement de données de santé nécessaire à l'évaluation de capacité d'un travailleur) n'a pas à être limitée « aux hypothèses où un " tiers neutre " traite des données concernant la santé aux fins de l'appréciation de la capacité de travail d'un travailleur ». La « casquette » d'employeur du responsable de traitement concerné est donc sans incidence sur la possibilité pour celui-ci, en tant qu'organisme de contrôle médical, de réaliser un tel traitement.

La CJUE a également précisé qu'il n'est pas nécessaire, par principe, que le responsable du traitement garantisse qu'aucun collègue de la personne concernée ne puisse accéder aux données se rapportant à l'état de santé de celle-ci.

Pour la Cour, il suffit que les traitements soient réservés à des personnes soumises à une obligation de secret, conformément aux conditions prévues par le RGPD (article 9§3 du RGPD).

Par ailleurs, les juges européens ont précisé qu'un traitement autorisé, par exception en vertu du RGPD, n'est pas pour autant dispensé de base légale et ce, comme tout traitement de données à caractère personnel. Un tel traitement doit donc également respecter l'une des conditions de licéité prévues à l'article 6§1 du RGPD (consentement, exécution d'un contrat, obligation légale, sauvegarde des intérêts vitaux, mission d'intérêt public, intérêt légitime).

Cette solution nous donne ainsi des éclairages pour apprécier la licéité de certains traitements de données de santé réalisés pour les besoins d'une mission légale/de service public, d'une part, et l'organisation de la protection du secret médical dans un tel cadre, d'autre part.

Source : ici