

## Bulletin d'information n° 57 (mars 2020)

Le Préposé cantonal à la protection des données et à la transparence (PPDT) vous adresse son bulletin d'information destiné aux personnes intéressées des institutions publiques cantonales et communales du canton de Genève.

Diffusé quatre fois par an, ce bulletin d'information renseigne sur les actualités relatives aux deux domaines d'action du PPDT, soit la transparence, d'une part, et la protection des données personnelles, d'autre part.

### Protection de la personnalité/Vidéosurveillance

#### **Arrêt de la Cour européenne des droits de l'homme du 17 octobre 2019 (Requêtes n<sup>os</sup> 1874/13 et 8567/13) – LÓPEZ RIBALDA ET AUTRES c. ESPAGNE**

Dans cette affaire, les requérantes avaient fait l'objet d'une vidéosurveillance, mise en place par leur employeur sur leur lieu de travail pendant une durée de dix jours, et dirigée vers les caisses du supermarché et leurs alentours.

En la matière, les juges alsaciens avaient préalablement estimé que la vidéosurveillance effectuée par l'employeur à l'insu d'une salariée, pendant environ cinquante heures sur une période de deux semaines et l'utilisation de l'enregistrement obtenu dans la procédure devant les juridictions du travail pour justifier son licenciement, constituaient une atteinte au droit de l'intéressée au respect de sa vie privée (affaire Köpke c. Allemagne, du 5 octobre 2010). La vidéosurveillance non dissimulée de professeurs d'Université pendant qu'ils dispensaient leurs cours, dont les enregistrements étaient conservés pendant un mois et consultables par le doyen de la faculté, a également été jugée attentatoire à la vie privée des intéressés (affaire Antović et Mirković c. Monténégro, du 28 novembre 2017).

Pour s'assurer de la proportionnalité de mesures de vidéosurveillance sur le lieu de travail, les juridictions nationales devraient tenir compte des facteurs suivants lorsqu'elles procèdent à la mise en balance des différents intérêts en jeu (rappel de l'arrêt Bărbulescu): i) L'employé a-t-il été informé de la possibilité que l'employeur prenne des mesures de vidéosurveillance ainsi que de la mise en place de telles mesures ? Si, en pratique, cette information peut être concrètement communiquée au personnel de diverses manières, en fonction des spécificités factuelles de chaque cas, l'avertissement doit en principe être clair quant à la nature de la surveillance et préalable à sa mise en place. ii) Quels ont été l'ampleur de la surveillance opérée par l'employeur et le degré d'intrusion dans la vie privée de l'employé ? À cet égard, il convient de prendre en compte notamment le caractère plus ou moins privé du lieu dans lequel intervient la surveillance, les limites spatiales et temporelles de celle-ci, ainsi que le nombre de personnes ayant accès à ses résultats. iii) L'employeur a-t-il justifié par des motifs légitimes le recours à la surveillance et l'ampleur de celle-ci ? Sur ce point, plus la surveillance est intrusive, plus les justifications requises doivent être sérieuses. iv) Était-il possible de mettre en place un système de surveillance reposant sur des moyens et des mesures moins intrusifs ? À cet égard, il convient d'apprécier en fonction des circonstances particulières de chaque espèce si le but légitime poursuivi par l'employeur pouvait être atteint en portant une atteinte moindre à la vie privée du salarié. v) Quelles ont été les conséquences de la surveillance pour l'employé qui en a fait l'objet ? Il convient notamment de vérifier de quelle manière l'employeur a utilisé les résultats de la mesure de surveillance et s'ils ont servi à atteindre le but déclaré de la mesure. vi) L'employé s'est-il vu offrir des garanties adéquates, notamment lorsque les mesures de surveillance de l'employeur avaient un caractère intrusif ? Ces garanties peuvent être mises en œuvre, parmi d'autres moyens, par l'information fournie aux employés concernés ou aux représentants du personnel sur la mise en place et sur l'ampleur de la vidéosurveillance, par la déclaration de l'adoption d'une telle mesure à un organisme indépendant ou par la possibilité d'introduire une réclamation (§ 116).

Présentement, la Cour a conclu que les autorités nationales n'avaient pas manqué à leurs obligations positives au titre de l'art. 8 CEDH de manière à outrepasser leur marge d'appréciation. Partant, il n'y a pas eu violation de cette disposition.

<https://hudoc.echr.coe.int/fre#%7B%22itemid%22%3A%22001-197095%22%7D>

~~~~~  
**Les actes émis par l'autorité**  
~~~~~

**Projet de règlement d'application de la loi sur la laïcité de l'Etat – Avis du 2 décembre 2019 à la Direction des affaires juridiques du Département de la sécurité, de l'emploi et de la santé (DSES)**

Par courriel du 19 novembre 2019, la Direction juridique du DSES a soumis pour avis au Préposé cantonal un projet de règlement d'application de la loi sur la laïcité de l'Etat (LLE; RSGe A 2 75). Le Préposé cantonal s'était déjà prononcé sur un projet de règlement provisoire d'application de cette même loi, ayant trait à la mise en application des art. 4 et 5 LLE concernant les relations entre autorités et organisations religieuses. Ce préavis a complété la veille du 12 novembre 2019, s'agissant notamment de la mise en application de l'art. 8 LLE. Les Préposés ont constaté avec satisfaction que les remarques émises dans leur préavis du 12 novembre 2019 avaient été prises en considération. S'agissant des nouvelles dispositions examinées, ils ont relevé que le projet de règlement prévoit la collecte de données sensibles et qu'il aurait été préférable que cette collecte soit prévue expressément par une base légale formelle. Par ailleurs, ils ont considéré qu'un cadre plus précis devait être défini s'agissant des renseignements pris auprès de tiers concernant les personnes proposées pour effectuer l'accompagnement afin de respecter les principes de proportionnalité et reconnaissabilité de la collecte. Finalement, les Préposés ont souligné qu'il est délicat de déduire d'un engagement à collaborer à la prévention des radicalisations une obligation de signaler, car une telle obligation, si elle doit revêtir un caractère contraignant, devrait figurer dans une base légale formelle.

<https://www.ge.ch/ppdt/doc/documentation/Avis-02-decembre-2019.pdf>

**Projet de règlement d'exécution de la loi d'application de la législation fédérale sur les denrées alimentaires et les objets usuels – Avis du 2 janvier 2020 au Service de la consommation et des affaires vétérinaires (SCAV)**

Par mail du 9 décembre 2019, le SCAV, rattaché au Département de la sécurité, de l'emploi et de la santé (DSES), a sollicité un avis du Préposé cantonal à la protection des données et à la transparence au sujet du projet de règlement d'exécution de la loi d'application de la législation fédérale sur les denrées alimentaires et les objets usuels (RaLDAI; RSGe K 5 02.01). En date du 27 avril 2018, les Préposés avaient rendu un avis concernant le projet de loi d'application de la législation fédérale sur les denrées alimentaires et les objets usuels (PL12400), lequel a été adopté par le Grand Conseil le 13 septembre 2019. Les art. 6 (devoir d'information) et 17 (communication) du projet de RaLDAI concernent la protection des données. Pour les Préposés, s'agissant de la première disposition, les informations contenues dans la liste (nom et adresse en Suisse de la personne responsable; raison sociale de l'entreprise; lieu précis où s'exerce l'activité; les dates d'activité; la nature de l'activité) sont toutes nécessaires au service, dès lors qu'elles doivent lui permettre d'identifier précisément les commerces itinérants et professionnels et, de ce fait, d'effectuer des contrôles et inspections de manière plus efficiente. Concernant l'art. 17, selon lequel les autorités pénales communiquent au chimiste cantonal ou au vétérinaire cantonal toutes les décisions pénales faisant suite à leurs dénonciations, les Préposés ont considéré que les éléments pouvant être transmis s'inscrivaient dans les missions respectives des deux autorités et que la finalité (protection du consommateur) apparaissait de manière claire.

<https://www.ge.ch/ppdt/doc/documentation/Avis-2-janvier-2020-Projet-reglement-RaLDAI.pdf>

**Projet de loi d'application de la loi fédérale sur les jeux – Avis du 3 janvier 2020 au Département de la cohésion sociale (DCS)**

En date du 17 décembre 2019, le Département de la cohésion sociale (DCS) a demandé au Préposé cantonal son avis concernant le projet de loi d'application de la loi fédérale sur les jeux d'argent, plus particulièrement l'art. 2, qui traite de la collaboration entre les autorités participant à l'application de la loi, et l'art. 22, qui habilite les autorités compétentes à traiter des données personnelles, y compris des données personnelles sensibles. Les Préposés ont estimé conforme à l'art. 39 al. 1 à 3 LIPAD la première disposition, qui prévoit que les renseignements et documents sont mutuellement transmis en tant que cela est nécessaire à l'accomplissement des tâches des entités concernées. S'agissant de la seconde norme, ils ont invité le DCS à préciser le type de données sensibles qui pourraient être traitées (condamnations pénales ou administratives, par exemple), pour assurer de la sorte le respect du principe de la proportionnalité. En

outre, préciser la durée de conservation des données est judicieux en termes de sécurité du droit. Pour les Préposés, une durée de 10 ans après la fin de l'événement auquel la récolte de données est liée ne semblait pas excessive et correspond au délai de conservation prévu par le droit fédéral, s'agissant des données collectées par la commission fédérale des maisons de jeu (CFMJ).

<https://www.ge.ch/ppdt/doc/documentation/Avis-3-janvier-2020-Projet-loi-jeux-argent.pdf>

### **Projet de loi sur les taxis et les voitures de transport avec chauffeurs – Avis du 8 janvier 2020 au Département de la sécurité, de l'emploi et de la santé (DSES)**

Le 19 décembre 2019, le DSES a requis un avis du Préposé cantonal au sujet du projet de loi sur les taxis et les voitures de transport avec chauffeurs, notamment les dispositions ayant trait à l'entraide administrative (art. 4) et au traitement des données personnelles (art. 39). Concernant la première norme, les Préposés ont salué la création d'une base légale formelle à la collaboration entre les autorités concernées, laquelle apparaît conforme aux conditions posées par l'art. 39 al. 1 à 3 LIPAD. Quant à l'art. 39 du projet, les Préposés ont estimé que, s'il s'agissait de créer une base légale formelle pour le traitement de données personnelles sensibles, il convenait toutefois de constater que le texte parlait uniquement de données personnelles (art. 4 litt. a LIPAD). Par ailleurs, le type de données personnelles sensibles qui pourraient être traitées devrait être précisé, afin de garantir, au niveau légal déjà, la bonne application du principe de la proportionnalité.

<https://www.ge.ch/ppdt/doc/documentation/Avis-8-janvier-2020-Projet-loi-taxis-voitures-transport-chauffeurs.pdf>

### **Recommandation du 30 janvier 2020 relative à une demande d'accès auprès de la Cour des comptes à un procès-verbal d'audition, ainsi qu'à tous les échanges avec une société auditionnée**

Par la voix de leur avocat, certains membres d'une entité ayant fait l'objet d'un audit de la Cour des comptes ont sollicité auprès de cette dernière l'accès à un procès-verbal d'audition, ainsi qu'à tous les échanges avec une société auditionnée. La demande d'accès aux documents a également été motivée sous l'angle de l'art. 47 LIPAD, afin de faire valoir la cessation d'un traitement illicite de données. La Cour des comptes n'a pas donné une suite positive à la requête, soulignant que seul le rapport qu'elle émet a vocation à être rendu public. Elle a également questionné sa soumission à la LIPAD et souligné ne pouvoir rendre de décision suite à une éventuelle recommandation. Même si de nombreux éléments laissent penser que le fait que la Cour des comptes ne soit pas mentionnée dans le champ d'application de la LIPAD relève d'une lacune du législateur plus que d'une réelle volonté, aucune recommandation n'a pu être formulée, faute d'accès aux documents.

<https://www.ge.ch/ppdt/doc/documentation/Recommandation-30-janvier-2020.pdf>

~~~~~

### **De quelques questions traitées ces derniers mois**

~~~~~

### **Un particulier souhaite que des informations le concernant (adresse, email, numéro de téléphone) publiées sur un site web sans son accord soient supprimées. Que peut-il faire ?**

Le Préposé cantonal est compétent uniquement pour les données personnelles traitées par des institutions publiques genevoises (art. 3 al. 4 LIPAD). S'agissant du secteur privé en Suisse, c'est le Préposé fédéral qui est l'autorité à laquelle il convient de s'adresser. La CNIL (organisme tenu de veiller à la protection des données personnelles en France) a rédigé un document qui détaille comment trouver le responsable d'un site d'origine (sur le site <https://www.whois.net/> par exemple) et les démarches à entreprendre pour l'effacement des données (<https://www.cnil.fr/fr/effacer-des-informations-me-concernant-sur-un-moteur-de-recherche>).

### **Une société coopérative genevoise traitant de données de collaborateurs est-elle soumise à la LIPAD ?**

Les sociétés coopératives du droit des obligations sont soumises à la loi fédérale sur la protection des données (LPD, RS 235.1). S'agissant de l'application extraterritoriale du RGPD, le site du Préposé fédéral

donne les informations suivantes: <https://www.edoeb.admin.ch/edoeb/fr/home/actualites/rgpd-last-minute.html#1428943096>.

### **Quid de la vidéosurveillance d'une école publique ?**

L'art. 16 al. 7 RIPAD prévoit qu'une institution publique exploitant un système de vidéosurveillance ne peut filmer un établissement scolaire ou ses abords immédiats durant les heures des activités scolaires et parascolaires, sauf autorisation expresse contraire du département de l'instruction publique, de la formation et de la jeunesse.

### **Les agents municipaux qui verbalisent un automobiliste sont-ils tenus de mentionner leur nom ?**

Oui. Depuis le 1<sup>er</sup> janvier 2020, l'art. 9 al. 1 litt. g de la loi sur les amendes d'ordre du 18 mars 2016 (LAO; RS 314.1) exige que la quittance de l'amende d'ordre mentionne le nom et le prénom de la personne ayant établi la quittance.

### **L'exploitant d'un hôtel doit-il garder une trace du séjour de ses clients ?**

Selon l'art. 32 de la loi sur la restauration, le débit de boissons, l'hébergement et le divertissement du 19 mars 2015 (LRDBHD; RSGe I 2 22), lors de chaque prise de chambre, l'exploitant et son personnel doivent enregistrer électroniquement les informations concernant l'identité de leurs hôtes. Alternativement, et après accord des services de police, il peut être renoncé à l'enregistrement électronique. Dans ce cas, l'exploitant et son personnel sont tenus de faire remplir par leurs hôtes un bulletin d'arrivée officiel (al. 1). Dans tous les cas, l'exploitant est tenu de vérifier l'exactitude des données fournies par les hôtes, sur la base de pièces d'identité à présenter par ces derniers (al. 2). L'exploitant qui effectue l'enregistrement électronique de l'identité des hôtes doit communiquer quotidiennement aux services de police ses fichiers d'arrivée de clients. L'exploitant utilisant les bulletins d'arrivée doit les remettre aux services de police, conformément aux directives de ces derniers (al. 3). L'exploitant qui effectue l'enregistrement électronique de l'identité des hôtes doit conserver les données de l'année en cours et ce jusqu'à la fin du mois de janvier suivant. Il doit les transmettre aux services de police à leur demande. L'exploitant utilisant les bulletins d'arrivée doit les transcrire dans un livre de police, qui sera tenu en tout temps à la disposition des services de police (al. 4). L'exploitant est tenu de respecter les conditions relatives à la capacité d'hébergement de son établissement et d'informer le département de toute augmentation ou diminution de cette capacité (al. 5).

~~~~~

## **Jurisprudence**

~~~~~

### **Arrêt du Tribunal fédéral du 15 novembre 2019 (1B\_164/2019) – Portée du principe de territorialité pour l'exploitation d'enregistrements issus de mesures techniques de surveillance secrètes autorisées en Suisse**

Dans ce jugement, le Tribunal fédéral précise les conditions dans lesquelles des enregistrements effectués à l'étranger, dans le cadre de mesures techniques de surveillance secrètes valablement autorisées en Suisse, peuvent être exploités au cours d'une procédure pénale. L'autorisation délivrée par une autorité suisse n'englobe que les enregistrements effectués sur le territoire suisse. Eu égard au principe de territorialité, un État ne peut effectuer des mesures d'instruction et de poursuite pénale sur le territoire d'un autre État sans le consentement de ce dernier. Une mesure technique de surveillance sur le territoire d'un autre État doit donc, dans la règle, être mise en œuvre en vertu du droit international (traité, accord bilatéral, droit international coutumier) ou, à défaut, en vertu du consentement préalable de l'État concerné dans le respect des règles régissant l'entraide internationale en matière pénale. A défaut d'avoir obtenu le consentement des autorités des pays étrangers concernés, les enregistrements effectués à l'étranger sont illicites et inexploitable.

### **Arrêt de la Chambre administrative de la Cour de justice du 17 décembre 2019 (ATA/1809/2019) – Demande d'accès à des notes**

A., collaborateur scientifique de la Ville de Genève, a recouru contre la décision lui octroyant la qualité de cadre intermédiaire auprès du Conseil administratif, concluant à ce qu'il soit confirmé qu'il n'avait pas cette qualité, vu l'absence de charge d'encadrement et d'arrêté de nomination indiquant qu'il serait cadre intermédiaire. Le Conseil administratif ayant rejeté ce recours, A. a porté l'affaire devant la Chambre administrative de la Cour de justice. La Ville a conclu au rejet de ce recours. Dans sa réplique, A. a sollicité des notes auxquelles se réfèrent les extraits de séances du Conseil administratif contenant ses positions relatives aux cadres intermédiaires. Dans leur arrêt, les juges ont constaté que la décision querellée du Conseil administratif se référait à des notes de la Direction des ressources humaines, de la Conseillère administrative en charge du Département des finances et du logement, et du directeur général. Pour eux, ces notes étaient indubitablement échangées entre les membres d'une autorité collégiale ou entre ces derniers et leurs collaborateurs, et étaient donc exclues du droit d'accès, conformément à l'art. 26 al. 3 LIPAD.

### **Arrêt du Tribunal administratif fédéral du 19 décembre 2019 (A-7131/2018) – Demande de suppression et de modification de données personnelles**

Dans cette affaire, un homme avait requis la suppression et la modification de données personnelles le concernant à l'Office fédéral de la police (fedpol). Initialement, il avait déposé une demande de permis de séjour, mais l'avait ensuite retirée à la suite d'un rapport négatif de fedpol, transmis au Secrétariat d'Etat aux migrations (SEM), dont il n'avait reçu qu'un résumé. La police fédérale considérait la présence de cet homme comme « une menace pour la sécurité publique et un risque pour la réputation de la Suisse ». Le requérant a fait valoir devant le Tribunal administratif fédéral que les informations transmises par fedpol au SEM ne reposaient que sur des soupçons et que leur transmission était donc illégale; la police fédérale aurait dû établir de manière transparente sur quels soupçons reposaient les reproches à son encontre. Le Tribunal administratif fédéral a rejeté le recours. Il confirme la position de fedpol, selon laquelle l'Office fédéral, en tant qu'autorité de poursuite pénale, peut traiter des données personnelles sur la base d'informations suspectes. Les juges ont estimé que ce type de données n'avait pas de valeur probante au sens du code de procédure pénale. Elles sont toutefois pertinentes dans le cadre d'enquêtes préliminaires et d'autres exigences légales comme la garantie de la sécurité intérieure. Et même si la procédure pénale contre le recourant avait été interrompue, cela ne signifiait pas que les suspicions à son encontre ne pouvaient pas subsister.

~~~~~  
**Plan genevois, intercantonal, fédéral et international**  
~~~~~

### **Financement des partis politiques**

En date du 16 décembre 2019, le Conseil des Etats a adopté, par 29 voix contre 13, un contre-projet indirect à l'initiative sur la transparence. Pour rappel, l'initiative "Pour plus de transparence dans le financement de la vie politique" veut contraindre les partis à communiquer chaque année leur bilan et leur compte de résultats, ainsi que l'origine de tous les dons d'une valeur supérieure à 10'000 francs. Les particuliers et les comités, qui dépensent un montant supérieur à 100'000 francs pour une campagne, devraient également communiquer leur budget global et déclarer les dons importants qu'ils ont reçus. Les sénateurs ont estimé que le texte allait trop loin. Par 32 voix contre 12, ils ont donc recommandé de le rejeter. Estimant néanmoins qu'il y avait lieu d'agir, ils ont adopté à la place un projet beaucoup moins strict, fixant la barre pour les dons à 25'000 francs par personne et par an. Et le seuil pour les particuliers, les entreprises et les comités à l'origine d'une campagne d'élection ou de votation, à 250'000 francs.

### **Dossier électronique du patient**

Le dossier électronique du patient (DEP), prévu initialement pour le printemps 2020, est retardé. Le problème réside notamment dans la certification des communautés de référence qui doivent mettre en place le dossier électronique. Les certifications permettent de garantir la protection des données des patients. En Suisse romande, ce sont les communautés CARA (FR, GE, JU, VD, VS) et ma santé connectée (NE) qui offriront les e-dossiers. La communauté Abilis SA couvre tout le pays. Le comité de programme de la Confédération et des cantons attend que chaque habitant de Suisse puisse ouvrir un e-dossier d'ici à l'automne. Il vérifie si les communautés de référence peuvent mettre à profit ce délai jusqu'à la certification définitive pour procéder à des tests.



## Conférences, formations et séminaires

- Jeudi 19 mars 2020 à 9h00 au centre de l'Espérance (8 rue de la Chapelle) – "*Les rendez-vous de la transparence*". Présentations de Mme Isabelle Ducret (Journaliste à la RTS), M. Alexandre Flückiger (Professeur à l'Université de Genève) et Mme Dominique Hänni (Greffière à la 1<sup>ère</sup> Cour de droit public du Tribunal fédéral) – Inscriptions: [ppdt@etat.ge.ch](mailto:ppdt@etat.ge.ch)
- Vendredi 20 mars 2020 à 8h00 à l'Université de Lausanne – Demi-journée de la protection des données: "Le droit d'accès" – Inscriptions: <https://www.unil.ch/cedidac/home/menuinst/manifestations/inscription.html>

## Publications

- BAERISWYL Bruno, Datennutzung und Datensouveränität, digma 2019, pp. 156 s.
- BLONSKI Dominika, Aus den Datenschutzbehörden, digma 2019, pp. 224 ss.
- BYDZOVSKY Pierre, Gestion des accès internes aux dossiers des clients et protection des données, Revue de l'avocat 2019, pp. 473 ss.
- FRÜH Alfred, Datenzuordnung und Datenzugang, digma 2019, pp. 172 ss.
- GRIESINGER Marcel, Der datenschutzrechtliche Auskunftsanspruch nach Art. 15 DSGVO, jusletter du 20 janvier 2020.
- GUISAN Alexandre/HIRSCH Célian, La surveillance secrète de l'employé, RSJ 115/2019, pp. 707 ss.
- JEANNERET Yvan, La preuve en droit pénal de la circulation routière: questions choisies et nouvelles technologies, PJA 6/2019, pp. 51 ss. |
- KARLEN Sascha, Data Management im Spital des 21. Jahrhunderts: Warum elektronische Gesundheitsdaten so schwer zugänglich sind und was dagegen getan wird, jusletter du 27 janvier 2020.
- LAUX Christian, Das Recht auf Datenportabilität, digma 2019, pp. 166 ss.
- MATHYS Roland, Datenschutz aus Sicht verschiedener Akteure beim Internet der Dinge, jusletter du 2 décembre 2019.
- NIKKEL Bruce, Herausforderungen der Datenlöschung, digma 2019, pp. 200–203;
- SCHMIDT Kirsten Johanna, Datenmärkte ohne «Dateneigentum», digma 2019, pp. 178 ss.
- SPRECHER Franziska, Sozialpflichtigkeit von Gesundheitsdaten, digma 2019, pp. 184 ss.
- STENGEL Cornelia/STÄUBLE Luca, Vom Persönlichkeitsprofil zum Profiling mit hohem Risiko, jusletter du 20 janvier 2020.
- SZUCS Thomas D./BRÄM Corina, Gesundheitsforschung mit Versicherungsdaten: Pflicht oder Kür?, jusletter du 27 janvier 2020.
- THOUVENIN Florent, Datenschutz auf der Intensivstation, digma 2019, pp. 206 ss.
- VOLKINGER Kerstin Noëlle, Gesundheitsdaten im digitalen Zeitalter, jusletter du 27 janvier 2020.
- VOLLERY Luc, Accès à des directives et à des informations budgétaires sur les informateurs de la police, RFJ 2019, pp. 186 ss.
- WEBER Rolf H. David, Zugang zu maschinengenerierten Daten, jusletter du 2 décembre 2019.

- WEYDNER-VOLKMANN Sebastian/FEITEN Linus, Vertrauensstiftende Videoüberwachung?, digma 2019, pp. 218 ss.
- WIDMER Barbara, Der lange Weg der digitalen Grundbuchzugriffe: Die Aufsicht über die Plattform Terravis – Oder: Wer kann elektronisch gestützt worauf, wie und auf welche Grundbuchdaten zugreifen?, PJA 12/2019, pp. 1303 ss.
- WIDMER Barbara, Der lange Weg der digitalen Grundbuchzugriffe: Die Aufsicht über die Plattform Terravis – Oder: Wie die Verantwortlichen die Aufsicht über die Plattform Terravis und deren Nutzer wahrnehmen, PJA 1/2020, pp. 30 ss.
- ZIEGLER Noémi/VASELLA David, Informationelle Selbstbestimmung, digma 2019, pp. 158 ss.
- ZOLLINGER-LÖW Floriane/KUHN Anna, Datenschutzrecht und Fernmelderecht im Internet of Things, jusletter du 2 décembre 2019.

~~~~~  
**Important**  
~~~~~

*N'hésitez pas à nous faire parvenir des informations pour un prochain numéro, envoyez vos messages avec une référence Internet à: [ppdt@etat.ge.ch](mailto:ppdt@etat.ge.ch)*

*Si vous ne souhaitez plus recevoir ce bulletin, vous pouvez vous désinscrire de cette liste de distribution en écrivant à: [ppdt@etat.ge.ch](mailto:ppdt@etat.ge.ch)*