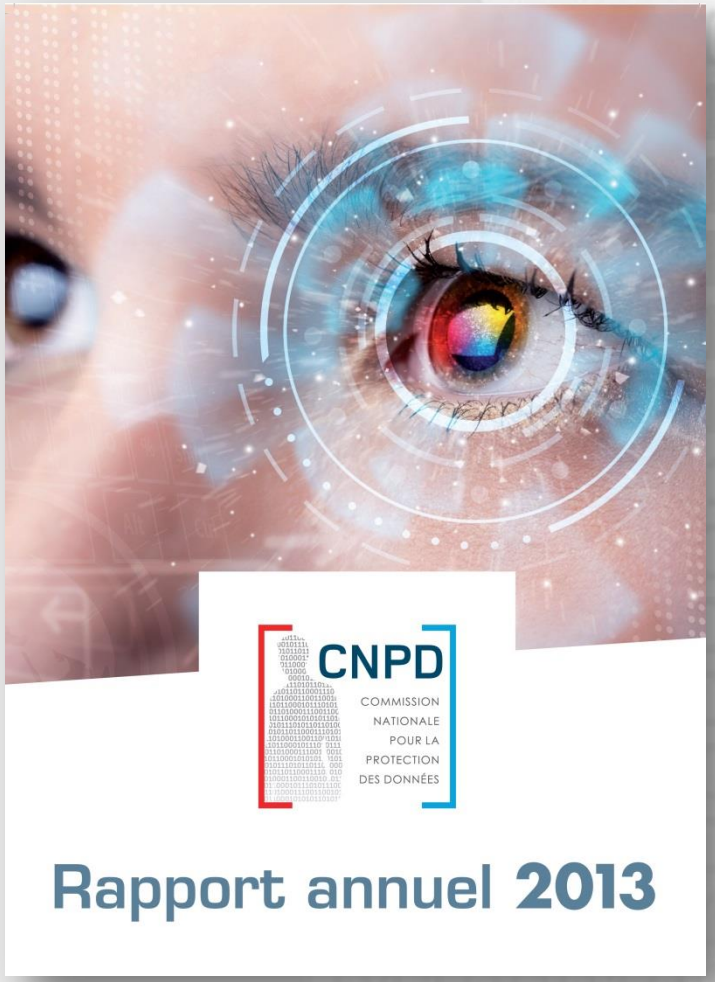
Commission nationale pour la protection des données



Présentation du rapport d'activité 2013

Conférence de presse du 27 mai 2014

Forte augmentation des sollicitations

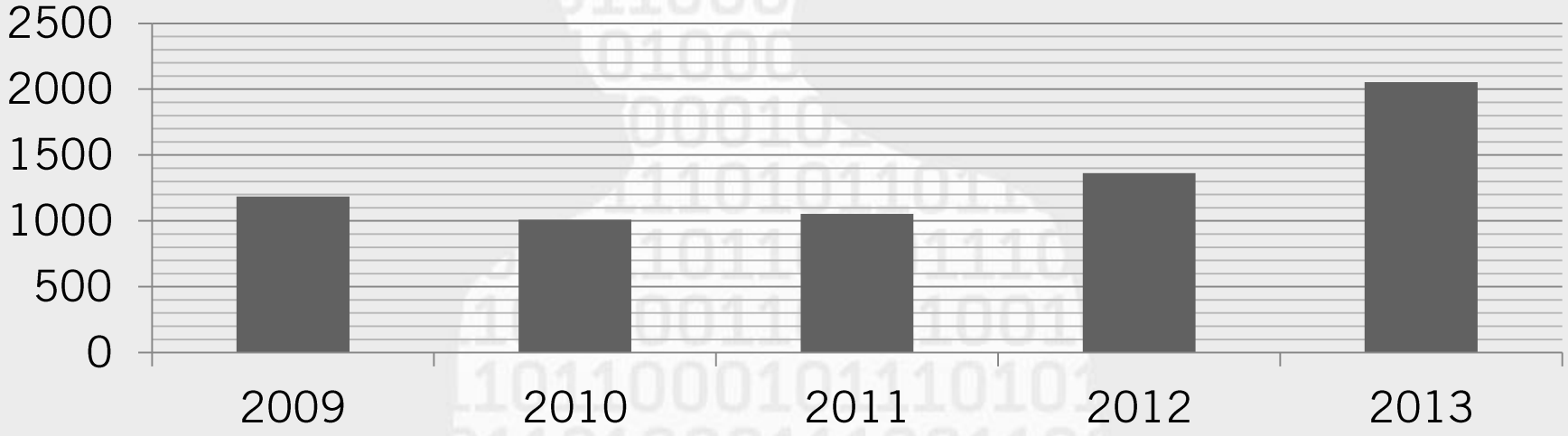
- 2054 déclarations, dont 833 soumises à autorisation préalable
  - >700 systèmes de surveillance sur le lieu du travail
  - >85 transferts de données vers des pays tiers sans niveau de protection adéquate
- De plus en plus de demandes de vérification et de plaintes:177
- 26 contrôles et investigations
- 2077 demandes de renseignement
- 10 avis législatifs ou réglementaires
- 20 agréments de chargés de la protection des données

Formalités préalables

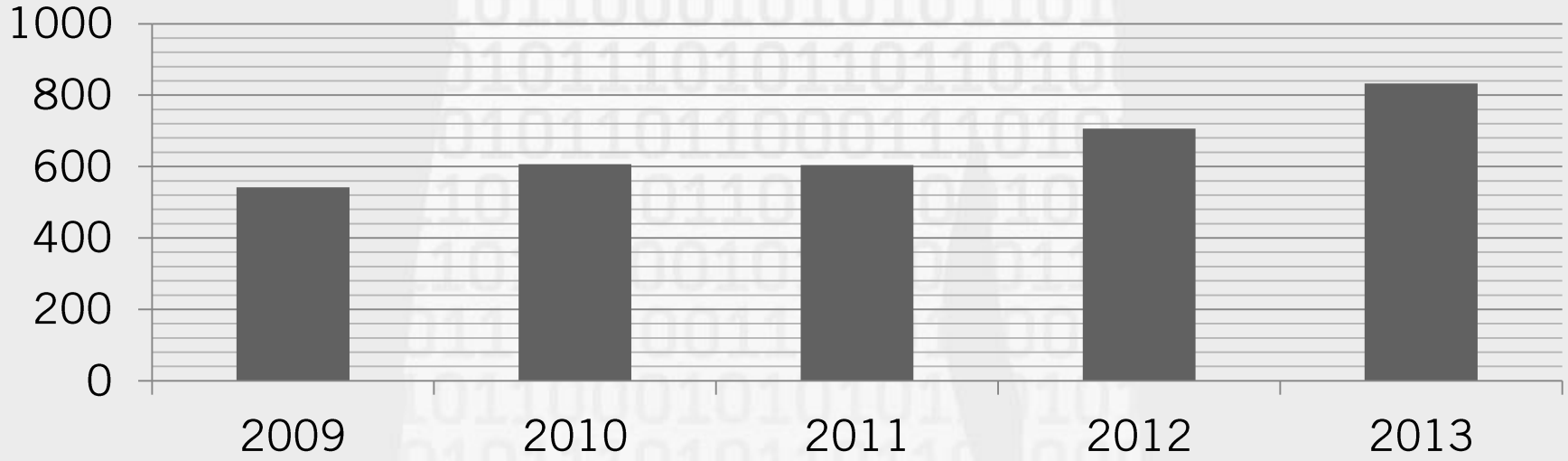
	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	
a) Notifications												
Notifications ordinaires	2.646	850	500	250	760	385	345	295	355	437	421	7.244
Notifications simplifiées	750	900	720	890	537	-	-	-	-	-	-	3.797
Engagement de conformité	-	-	-	-	-	942	227	15	46	149	651	2.030
Total	**3.396**	**1.750**	**1.220**	**1.140**	**1.297**	**1.327**	**572**	**310**	**401**	**586**	**1.072**	**13.071**
b) Autorisations préalables												
Demandes d'autorisation	765	406	317	295	392	606	542	607	604	706	833	6.073
Engagements de conformité	718	14	17	19	151	220	70	92	49	70	149	1.569
Total	**1.483**	**420**	**334**	**314**	**543**	**826**	**612**	**699**	**653**	**776**	**982**	**7.642**
c) Total	**4.879**	**2.170**	**1.554**	**1.454**	**1.840**	**2.153**	**1.184**	**1.009**	**1.054**	**1.362**	**2.054**	**20.713**
d) Déclarants *(responsables ayant accompli des formalités)*	*2.220*	*2.500*	*2.850*	*3.300*	*3.754*	*4.357*	*4.772*	*5.110*	*5.399*	*5.821*	*6.559*	

Formalités préalables

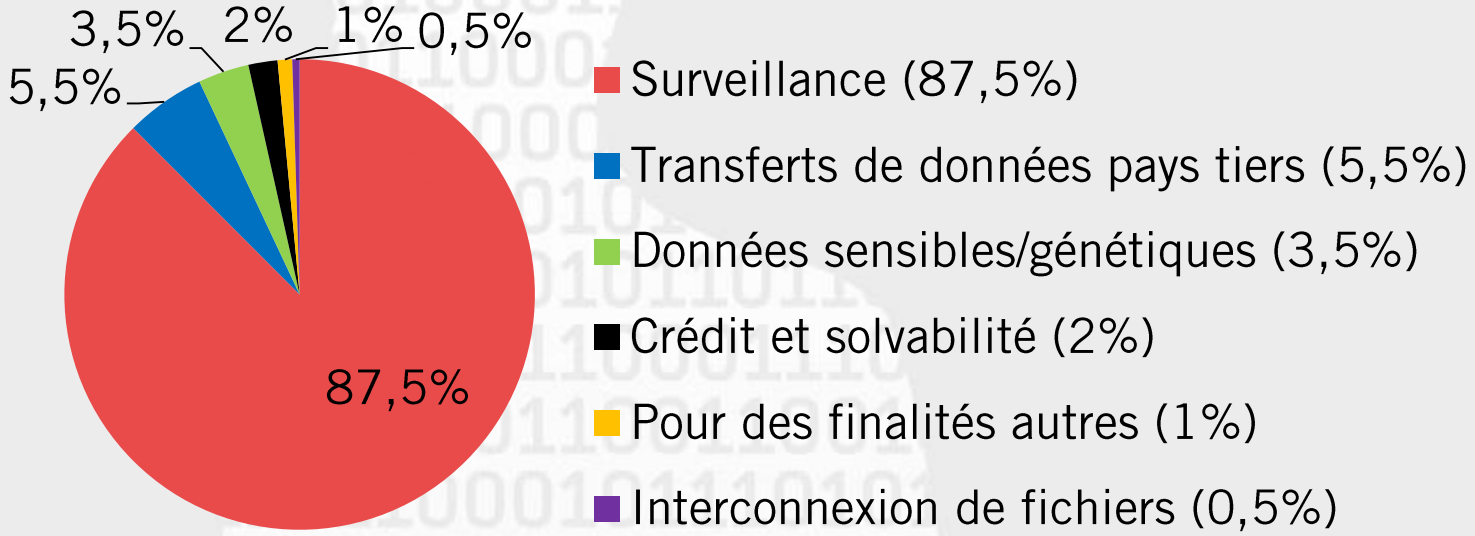
Notifications et autorisations préalables (2009-2013)

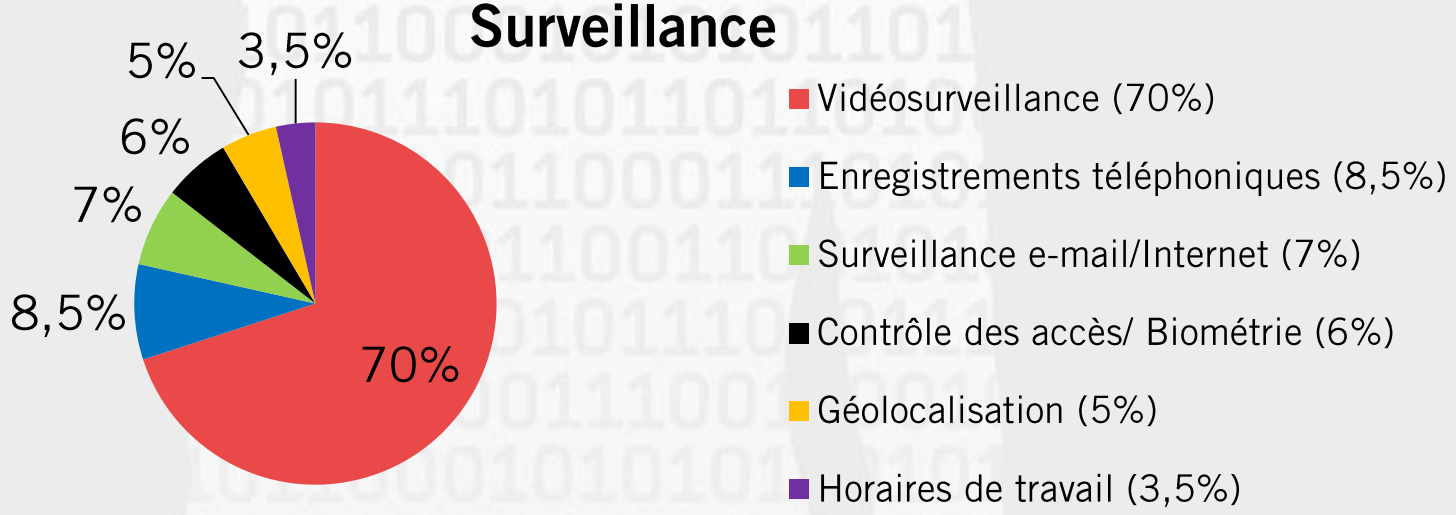


Demandes d'autorisation (2009-2013)

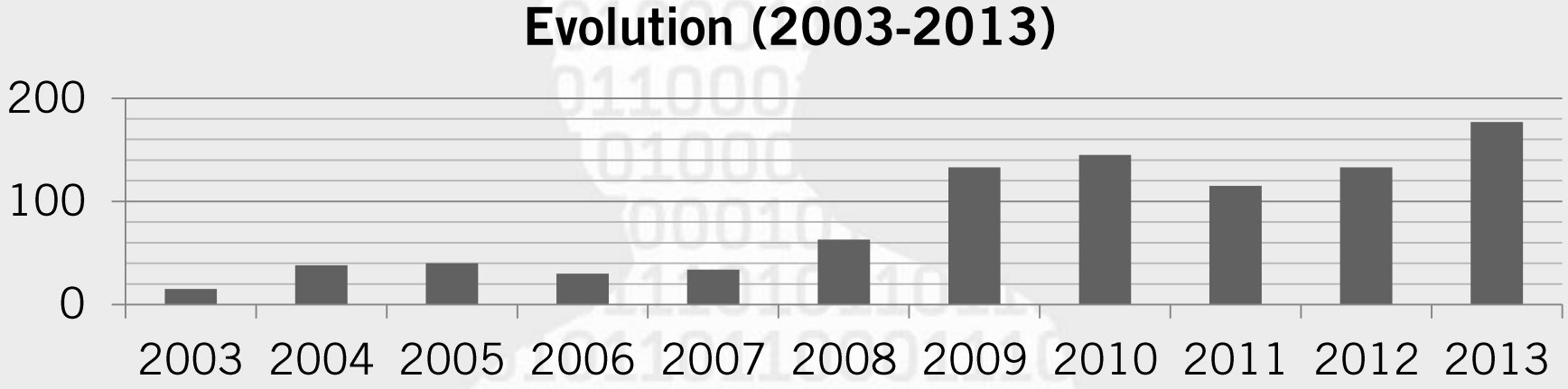


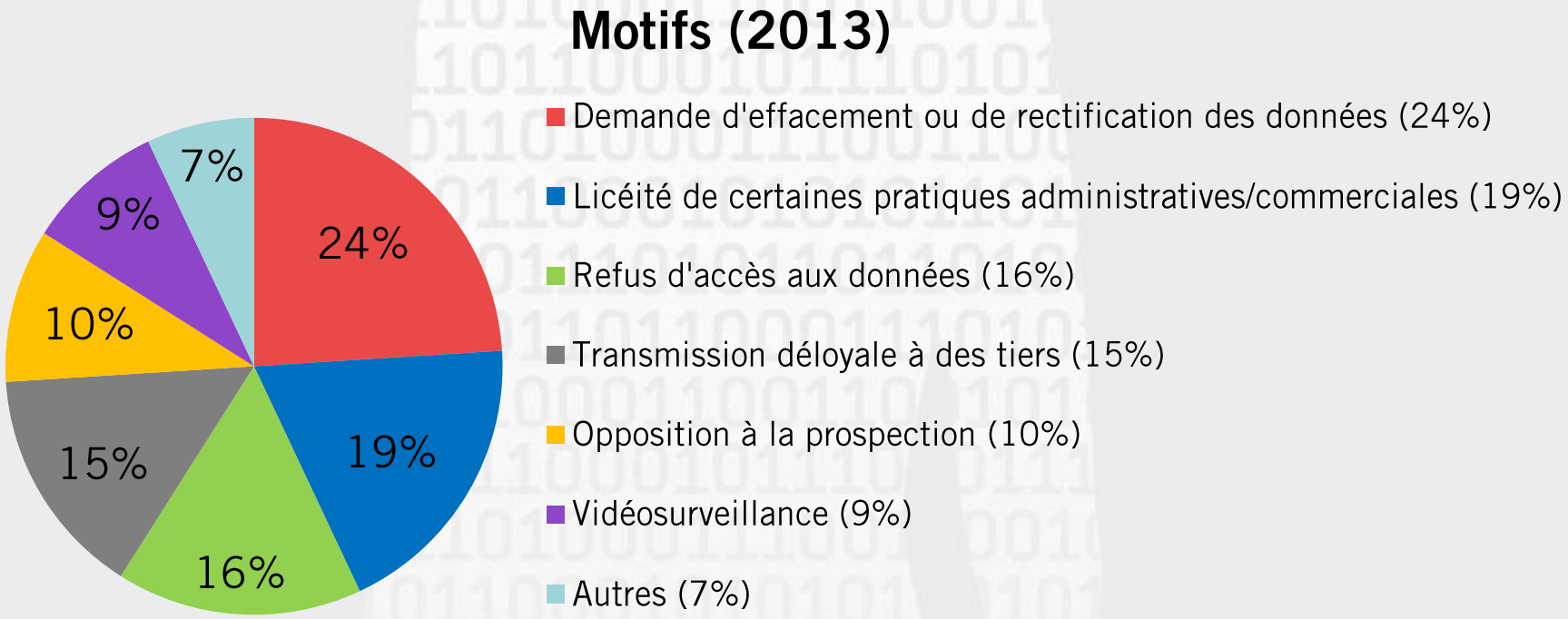
Autorisations préalables – traitements (2003-2013)





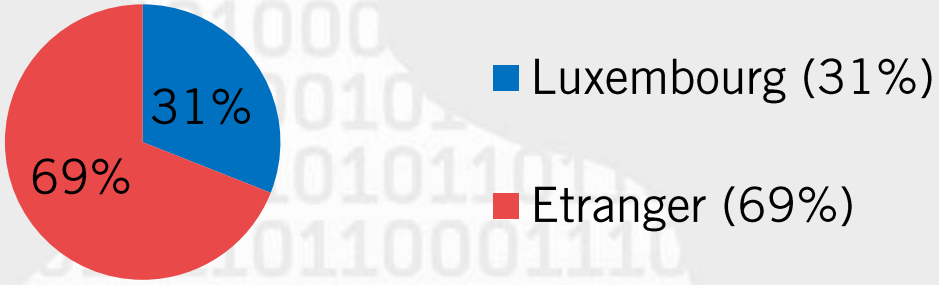
Plaintes et demandes de vérification



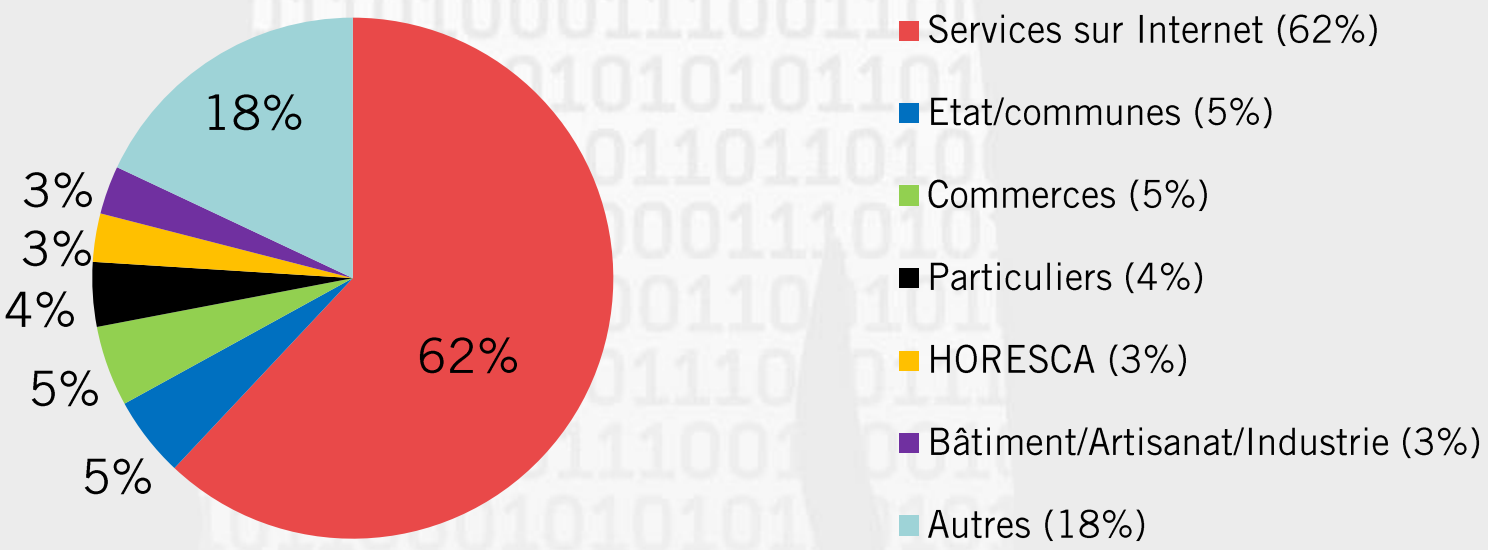


Plaintes et demandes de vérification

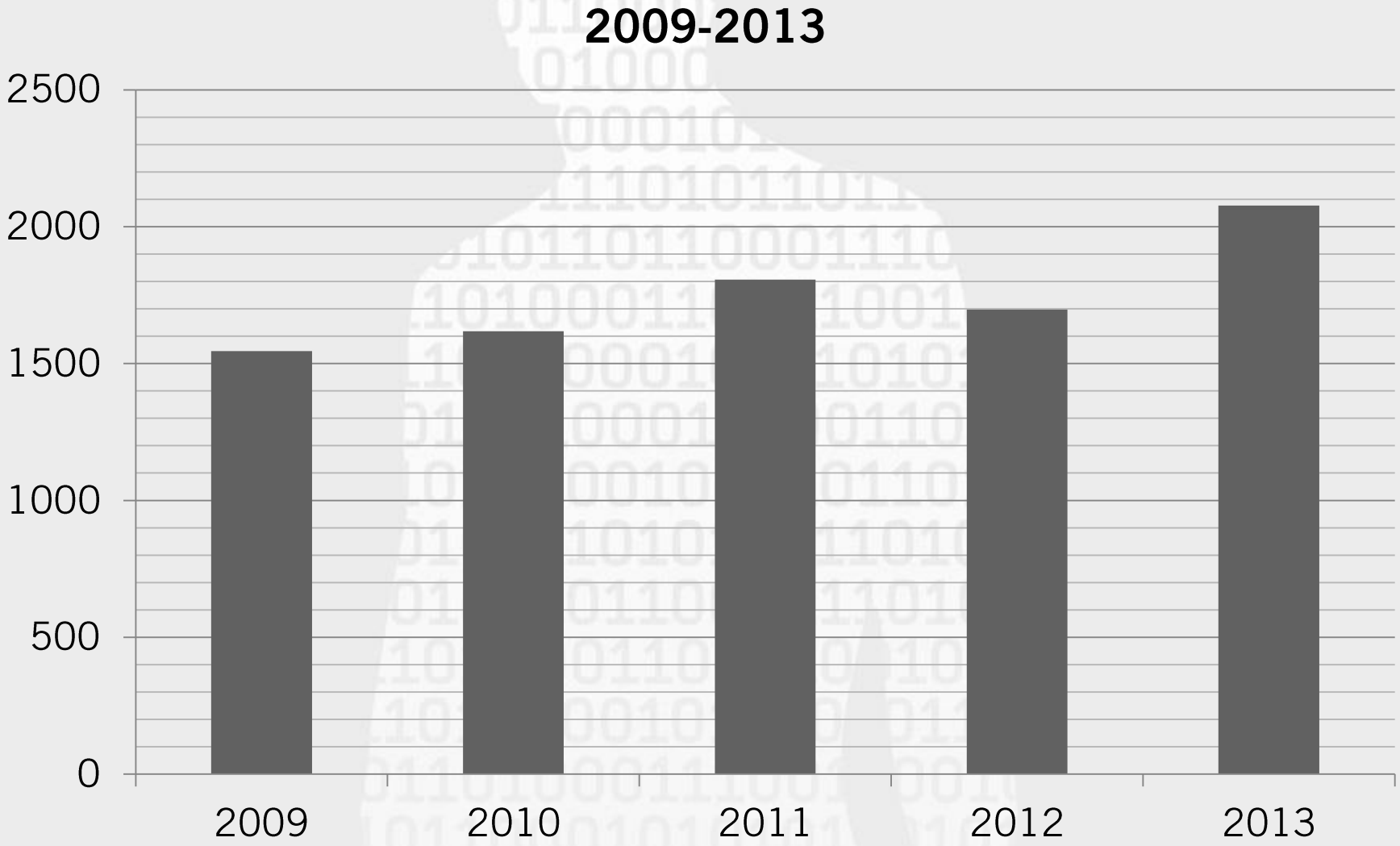
Origine (2013)



Secteur d'activité (2013)



Demandes de renseignement



Avis de la CNPD de plus en plus demandé

- Réglement grand-ducal sur l'organisation du **Service de Renseignement de l'Etat**;
- … le statut, les modalités de désignation et les attributions du **médecin-coordinateur**;
- La réforme de la législation sur la **fonction publique** (PL6457);
- La **réforme de l'exécution des peines** (PL6381) et **réforme de l'administration pénitentiaire** (PL6382);
- L'échange transfrontalier dans l'UE d'informations concernant les **infractions en matière de sécurité routière** (PL6566);
- *La CNPD a attiré l'attention sur la transposition non satisfaisante de la décision-cadre 2008/977/CE* (protection des données échangées dans le domaine pénal)
- Le **registre national du cancer**;
- Les modalités du **comptage de l'énergie électrique et du gaz naturel**;
- L'organisation du **centre socio-éducatif de l'Etat**;
- Règlementation de **l'accès à certaines professions**;
- **PL 6394 portant approbation de différents accords en matière de coopération transfrontalière**.

Des dossiers technologiques sophistiqués et souvent à implications transfrontalières

- **Examen critique des conditions contractuelles MSA de Microsoft pour EMEA (2013)**
  - porte sur le contenu de l'information fournie aux utilisateurs, la gestion de la publicité comportementale, combinaisons de données entre services offerts, périodes de rétention des données, potentielles analyses de contenu des utilisateurs…
- **Contrôle Skype et Microsoft (2013/14)**
  - plaintes reçues en juin 2013 concernant l'exposition des données des utilisateurs européens au programme PRISM
- **Dialogue et enquête Amazon (2012/13)**
  - concernant l'organisation et les modalités de traitements des données personnelles effectués en Europe
- **Approbation des BCR** (Binding Corporate Rules) **du groupe ArcelorMittal (2013)**

Conseils et guidance

- Accompagnement du cadre réglementaire en élaboration avec des PIA (Evaluation d'impact sur la vie privée):
  - **PIA smart metering** (Accompagnement de Luxmetering dans la mise en place des compteurs intelligents d'électricité et de gaz)
  - **PIA eSanté** (DSP - dossier de soins partagés)
- Entrevues et consultations régulières (Agence E-santé, Fédération des hôpitaux, Biobanque, CNER, CEFIS, STATEC, CEPS INSTEAD, Commission du registre national des personnes, ABBL, etc.)
- Projet d'édition de brochures et guides d'orientation et organisation périodique d'ateliers thématiques/sectoriels

Communication et prospective

- Partenariat avec SnT/Université du Luxembourg (depuis 2011): *nouvelles tendances de la régulation et innovations technologiques (privacy by design)*
- Conférences, interventions et formations: Uni.lu, ISACA, Association des chargés de la PD, KPMG, CASES, INAP, ALCO, Union Internat. des Avocats,…
- Création d'une association pour la protection des données au Luxembourg (début 2014)
- *L'enjeu des droits individuels dans notre monde connecté, à l'ère du numérique, des possibilités technologiques sans limites de surveillance, de profilage interpelle et nécessite des réponses européennes.*

Partenariat avec SnT/Université du Luxembourg

Conférence de D. Spielmann (2013)

Conférences et formations

Participation aux travaux européens

- **Groupe de l'Art. 29** (Art. 29 Working Party), sous-groupe Internet et technologique, divers autres sous-groupes sectoriels ou thématiques (santé & recherche, biométrie, e-Government, flux internationaux de données, secteur financier…)
- Comité consult. de la Convention 108 du Conseil de l'Europe T-PD
- **Groupe de Berlin** (secteur ICT et télécom.)
- « *Case handling Workshop* » (Echanges d'expérience dans le traitement des plaintes et de cas pratiques)
- Accompagnement des travaux du DAPIX et du CAHDATA (CoE) : consultations gouvernementales sur le paquet législatif de réforme du cadre juridique communautaire et sur la révision de la Convention 108
- **Association des autorités francophones** de protect. des données
- Adhésion au « *Global Privacy Enforcement Network* » (**GPEN**) en octobre 2013

Conclusions

- **A poursuivre**: Information des citoyens, consommateurs, internautes
  - Recherche de relais dans la société civile (ULC, syndicats, …) formations et conférences; collaboration suivie avec Cases, BeeSecure, interaction avec d'autres autorités, organismes publics et diverses organisations sectorielles/professionnelles…
- **A développer:** Activités de guidance des acteurs et de promotion des bonnes pratiques, capacité d'enquête et de contrôle renforcée
- La coopération internationale s'intensifie, l'assistance mutuelle deviendra obligatoire entre autorités de protection, "actions concertées"
  - Perspective: Harmonisation européenne à venir: «one stop shop» et *«consistency mechanism»,* sollicitations qui augmentent déjà, enquête Microsoft analyse MSA ensemble avec la CNIL,…
  - Ces dernières années la CNPD a gagné en reconnaissance, Spring Conference 2012
  - Crucial au vu des intérêts des entreprises à activité transfrontalière établies à Luxembourg (TIC, services en ligne, etc) Amazon, Skype-Microsoft, eBay-PayPal,…
- **A renforcer**: Effectifs de la CNPD (actuellement 13 + 2 experts CDD)
  - Consolider la crédibilité internationale acquise et conforter ses moyens d'action

Présentation du rapport d'activité 2013

Conférence de presse du 27 mai 2014

Questions?

CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

Gérard Lommel
Pierre Weimerskirch
Thierry Lallemang

Commission nationale pour la protection des données

Nouveau règlement européen: *"Accountability"*

- Responsabilisation des acteurs, incitatifs de bonnes pratiques
  - Privacy by Design (Protection des données dès la conception)
    - Les systèmes et architectures devront être adaptés suivant les considérations de protection des données dès leur conception
  - Privacy / DP by Default
    - Datenschutzfreundliche Voreinstellungen (réseaux sociaux, messageries)
  - Outils modernes d'évaluations des risques/ vie privée (PIA, DP Audits)
  - Certification / Chartes intra entreprise/groupe
    - L'attribution de labels contribuera à forger la confiance des utilisateurs
  - Désignation de chargés internes, délégués à la protection … (DPO)
    - Obligatoire du moins dans les grandes entreprises, celles traitant des fichiers massifs ou sensibles ainsi que dans le secteur public
    - Rôle: Experts internes et interlocuteurs des APD, traitement des plaintes
- Généralisation de la déclaration des incidents *« Data Breach notification »*
  - Les violations de la sécurité/confidentialité des données devront être notifiées dans des délais brefs, rendues publiques dans les cas graves

Avancées de la réforme: Effectivité

- Allègements des formalités obligatoires; « one stop shop » pour les entreprises et proximité pour les citoyens (recours)
- Des règles uniformes dont le respect pourra être imposé
- Des autorités de protection des données avec des dents *(Pas de simples "Paper tiger")*
  - Statut et indépendance des APDs nationales renforçés
    - Moyens et ressources nécessaires
    - Pouvoirs d'investigation et de sanction
      - Amendes jusqu'à hauteur de 2% du chiffre d'affaires annuel/groupe
    - Renforcement de la coopération des APD. Assistance mutuelle
    - Enquêtes et actions conjointes de mise en conformité en EU
  - Coordination de leur action, uniformisation de l'interprétation juridique via le Comité Eu de la Protection des Données (*mécanisme de cohérence*)