COMMISSION CANTONALE DE LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

Président a.h. : Olivier Vallat
Membres : Luc Dobler et Philippe Berthoud
Secrétaire : Gladys Winkler Docourt

DECISION DU 29 MARS 2012

dans la procédure introduite d'office, ainsi que sur requêtes de

1. **X**;
   - représenté par **Me Jean-Marie Allimann**, avocat à Delémont,
2. **Y**;
3. **Z** ;
   - représenté par **Me Alain Schweingruber**, avocat à Delémont,

requérants,

concernant le traitement de données personnelles de fonctionnaires et magistrats dans le cadre de la surveillance informatique intervenue, fin 2008 et début 2009, au sein de la fonction publique jurassienne.

CONSIDERANT

En fait :

A. Par courrier du 29 janvier 2009, A., responsable du Groupe Sécurité au sein du Service de l'informatique (ci-après le SDI), a soumis au Président de la Commission de protection des données (ci-après la CPD) le descriptif d'un processus relatif à la manière de procéder en cas d'abus d'utilisation des accès à Internet. Le SDI sollicitait un avis dans les plus brefs délais sur la conformité de ce processus aux règles de la protection des données et à la Directive technique du 13 mars 2001 relative aux enregistrements et à la surveillance informatique au sein de la République et canton du Jura, validée par le Gouvernement et la CPD.

Le processus décrit par A. comprenait les étapes suivantes :

1. Des lenteurs et des dysfonctionnements de l'accès à Internet sont constatés.

2. Afin d'en déterminer la cause, un contrôle technique de routine est initié par le SDI.

3. Ce contrôle amène le SDI à effectuer une analyse technique des journaux d'accès à Internet, sur une période de 5 jours, week-end compris.

4. Le SDI découvre, au sein de cette liste, des noms de sites explicitement pornographies, voire pénalement répréhensibles si l'on considère les catégories mentionnées à l'article 197 du Code pénal suisse.

5. Face à ce constat, l'analyse est étendue à une période d'un mois.

6. Compte tenu de la volumétrie importante des journaux d'accès à Internet durant la période, une société externe spécialisée est mandatée pour extraire une liste des sites pornographiques et en faire un rapport mentionnant les postes informatiques ayant accédé plus de cent fois à de tels sites durant le mois.

7. Les adresses IP associées à ces noms de sites permettent au mandataire et au SDI de retrouver les noms des services et plus précisément l'identifiant (numéro d'inventaire) pour une grande partie des postes informatiques ayant servi à commettre ces abus.

8. Les outils de gestion d'inventaire du SDI ne permettant pas de lever le doute dans certains cas (remplacement de certains postes, postes partagés entre plusieurs collaborateurs, postes itinérants, etc.), il est suggéré d'étendre la vérification en effectuant une analyse technique directe des postes informatiques concernés.

9. Pour chacun des postes concernés, le responsable du support technique du SDI prend contact par téléphone avec la personne connectée sur le poste et lui demande l'autorisation que l'on prenne son poste en télémaintenance, dans le cadre des accès Internet, sans pour autant expliquer la nature exacte de cette opération ; le risque étant en effet grand que les traces probantes soient alors supprimées dans le cas où la personne contactée est effectivement à l'origine de ces accès.

10. Une fois le poste pris en télémaintenance, le mandataire effectue à l'aide d'un outil spécialisé, une recherche de mots-clefs de type « sex », « porno », etc., parmi les fichiers de gestion technique « index.dat » situés sur le disque C:.

11. Lorsque des éléments probants sont identifiés, les traces sont sauvegardées par le mandataire. Lorsque le poste ne révèle aucune trace pertinente, il est supprimé de la liste.

12. La procédure est suivie de manière strictement identique pour chacun des postes et réitérée jusqu'à ce que l'ensemble des postes concernés ait été vérifié.

13. Une fois les traces collectées, le mandataire vérifie si, pour les sites pornographiques affichés, il est fait mention d'un ou de plusieurs identifiants d'utilisateurs (login Novell).

14. Si cela est le cas et qu'il est donc possible d'associer aux sites pornographiques visités un ou plusieurs identifiants Novell, une dernière vérification est réalisée à l'aide du système d'annuaire Novell afin de retrouver l'identité de la ou des personnes concernées ainsi que le nom du ou des services concernés.

15. Une liste nominative est établie.

En date du 30 janvier 2009, le Président de la CPD a répondu au courrier du SDI, en relevant préalablement qu'il ne lui appartenait pas de « valider l'opération », mais qu'il était autorisé à transmettre son appréciation, sous la forme d'un conseil au sens de l'article 50 al. 2 litt. g LPD et sous réserve d'une décision de la CPD qui serait saisie d'office ou sur requête d'une personne concernée. Aux termes de sa réponse et en substance, le Président de la CPD relevait que, d'une manière générale, le processus décrit par le SDI apparaissait conforme aux directives et aux processus préconisés par la doctrine. Toutefois, le Président de la CPD déclarait « réitérer ses doutes quant au chiffre 9 » du processus en question, à savoir la prise en main par le SDI du poste en télémaintenance, sans expliquer à l'utilisateur la nature exacte de cette opération. Toujours aux termes de son courrier du 30 janvier 2009, le Président de la CPD évoquait la question de la transmission de la liste nominative obtenue par le SDI à la fin du processus, en relevant qu'il appartenait au SDI de requérir des instructions auprès du chef du Département auquel est rattaché le Service du personnel, voire auprès du Gouvernement qui exerce l'autorité de surveillance sur l'administration.

B. En date du 11 février 2009, le SDI a adressé au Gouvernement une note, aux termes de laquelle il informait celui-ci du fait qu'à la suite de saturations fréquentes des accès Internet, notamment lors de soucis récurrent durant la retransmission des séances du Parlement, le SDI aurait été amené à réaliser un contrôle de routine afin d'en déterminer les causes et d'y remédier, contrôle qui aurait notamment consisté à examiner l'activité de la passerelle d'accès à Internet « proxy » sur une période de cinq jours. Lors de ce contrôle, la présence de nombreux noms de sites Internet à connotation pornographique aurait été constatée.

Ainsi, du 1er au 5 novembre 2008, au moins 7 postes utilisateurs auraient été utilisés pour accéder à des sites pornographiques de manière intensive. Cette première

analyse, effectuée de façon manuelle par le SDI, aurait permis d'identifier les adresses IP des postes informatiques concernés, le nom des services de l'Etat concernés, la liste des sites Internet visités et les horaires de connexion. Trois services auraient été identifiés comme étant en possession d'ordinateurs ayant servi à accéder à de tels sites de manière assez intense, à savoir la Police cantonale, le Secrétariat du Parlement et les Ponts et chaussées. Le Commandant de la Police cantonale, le Chef de Service des Ponts et chaussées, ainsi que le Président du Parlement auraient été informés oralement de la situation, cela dès la découverte des abus. Suite à une séance avec le SDI, le Commandant de la Police cantonale aurait élaboré une note de service mentionnant que des abus avaient été constatés et que les auteurs des abus en question devaient venir s'annoncer directement auprès de lui pour ne pas subir de sanctions. En parallèle, une séance aurait été organisée avec le Chef du Service du personnel qui aurait abouti notamment sur la décision d'étendre la période d'analyse des journaux sur le mois de novembre 2008 complet, de préparer le dossier à l'attention du Gouvernement et, si nécessaire, lui proposer de démarrer des enquêtes administratives, au moins pour les cas les plus importants.

Une seconde analyse des journaux de connexion Internet, portant cette fois-ci sur la période du 1er au 30 novembre 2008, aurait donc été confiée par le SDI à une société spécialisée en analyses de sécurité, à savoir SCRT Sàrl, à Préverenges (ci-après SCRT). Ladite analyse aurait également permis d'identifier les adresses IP des postes informatiques concernés, le nom des services de l'Etat concernés, la liste des sites visités et les horaires de connexion à ces sites, cela cette fois pour l'ensemble du mois de novembre 2008.

Compte tenu de la présence de certaines références à des sites pouvant relever de l'article 197 CP, le SDI aurait pris contact avec M. C., de la Police judiciaire, afin d'avoir plus d'éléments sur la démarche à adopter. Ce dernier lui aurait confirmé qu'en cas d'accès sur de tels sites, les services compétents de la Police devaient être informés.

Enfin, le SDI mentionnait les contacts téléphoniques avec le Président de la CPD et le courrier de ce dernier du 30 janvier 2009. Selon le SDI, le Président de la CPD aurait confirmé que ce dossier devait suivre son cours, bien qu'un point de la procédure puisse soulever le principe de la bonne foi.

C. Il résulte du rapport « Analyse trafic réseau » de la société SCRT, remis par le SDI au Gouvernement en annexe à sa note du 11 février 2009, que ladite société aurait été mandatée pour effectuer l'analyse des fichiers journaux (logs) du proxy permettant l'accès à Internet depuis le réseau interne de l'Etat du Jura. Cet audit aurait été destiné à déterminer les machines d'où provenaient ces flux, la teneur de ces flux et le volume échangé.

Les données brutes fournies à SCRT l'auraient été sous la forme de fichiers quotidiens au format « log Squid », correspondant au mois de novembre 2008 (du 1er au 30). L'extraction des liens Internet (URL) amenant à des contenus de type adulte aurait été

faite en testant si ces URL contenaient une liste de mots clefs. Ainsi, aux termes de son rapport (ch. 3.1), SCRT produisait une liste recensant les machines, au moyen de leur adresse IP source, ayant fait plus de cent appels (hits) sur tout le mois de novembre 2008 vers un site contenant des mots clés à connotation sexuelle. La liste en question concernait 56 adresses IP et mentionnait, pour chacune d'elles, le nombre de hits effectués vers de tels sites. En outre, les machines ayant effectué le plus grand nombre d'appels (plus de 1000 sur le mois) ont été analysées de plus près par SCRT (ch. 3.2 du rapport). Quelques faux positifs seraient apparus pour certaines de ces machines, représentant toutefois dans la plupart des cas un pourcentage non significatif et une quantité marginale en proportion aux sites réellement illicites. Aux termes de son rapport, SCRT fournissait donc une liste de machines les plus impliquées, identifiées au moyen de leurs adresses IP avec, pour chacune d'entre elles, un graphique représentant le nombre de hits illicites et leur répartition horaire sur tout le mois, un tableau faisant correspondre un nombre de hits à telle heure d'une date donnée, le nom des 50 sites les plus consultés par ordre descendant et un graphique montrant la fréquentation des 10 sites les plus consultés sur le mois. Selon l'extrait du rapport de SCRT contenu dans le dossier fourni par le Gouvernement à la CPD, cette analyse aurait porté sur 17 machines (ch. 3.3 à 3.19).

Sous un chiffre 4 du rapport SCRT, intitulé « Utilisateurs potentiels des machines », il est mentionné que, pour les machines les plus incriminées, des suppositions auraient été faites quant à l'utilisateur-trice de ladite machine lors de la première phase de l'enquête déjà. Ainsi, au moyen de deux logiciels, PsSoft et Zenworks et sur la base de l'état au 7 janvier 2009, SCRT aurait pu réaliser l'association entre la machine et l'utilisateur pour un certain nombre de cas. Cette méthode aurait permis de délimiter une série de machines et d'utilisateurs vraisemblables, mais dépendant de trop de paramètres incontrôlables pour être utilisée sans vérifications. C'est-à-dire que, sans les historiques du DHCP, des doublons seraient apparus dans les résultats et, s'il y avait plusieurs utilisateurs partageant la même machine, les données à disposition n'auraient pas permis de déterminer l'utilisateur concerné. Ceci aurait conduit SCRT à effectuer une seconde phase d'enquête qui a consisté à reprendre les résultats de la première phase et à contrôler sur les postes de travail quels utilisateurs avaient des historiques Internet Explorer contenant des accès à des sites problématiques. Les contrôles ont été faits à distance, par RDP (Remote Desktop Protocol), avec un outil qui a permis de récupérer ces informations et de les sauvegarder pour analyse. Ainsi, toujours aux termes du ch. 4 de son rapport, SCRT fournissait un tableau résumant les résultats de la seconde phase. Celui-ci mentionnait une liste de 35 machines avec, pour chacune d'elles, le nombre de hits problématiques, l'adresse IP initiale, l'adresse IP au 15 janvier 2009, le Département / Service / Office / Tribunal concerné, ainsi que le résultat de l'analyse. S'agissant de la rubrique « Résultat » en particulier, le rapport indiquait pour six machines : « Ordinateur non inventorié au SDI : analyse non effectuée ». Pour les 29 autres machines, figurait dans la rubrique « Résultat » la mention : « Prouvé ».

D. En date du 12 février 2009, le Service du personnel de la République et canton du Jura a adressé au Gouvernement une note relative au rapport « Analyse trafic réseau » de SCRT.

Pour l'essentiel, le Service du personnel indiquait qu'il aurait pris connaissance des documents électroniques relatifs aux abus Internet en date du 27 janvier 2009. S'agissant de la procédure suivie par le SDI, le Service du personnel déclarait partager les doutes exprimés par le Président de la CPD dans sa lettre du 30 janvier 2009, notamment au sujet de la problématique, sous l'angle du principe de la bonne foi, de la prise en main à distance des postes concernés sans en indiquer la véritable raison au collaborateur. Ainsi, le Service du personnel recommandait notamment au Gouvernement, compte tenu des indices d'abus Internet, de collecter les moyens de preuve nécessaires au moyen d'une copie du disque dur du poste de travail, en présence du collaborateur soupçonné. S'agissant des abus commis par des magistrats, le Service du personnel conseillait au Gouvernement de transmettre au Conseil de surveillance de la magistrature les dossiers ressortant de sa compétence.

Enfin, le Service du personnel recommandait d'adapter la directive du 13 mars 2001 relative aux enregistrements et à la surveillance informatique au sein de la République et canton du Jura.

E. En date du 12 février 2009, le Service juridique de la République et canton du Jura a également adressé au Gouvernement une note complémentaire relative au rapport « Analyse trafic réseau » de SCRT.

En substance, le Service juridique relevait que les directives de 2001 manquaient réellement de clarté et soutenait leur révision.

A l'instar du Service du personnel, le Service juridique faisait état de ses doutes quant à la validité de la prise en main faite par le SDI sans en indiquer la vraie raison au collaborateur. En outre, le Service juridique mentionnait que, même si cela n'avait pas été relevé par le Président de la CPD dans son courrier du 30 janvier 2009, les directives soulevaient également des risques quant à la validité de la collecte de données sans avertissement individualisé au collaborateur et préalable au contrôle.

F. Par décisions des 17 et 24 février 2009, le Gouvernement a, notamment, décidé d'ouvrir des enquêtes disciplinaires à l'encontre de 27 collaborateurs mentionnés dans le document « Analyse trafic réseau ».

Par décision du 27 février 2009, le Conseil de surveillance de la Magistrature a également ouvert une enquête disciplinaire à l'encontre de deux magistrats concernés par ledit rapport.

G. En date du 15 mai 2009, la Commission d'enquête disciplinaire présidée par le Juge fédéral Jean-Luc Baechler (ci-après la Commission d'enquête), nommée suite aux décisions du Gouvernement des 17 et 24 février 2009, a rendu son rapport final.

Il en ressort que le rapport d'audit de la société SCRT a été remis à la Commission d'enquête. La Commission d'enquête a elle-même procédé à l'exécution des mesures conservatoires urgentes visant à préserver les moyens de preuve essentiels, composés pour une grande part des disques durs des postes sur lesquels étaient occupés les collaborateurs concernés. Selon le processus décrit par la Commission d'enquête, lors de la saisie des disques durs, intervenue principalement le 5 mars 2009, le collaborateur était informé de l'enquête disciplinaire ouverte à son encontre et des mesures conservatoires qui allaient être opérées. Le disque dur était ensuite extrait de l'ordinateur, puis copié ou séquestré en présence du collaborateur. Enfin, le disque dur était remis en place ou était substitué par un appareil de remplacement.

Une analyse des disques durs copiés ou séquestrés a été ultérieurement réalisée, notamment afin de retrouver les traces d'accès à des sites non professionnels via la poubelle, l'historique et les dossiers provisoires (caches), et de permettre la visite des sites les plus utilisés et d'en copier le contenu sur DVD, d'envisager, le cas échéant, une collaboration avec la police judiciaire ou la police fédérale, d'imprimer un échantillon de clichés aux fins de vérification et d'établir, dans chaque cas, un rapport comprenant notamment le nombre de hits prohibés, les moments de l'utilisation durant la journée ou la nuit, ainsi que la volumétrie. Il est articulé un temps de un jour à un jour et demi de travail par disque pour effectuer ladite analyse. Finalement, les analyses forensiques des disques durs, débutées dès la copie des disques durs litigieux, se seraient révélées plus complexes et plus longues qu'originellement prévu. La Commission d'enquête n'aurait ainsi pu prendre connaissance des rapports d'analyse forensique que peu de temps avant les auditions des collaborateurs, au fur et à mesure de leur élaboration. Ainsi, du 20 mars au 24 avril 2009, la Commission d'enquête a entendu les 27 collaborateurs faisant l'objet d'une enquête disciplinaire. A l'issue des auditions de chaque personne, la commission a rédigé un rapport individuel émettant un avis quant à l'existence ou l'inexistence d'une violation du devoir de fonction, examinant les actes finalement retenus sous l'angle du droit pénal, et posant une évaluation sur le degré de gravité des violations commises. Pour motiver chacun des rapports individuels, la commission d'enquête s'est fondée principalement sur les propres déclarations de l'intéressé, le rapport d'analyse forensique effectué par SCRT, les fiches de timbrage, le dossier personnel et un rapport récent sur les activités professionnelles du collaborateur établi par le supérieur hiérarchique.

Sur le plan juridique, la Commission d'enquête considère que la procédure prescrite par les Directives techniques du 13 mars 2001 relatives aux enregistrements et à la surveillance informatique au sein de la République et canton du Jura – notamment s'agissant des mesures prises en cas d'abus d'accès à Internet – aurait été respectée in casu pour mettre en exergue les comportements abusifs des différents collaborateurs impliqués. En effet, aux termes desdites directives, des mesures pourraient être prises dans deux cas d'abus, à savoir si un comportement est contraire au contrat de travail ou si un comportement est contraire au droit. A cet égard, la Commission d'enquête relève que si le simple manquement au contrat de travail ne justifierait pas en soi un examen des enregistrements existants, en revanche, en cas

d'accès à Internet, une procédure se révèlerait non seulement possible, mais les différentes étapes de celle-ci seraient spécifiquement définies dans les directives mêmes. En l'espèce, les soupçons ne seraient pas nés des contrôles effectués, lesquels n'auraient été que la conséquence d'une anomalie préexistante – une saturation récurrente de l'ensemble du réseau informatique de la RCJU – mais non la cause. Faisant suite à ce dysfonctionnement, un premier contrôle général a été opéré sur une courte période de 5 jours. Cette analyse générale, qui a concerné tous les postes de travail, a permis de mettre en évidence non seulement un abus dans les accès Internet, mais aussi – et surtout – l'accès depuis des postes professionnels, durant le temps de travail, à des sites à caractère pornographique. Ainsi, un tel comportement de la part de certains collaborateurs de l'Etat constituerait manifestement autant une violation de leur contrat de travail que de normes de droit positif administratives et éventuellement pénales. Dès lors que l'ensemble des conditions permettant un contrôle plus avancé étaient réunies, la procédure prévue aux ch. 1 à 4 de la page 2 des directives idoines pouvait être engagée. En particulier, les investigations qui ont suivi, de manière toujours non discriminatoire, ont été étendues sur une période d'un mois entier, soit en novembre 2008. Les contrôles opérés, non discriminatoires, auraient été effectués de manière globale et sur tous les postes informatiques de l'administration (ch. 2 des Directives du 13 mars 2001). Dans la mesure où des soupçons concrets d'abus intolérables ont été mis en évidence, les démarches entreprises subséquemment auraient été rendues nécessaires pour repérer les collaborateurs faillibles au sens de la procédure décrite dans les directives (ch. 3 des Directives du 13 mars 2001). Une note interne avait été adressée à l'ensemble des collaborateurs (ch. 3 des Directives du 13 mars 2001) ; en outre, ceux-ci ont été personnellement informés de l'ouverture de la procédure, peu de temps après que le Gouvernement a été mis au courant des résultats définitifs du mandat mené par SCRT sur l'analyse réseau.

Selon la Commission d'enquête, le Président de la CPD partagerait le point de vue selon lequel la procédure entreprise serait conforme aux directives et aux processus préconisés par la doctrine, vu les termes de son courrier du 30 janvier 2009. S'agissant de la réserve quant à la prise des postes en télémaintenance en n'expliquant pas la nature exacte de l'opération, la Commission d'enquête relève qu'il conviendrait de ne pas perdre de vue que le but de ces interventions était précisément de découvrir d'éventuels sites à caractère pornographique sur les appareils identifiés et, de cette façon, de procéder à une sélection entre les appareils vierges de sites à caractère pornographique des autres. De ce constat, il en découlerait tout naturellement que si les personnes contactées avaient été au fait de la raison précise de la démarche, le risque de destruction des traces probantes aurait été très important. Pour le surplus, même si le procédé pourrait paraître à la limite de la bonne foi, rien n'aurait changé quant au fond de l'affaire : les possesseurs des appareils auraient malgré tout fait l'objet d'une enquête disciplinaire (puisque leur appareil avait précisément été identifié) ; seulement, sans cette procédure préalable de sélection, au lieu d'une trentaine de cas, il y en aurait eu le double selon le SDI. On ne saurait donc raisonnablement en déduire une entorse au principe de la protection des données.

Bien au contraire, cette procédure préalable aurait permis d'éviter l'ouverture d'une trentaine d'enquêtes supplémentaires avec toutes les conséquences négatives que cela suppose pour les intéressés qu'elle qu'en soit l'issue.

H. Par courrier du 10 juin 2009, suite à l'ouverture par le Président de la CPD d'une procédure d'office tendant à examiner la régularité de la surveillance Internet intervenue à l'égard des membres de la fonction publique, le Président du Conseil de surveillance de la magistrature a indiqué au Président de la CPD qu'il avait été informé, le 24 février 2009 par téléphone, puis lors d'une séance du 27 février 2009, de l'enquête menée par le SDI concernant la consultation de sites Internet par des magistrats de l'ordre judiciaire. En outre, le Conseil de surveillance de la magistrature a indiqué n'avoir pas lui-même ordonné ou autorisé le SDI à identifier les magistrats suspectés de consultations illicites. La liste nominative des personnes suspectées lui a été fournie lors de la séance du 27 février 2009. C'est également à cette date qu'une enquête disciplinaire contre les magistrats concernés a été ouverte par le Conseil de surveillance de la magistrature.

I. Par courrier du 7 juillet 2009 adressé au Président de la CPD dans le cadre de la même procédure d'office, le Gouvernement a indiqué que c'était en date du 17 février 2009, lors de la présentation du rapport technique d'analyse du trafic réseau, que celui-ci avait été informé officiellement de l'enquête menée par le SDI concernant la consultation de sites Internet non autorisés au sein de la fonction publique jurassienne et que la liste nominative des personnes suspectées lui avait été communiquée. Le Gouvernement n'a pas non plus ordonné ou autorisé préalablement le SDI à identifier les membres de la fonction publique suspectés de consultations illicites. Cependant, le Gouvernement relève que l'article 146 DOGA attribuerait au SDI la responsabilité du traitement électronique de l'information. Il reviendrait donc au SDI de s'assurer de son bon fonctionnement et d'appliquer les mesures qui s'imposent en cas de dérangement. Le Gouvernement se réfère également aux différents échanges téléphoniques du mois de décembre 2008 entre le responsable de la sécurité au sein du SDI et le Président de la CPD, échanges téléphoniques qui auraient permis de valider la procédure de contrôle des accès Internet. De plus, le Gouvernement renvoie à la position du Président de la Commission d'enquête disciplinaire qui retient que la procédure prescrite par les Directives techniques du 13 mars 2001 aurait été respectée. Enfin, c'est en date du 24 février 2009 que l'ouverture d'enquêtes disciplinaires contre les fonctionnaires suspectés a été décidée par le Gouvernement.

J. Par décisions du 2 octobre et 23 novembre 2009, la Cour administrative a, notamment, admis la demande de déport présentée par le Président de la CPD et désigné son remplaçant.

K. En date du 2 mars 2010, la CPD a entendu M. B., chef du SDI, et M. A (responsable du Groupe Sécurité au sein du SDI) .

Il ressort des auditions précitées, en substance, qu'en date du 29 octobre 2008, de nombreuses personnes ne seraient pas parvenues à visionner la retransmission en direct de la séance du Parlement, ce qui aurait débouché sur des demandes de support adressées au SDI. Celui-ci en aurait déduit l'existence d'un problème d'accès, respectivement de saturation de la bande passante. Le SDI aurait également constaté une saturation périodique de la bande passante durant la journée, ce qui aurait perturbé l'envoi et la réception de mails et pas seulement l'accès à Internet. Un échantillon a donc été analysé pour comprendre le phénomène de saturation, du samedi 1er au mercredi 5 novembre 2008. Lors des recherches manuelles des anomalies de bande passante, il aurait été découvert fortuitement de nombreux sites contenant le mot « sex ». M. A. aurait ensuite déterminé les adresses IP à l'origine des consultations de ces sites suspects, pour savoir si elles étaient d'origine interne, paraétatique ou externe. A l'aide de ces adresses IP, il aurait déterminé la localisation géographique, à un étage près ou au niveau du bâtiment, des services concernés. Trois services semblaient très affectés par ce problème, à savoir les Ponts et chaussées, la Police cantonale et le Parlement. M. A. aurait téléphoné directement aux chefs de service concernés et averti son supérieur, M. B.. Seul le Commandant de la Police cantonale aurait réagi aux remarques faites par le SDI. En raison des informations découvertes, le SDI aurait décidé d'étendre l'analyse au mois de novembre 2008 en recourant à une société externe, à savoir SCRT. Celle-ci a fourni son rapport le 19 décembre 2008, faisant état de 54 adresses IP ayant généré du trafic à caractère pornographique. Au vu des sites recensés, il n'aurait pas été exclu que certains aient un caractère pénal et si le SDI n'avait rien entrepris, SCRT aurait pris des mesures telles qu'une dénonciation pénale. Dès lors, fin décembre 2008, le SDI aurait pris contact avec le Service du personnel afin de l'informer de la situation, des contrôles effectués et des résultats obtenus, ainsi que de la nécessité de poursuivre les investigations.

Comme le système DHCP alloue les adresses IP qui pourraient varier d'un jour à l'autre, un poste n'aurait pas toujours la même adresse IP. Il n'aurait donc pas été possible de se contenter du rapport de SCRT du 19 décembre 2008 et il aurait été nécessaire de procéder à des contrôles supplémentaires. Les investigations ultérieures, à savoir la prise en main à distance des postes soupçonnés, auraient eu lieu en parallèle avec les démarches effectuées auprès du Président de la CPD au mois de janvier 2009. Sur la base des informations données par celui-ci, par téléphone et courrier, le SDI aurait pris le contrôle des postes à distance. Selon A., il fallait agir très vite, en dépit des réserves émises par le Président de la CPD dans son courrier du 30 janvier 2009, pour éviter que les données de novembre 2008 soient écrasées. Dans le cadre de la prise en main des postes à distance, l'utilisateur donnait son approbation pour que le SDI prenne le contrôle du poste. Selon M. B., à ce stade, le SDI n'effectuait pas d'enquête et les données récoltées ne servaient pas de moyens de preuve. Les outils peu fiables dont disposait le SDI à cette époque ont fait que l'agrégation des données contenait des erreurs et que des postes soupçonnés l'étaient à tort. Les outils utilisés n'auraient pas été en mesure de fournir des preuves assez précises. La prise en main à distance aurait permis de passer de 54 à 30 postes. Même avec la prise en

main, il y aurait eu encore des faux positifs qui ont été révélés avec la saisie des disques durs. La prise en main à distance n'aurait pas visé à récolter des preuves formelles mais à permettre de constituer un dossier à l'attention du Gouvernement, pour que celui-ci décide en toute connaissance de cause s'il souhaitait aller plus loin. Pour le SDI, seule la saisie des disques durs pouvait fournir des preuves utilisables dans une enquête ultérieure. En particulier, les rapports du SDI, puis ceux élaborés par SCRT durant cette étape, n'auraient pas été utilisés comme moyens de preuve lors de l'enquête de la Commission présidée par le Juge Baechler. Il s'agissait en revanche d'arriver devant le Gouvernement avec un dossier solide et d'éviter de saisir trop de disques durs. Le dossier serait reparti de zéro avec la saisie des disques durs. Les données collectées préalablement, dans le cadre de la prise à distance, n'auraient pas été utilisées ni versées aux dossiers des procédures disciplinaires. Le SDI, respectivement M. A., conserve les données récoltées lors de la prise en main à distance. S'agissant des modalités de la prise en main à distance décrites par M. A. à la CPD, il apparaît qu'un technicien du support du SDI aurait appelé par téléphone l'utilisateur du poste soupçonné pour que celui-ci indique le numéro d'inventaire de son poste (autocollant sur la machine). Ensuite, une demande d'autorisation de contrôle à distance se serait affichée sur l'écran de l'utilisateur. Ce dernier devait donner son accord. SCRT lançait alors le programme X-Ways Trace qui analysait les URL sur le poste, soit les fichiers index.dat, en recherchant les URL dont le nom contenait « .sex ». Selon M. A., l'utilisateur voyait vraisemblablement la recherche par « .sex », les écrans étant partagés. Si des occurrences apparaissaient, le programme permettait de récupérer les URL sur le poste, lesquels étaient ensuite sauvegardés. Les données personnelles des collaborateurs n'auraient pas été contrôlées. Les sites recensés n'auraient pas été consultés. Selon M. B., les outils employés par SCRT permettaient de lancer l'opération très rapidement, sans que l'utilisateur ne voie concrètement ce qui se passait. Les utilisateurs aurait simplement été informés du fait qu'il y avait des « problèmes internet ». En revanche, on n'aurait pas parlé d'abus en lien avec internet, ni de surcharge de réseau. Si le SDI avait indiqué que l'on recherchait des traces, les utilisateurs auraient pu effacer celles-ci, soit en détruisant leur ordinateur, soit en lançant un outil gratuit qui supprime les traces. Au final, le SDI aurait obtenu une liste de postes sur lesquels la présence de traces d'accès à des sites pornographiques était avérée. Mais l'identité des personnes ayant utilisé les postes à ces fins n'était pas établie avec certitude. C'est à ce stade que le Service juridique, le SDI et le Service du personnel ont décidé de constituer le dossier et d'en informer le Gouvernement, le 17 février 2009.

Selon M. A., le Président de la CPD aurait admis, lors de l'échange téléphonique, le fait que la méthode envisagée ne pouvait être différente si l'on voulait pouvoir conserver des traces sans éveiller les soupçons des usagers qui auraient pu les effacer. Cette solution aurait également été conseillée par la société SCRT. Du reste, de l'avis de MM. B. et A., cette étape préliminaire à la poursuite du dossier ne visait qu'à réduire le nombre de postes de travail à traiter par la suite et à éliminer tout faux positif.

Selon M. B., une analyse de disque dur prend 4 à 6 heures et nécessite de disposer du disque dur physique ou de sa copie exacte, alors que la prise en main ne dure que quelques minutes. Lors des enquêtes disciplinaires, la saisie et la copie des disques durs elles-mêmes, en présence du collaborateur, duraient de 1 à 2 heures.

Toujours selon M. B., le Service du personnel aurait été consulté au mois de janvier, puis rapidement le Service juridique aurait été associé de manière informelle aux recherches. Suite à l'analyse effectuée sur les postes de travail fin janvier 2009, ils auraient été associés formellement. Le Chef du Département du Service du personnel et du SDI avaient peut-être l'information « informelle », peut-être le Chef du Département du Service juridique également. Mais l'information formelle, avec un dossier, n'aurait été donnée au Gouvernement que lors de sa séance du 17 février 2009.

L. Par requête du 15 mars 2010, le requérant Z. a saisi la Commission de protection des données, en concluant à ce que celle-ci examine la façon dont l'administration, respectivement le SDI, avait procédé pour obtenir des données contenues dans son ordinateur, respectivement d'autres fonctionnaires ou magistrats, ainsi que la question de savoir qui avait la compétence d'ordonner la surveillance et l'enregistrement de telles données informatiques et, enfin, si et dans quelle mesure le Gouvernement jurassien était habilité à divulguer, respectivement à rendre publique, l'enquête ouverte à l'encontre du requérant, respectivement d'autres fonctionnaires ou magistrats. En outre, le requérant concluait à ce que la Commission constate l'illicéité des démarches et comportements mentionnés ci-dessus et en désigne les auteurs, le tout sous suite des frais et dépens.

A l'appui de ses conclusions, le requérant relevait, en substance, que le Gouvernement de la République et canton du Jura avait décidé, en date du 3 mars 2009 et alors que le requérant occupait la fonction de Secrétaire du Parlement jurassien, l'ouverture d'une enquête à l'encontre de celui-ci, suite à des informations fournies par le SDI. Selon le requérant, ce même SDI aurait utilisé un prétexte, respectivement un faux motif, pour obtenir des fonctionnaires concernés l'autorisation de s'introduire dans le disque dur de leur PC, afin d'obtenir les informations en question. Or, selon l'usage et la réglementation en la matière, lorsque le SDI veut avoir accès aux données contenues dans un PC, il devrait préalablement en faire la demande à son utilisateur, en indiquant clairement le motif d'une telle demande. Le requérant mentionne encore que le Gouvernement jurassien aurait, de son propre chef, diffusé une très large information au sujet de l'affaire en question, ce qui aurait entraîné un préjudice considérable pour le requérant. Ce dernier demande ainsi à la CPD de constater l'illicéité, au sens de l'article 36 al. 1 lit. c de la LPD, des démarches entreprises par l'administration.
En outre, par courrier du 6 avril 2010, le requérant sollicitait auprès de la Cour administrative la récusation de l'un des membres de la CPD.

M. Par requête du 16 mars 2010, le requérant Y. a également saisi la CPD, en concluant à ce que celle-ci constate le caractère illicite du traitement des données à caractère personnel qui figuraient sur son PC professionnel, alors qu'il exerçait la fonction de Procureur général, cela entre la période se situant entre la fin de l'été 2008 et fin février 2009, à ce que la CPD formule toutes autres constatations utiles sur la légalité du déroulement de cette enquête administrative en lien avec les dispositions sur la LPD, notamment avec les principes définis sous section 2 de ladite Loi, en particulier sur la communication et la diffusion qui ont été faites des données récoltées, et à statuer ce que de droit sur les frais.

Le requérant invoque, notamment, qu'il aurait fait l'objet, courant novembre 2008, d'une surveillance de son ordinateur professionnel qui ne lui aurait pas été communiquée et dont le motif officiel (lenteurs dans l'utilisation de la messagerie et d'Internet) ne serait pas établi scientifiquement. En outre, le SDI aurait utilisé de faux prétextes pour prendre en main son ordinateur aux fins d'identification. Or, l'accès à de telles données par le SDI aurait nécessité une demande préalable auprès de l'utilisateur, avec l'indication claire du motif d'une telle demande. Le processus d'identification aurait donc été, à tout le moins, contraire au principe de la bonne foi. De plus, agissant sans mandat du Conseil de surveillance de la magistrature, le SDI aurait été incompétent pour collecter les données personnelles du requérant. Enfin, le Gouvernement aurait donné à cette affaire une ampleur médiatique orchestrée sans précédent, à coup de communiqués et de conférence de presse.

Par même acte de procédure du 16 mars 2010, le requérant demandait la récusation de l'un des membres de la CPD.

N. Par requête du 16 mars 2010, le requérant X. a également saisi la CPD, en demandant formellement à ce que celle-ci constate l'illicéité des procédés utilisés par les instances administratives cantonales pour aboutir à la sanction disciplinaire dont il a fait l'objet, fasse interdiction de tels traitements de données le concernant à l'avenir et ordonne la destruction de toutes les données recueillies de manière illicite et illégale.

Le requérant allègue, en substance, que le Gouvernement a ouvert une enquête disciplinaire à son encontre, le 3 mars 2009, en raison des informations fournies par le SDI à son sujet, alors qu'il était inspecteur principal adjoint à la Police cantonale. Par décision du 24 juin 2009, le Gouvernement a prononcé le déclassement du requérant qui a recouru contre cette décision auprès de la Cour administrative du Tribunal cantonal. Selon le requérant, le Gouvernement et l'administration auraient obtenu des preuves pour le dénoncer, l'accuser, puis le sanctionner de manière illégale. Ainsi en est-il en particulier de la surveillance et de l'enregistrement de ses données qui auraient été effectués par le SDI, notamment par télémaintenance.

Aux termes de sa requête, M. X. a également demandé la récusation de l'un des membres de la Commission.

O. Par arrêts des 27 mai et 5 juillet 2010, la Cour administrative du Tribunal cantonal a admis les demandes de récusation formulées par les trois requérants à l'encontre de l'un des membres de la CPD et a statué favorablement sur les demandes de déport présentées par le Président de la CPD et un troisième membre de la Commission, respectivement a désigné les remplaçants du Président et des membres de la CPD récusés.

P. Aux termes de son ordonnance du 27 juillet 2010, la CPD a ordonné, rière la Chancellerie du Tribunal cantonal, l'édition du dossier relatif au recours déposé par le requérant X. devant la Chambre administrative contre la décision du Gouvernement du 24 juin 2009 (Adm. 92/2009).

Figure dans le dossier de la Chambre administrative le rapport individuel de la Commission d'enquête disciplinaire au sujet du requérant. Le rapport en question mentionne, sous la rubrique « Etat de fait », les données suivantes : le résultat de l'analyse de novembre 2008, avec la mention : « effectuée sur l'IP 10.28.61.40 (identifié comme celui de X.) », permettant de mettre en évidence notamment le nombre de hits que celui-ci est présumé avoir effectué lors la période considérée ; le résultat de l'analyse du disque dur après copie du 5 mars 2009 permettant d'établir le nombre d'images et de vidéos pornographiques présentes sur le cache du navigateur web et celui des sites consultés ; l'audition du requérant ; l'analyse des plans de service de ce dernier.

Le rapport d'analyse forensique relatif à la machine du requérant, finalisé le 26 mars 2009, a également été produit dans le cadre de la procédure de recours. En sus du résultat de l'analyse de disque sous chiffre 3, le rapport d'analyse forensique versé au dossier de l'enquête disciplinaire reproduisait, sous chiffre 2 « réseau », les résultats des analyses du mois de novembre 2008 effectuées par SCRT avant la saisie du Gouvernement, tels qu'ils figuraient sous le chiffre 3 du rapport « Analyse trafic réseau » sous la forme de graphiques, tableaux et listes recensant le nombre de hits illicites et leur répartition horaire, les 50 sites les plus consultés, la correspondance d'un nombre de hits à telle heure d'une date donnée, ainsi que la fréquentation des 10 sites les plus consultés sur le mois.

Il a encore été versé par le Gouvernement au dossier de la procédure de recours de X. un complément au rapport d'analyse forensique, complément qui aurait été finalisé le 11 mai 2009. Celui-ci comprend les mêmes analyses que dans le rapport forensique principal, mais effectuées cette fois-ci uniquement pour l'utilisateur poc28. Sous chiffre 2 « réseau », il était mentionné que l'analyse principale n'aurait pas permis d'associer des consultations de sites à des utilisateurs, mais uniquement des consultations de sites à des ordinateurs (à des numéros IP).

Lors de l'audience de débats du 17 mars 2010, la Cour administrative a entendu M. A. du SDI qui a déclaré en substance que, suite à l'analyse faite par la société SCRT des

données sur le mois de novembre 2008, la liste d'adresses IP fournie par ladite société au SDI était assez large et il aurait fallu s'assurer que les éléments présentés étaient fiables, à savoir qu'ils ne contenaient pas de faux positifs. Il aurait donc fallu déployer des moyens conséquents en saisissant tous les disques durs. Une autre méthode consistait à s'assurer qu'il y avait effectivement certains éléments sur les ordinateurs. Ainsi, en vue d'affiner cette liste, le SDI devait prendre en main les ordinateurs susceptibles d'être problématiques pour permettre à SCRT d'exécuter un logiciel permettant d'effectuer des recherches sur les données techniques résiduelles des postes. Cette démarche aurait donc été faite pour éviter de saisir trop de disques durs et pour simplifier la suite de la procédure, c'est-à-dire pour éviter que quelqu'un ne soit finalement pas concerné. Lors de la prise en main, le SDI aurait invoqué auprès de l'utilisateur un problème d'accès à Internet. Quand un ordinateur est allumé, il y aurait deux manières de prendre celui-ci en main, soit en tapant le numéro d'inventaire, soit en tapant l'adresse IP. Concrètement, l'adresse IP permet de se connecter sur l'ordinateur et on a le nom de la personne qui est elle-même connectée au moment de la prise en main.

La Cour administrative a également entendu le directeur de la société SCRT. Celui-ci a déclaré, pour l'essentiel, que la prise en main aurait été faite sur la base du premier rapport de la société SCRT contenant une liste d'adresses IP. SCRT n'aurait pas initié la démarche de la prise en main, même si celle-ci lui a été utile. Il aurait été techniquement impossible de saisir tous les disques durs et de les analyser. En outre, une adresse IP peut changer. L'objectif de la prise en main aurait donc été de vérifier si les adresses IP identifiées au départ étaient toujours les mêmes et s'il y avait des traces.

En juin 2010, SCRT a encore répondu par écrit à des questions complémentaires de la Cour administrative. En particulier, SCRT considère, d'après sa connaissance de l'infrastructure informatique/réseau qui était en place à la date des faits, qu'il aurait été impossible de connaître les noms des utilisateurs ayant consulté des sites non professionnel sans avoir recours à l'analyse des machines concernées que cela soit fait via une prise en main à distance ou une saisie du disque. Sans accès aux machines concernées, il aurait été possible de connaître uniquement et dans le meilleur des cas l'adresse IP (susceptible de ne plus être exacte et d'avoir changée) des machines ayant consulté des sites non professionnels. Il aurait été toutefois impossible de s'assurer de l'utilisateur (particulièrement dans le cas des machines partagées par plusieurs utilisateurs) sans avoir accès au disque de la machine (prise en main à distance ou saisie du disque).

A l'occasion de nouvelles questions complémentaires de la Cour administrative, en juillet 2010, le représentant de SCRT a encore précisé qu'à son avis, il aurait été extrêmement difficile, voire impossible sans prise en main à distance préalable, de saisir et d'analyser d'une manière fiable les disques durs des 54 postes ressortant de

la liste des machines les plus impliquées qui résultait du premier contrôle, cela pour les raisons suivantes :

- L'existence d'un risque de saisir de mauvaises machines, notamment dans le cas de machines partagées par plusieurs utilisateurs ou des machines ayant changé d'adresse IP. Il aurait été ainsi souhaitable de limiter l'effet traumatisant de la saisie de disques en présence des forces de l'ordre en procédant à cette prise en main à distance.

- Il aurait été strictement impossible d'analyser 54 disques durs dans un délai raisonnable, chaque disque à analyser nécessitant plusieurs jours de travail.

- Le coût engendré par l'analyse de 54 disques durs, lié au facteur temps.

Il convient encore de relever que, dans le cadre de la procédure de recours, la société SCRT a produit son rapport « Analyse trafic réseau » sous forme numérique. Dans cette version, on constate que l'analyse des machines les plus impliquées, figurant sous chiffre 3 dudit rapport, a porté sur un nombre de 31 machines (ch. 3.3 à 3.33), au lieu des 17 figurant dans l'extrait de rapport contenu dans le dossier du Gouvernement remis à la CPD.

Q. En date du 22 février 2011, le Gouvernement a fourni à la CPD ses réponses aux requêtes de MM. Z., Y. et X. en concluant à leur rejet, sous réserve de leur recevabilité, le tout sous suite des frais et dépens.

En substance, le Gouvernement estime n'être pas habilité à se prononcer sur la requête de Y., les données le concernant ayant été fournies par le SDI au Conseil de surveillance de la magistrature qui était l'autorité disciplinaire compétente.

S'agissant de la requête de M. Z., le Gouvernement conteste l'existence d'un intérêt actuel digne de protection au constat d'une éventuelle illicéité et conclut à l'irrecevabilité de ladite requête. En outre, concernant le grief d'avoir divulgué des éléments de l'enquête disciplinaire, le Gouvernement le conteste également et souligne qu'il n'a diffusé aucune information permettant d'identifier le requérant, ni aucune autre personne concernée.

En ce qui concerne le processus suivi par le SDI avant l'ouverture des procédures disciplinaires, le Gouvernement invoque que le Président de la CPD, aux termes de son courrier du 30 janvier 2009, aurait émis des doutes uniquement sur un point particulier du processus en question, à savoir le chiffre 9 relatif à la prise en main à distance des postes, et qu'il aurait admis pour le surplus ledit processus, en particulier le fait que le SDI puisse établir et disposer d'une liste nominative des personnes concernées avant de saisir l'autorité disciplinaire. Le Gouvernement se réfère

également au rapport de la Commission d'enquête validant les investigations effectuées par le SDI.

Au demeurant, les procédures disciplinaires engagées contre les requérants auraient permis de procéder à la collecte des preuves de manière légale. La mesure disciplinaire concernant le requérant X. aurait été prise sur la base de ces preuves. En outre, une partie de la doctrine n'exclut les preuves obtenues de manière illégale que si elles n'auraient pas pu être collectées de manière légale. Partant, même dans l'hypothèse où le traitement des données par le SDI devait être illicite, les données auraient été recueillies de manière incontestablement légale par la copie de nombreux disques durs.

Par même acte de procédure, le Gouvernement requérait la jonction des procédures introduites par les requérants, ainsi que l'appel en cause du Conseil de surveillance de la magistrature.

Pour sa part, le SDI n'a pas répondu aux requêtes dans le délai qui lui était imparti par la CPD.

R. En date du 5 avril 2011, le Gouvernement a fourni à la CPD les deux communiqués de presse qui ont été diffusés, l'un le 6 mars 2009, l'autre le 29 juin 2009, au sujet de l'affaire de la consultation de sites Internet par les membres de la fonction publique cantonale. La CPD reviendra, ci-dessous, sur le contenu de ces deux communiqués.

S. En date du 7 avril 2011, il a été versé au dossier le rapport du 5 novembre 2009 du Tribunal cantonal à l'attention du Gouvernement concernant la surveillance informatique au sein des autorités judiciaires.

Le rapport précité relève que la surveillance administrative des autorités judiciaires serait dévolue au Tribunal cantonal. La surveillance disciplinaire serait, quant à elle, exercée par le Conseil de surveillance de la magistrature. Ainsi, le contrôle de l'utilisation d'Internet par le personnel judiciaire serait de la compétence du Tribunal cantonal. Lorsque la surveillance concerne des comportements imputés à des personnes déterminées, elle incomberait au Conseil de surveillance de la magistrature, si ces personnes ont le statut de magistrat de l'ordre judiciaire.

Ainsi, dès le moment où il a été découvert que des sites pornographiques étaient consultés au sein de l'administration judiciaire, le Tribunal cantonal, en sa qualité d'autorité de surveillance administrative, aurait dû être averti. En particulier, il aurait appartenu à celui-ci d'autoriser l'extension de la surveillance administrative sur les postes de l'administration judiciaire pour la période de novembre 2008. Par ailleurs, le mandat pour effectuer l'analyse des fichiers du journal d'accès à Internet n'aurait pu être confié à la société SCRT sans l'aval du Conseil de surveillance de la magistrature, en tant que la finalité de cette analyse pouvait permettre d'associer les adresses IP

mises en cause à des numéros d'inventaire de postes informatiques de magistrats et, finalement, après prise en main à distance de ces postes, d'identifier des magistrats déterminés.

Le Tribunal cantonal retient donc que tous les actes effectués dans le cadre de cette analyse jusqu'à l'établissement d'une liste nominative des magistrats mis en cause, ainsi que le rapport remis au Conseil de surveillance de la magistrature, constitueraient des actes d'enquête disciplinaire qui ont été effectués sans consultation de l'autorité compétente pour les ordonner, étant rappelé que les procédures disciplinaires dirigées contre les deux magistrats en question n'ont été ouvertes que le 27 février 2009. Il en découlerait que le principe de l'indépendance de la Justice n'aurait pas été respecté.

T. Par courrier du 20 avril 2011 de son mandataire, le requérant X. a adressé à la CPD sa détermination sur la réponse du Gouvernement. En substance, le requérant confirme que l'administration et le Gouvernement auraient obtenu des preuves pour l'accuser, le dénoncer et le sanctionner de manière illégale, en particulier en ce qui concerne la surveillance et l'enregistrement par télémaintenance exécutés par le SDI. Le requérant relève en outre que le Gouvernement aurait été au courant de la situation bien avant sa saisie formelle du 19 février 2009 par le SDI. La prise en main par télémaintenance de l'ordinateur du requérant décrite par le SDI dans son courrier du 30 janvier 2009 aurait contrevenu à l'avis formulé par le Président de la CPD. Lors de ladite prise en main, le requérant aurait été trompé par le SDI, ce dernier ayant simplement invoqué un problème d'accès à Internet, sans annoncer l'ouverture d'une enquête. Le Chef du Service juridique a également retenu que les directives de 2001 soulevaient des risques quant à la validité de la collecte de données sans avertissement individualisé aux collaborateurs et préalable au contrôle. Pour le requérant, la mise en œuvre du processus de surveillance aurait été décidée sans que les organes compétents n'aient été avisés ni consultés. Selon les directives du Préposé fédéral à la protection des données, il appartiendrait à l'employeur d'informer le travailleur immédiatement en cas de constat d'abus ou d'utilisation abusive d'une installation. Il serait donc contraire au devoir de loyauté et de diligence incombant à l'employeur de ne pas informer le fonctionnaire et de le laisser ainsi poursuivre ses consultations sur des sites, puis par la suite de le sanctionner.

Par courrier du 2 mai 2011, le requérant Y. s'est également prononcé sur la réponse du Gouvernement, en rappelant, notamment, que le litige ne portait pas sur la procédure disciplinaire proprement dite, mais sur toute la phase antérieure à l'ouverture de cette procédure, soit sur la légalité de la surveillance instaurée et des méthodes utilisées pour l'identifier, en particulier la prise en main à distance des postes informatiques par le SDI. Or, le service en question n'aurait pas eu la compétence, par plus que le Gouvernement dont il dépend, de décider de surveiller l'ordinateur du requérant. En outre, la prise en main sous un faux prétexte serait illicite.

Par courrier du 5 mai 2011 de son mandataire, le requérant Z. a également adressé à la CPD sa détermination sur la réponse du Gouvernement. Notamment, il ressortirait du dossier que les démarches effectuées par l'administration cantonale, sous la responsabilité du Gouvernement, pour pénétrer dans les systèmes informatiques de certains fonctionnaires aurait été illicites. En particulier, la prise en main faite par le SDI sans avertissement individualisé aux collaborateurs et préalable aux contrôles ne serait pas autorisée par la loi. Le requérant relève par ailleurs que, dans les éditions de plusieurs journaux, notamment celle du « Matin » du 12 mars 2009, toute l'affaire aurait été dévoilée et la photographie du requérant, de même que celles des deux magistrats impliqués, figuraient en tête de page. Selon le requérant, ces médias n'auraient évidemment pas pu citer les trois noms en question sans avoir obtenu des indications précises à ce sujet. En outre, lors de la séance du Bureau du Parlement du 19 mars 2009, le Président du Parlement a officiellement fait part de l'enquête ouverte contre M. Z. L'ancien Président du Parlement aurait été également au courant des faits en novembre 2008 déjà, de même que certains Chefs de Service.

U. Par décision du 12 mai 2011, le Président a.h. de la CPD a rejeté la demande d'appel en cause du Conseil de la magistrature formulée par le Gouvernement.

V. Par décision du 13 mai 2011, le Président a.h. de la CPD a ordonné la jonction des trois procédures introduites sur requêtes devant la CPD et de la procédure ouverte d'office en 2009.

W. Lors de ses remarques finales du 31 mai 2011, le Gouvernement a rappelé n'avoir été saisi du dossier qu'en février 2009 et n'avoir pas lui-même ordonné, au travers du SDI, une surveillance informatique des ordinateurs professionnels des requérants. Antérieurement, le SDI ne lui aurait pas soumis de dossier, ni le processus qu'il entendait suivre ou le mandat qu'il a confié à SCRT.

Le Gouvernement revient sur la détermination du Président de la CPD du 30 janvier 2009 qui aurait admis la détention par le SDI d'une liste nominative des agents publics impliqués avant la saisie de l'autorité disciplinaire. Dans tous les cas, même à admettre par hypothèse que le processus suivi par le SDI aurait été illicite, cela ne signifierait pas encore que le traitement ultérieur des données par le Gouvernement l'était.

En ce qui concerne les articles parus dans la presse au sujet des requérants Y. et Z., le Gouvernement relève que l'ensemble de ses communications ont été totalement anonymes. Partant, les requérants imputeraient au Gouvernement un état de fait qui peut être issu d'une violation du secret par une personne totalement indépendante de celui-ci.

X. Par lettres des 1er, 6 et 30 juin 2011, les requérants Y., X. et Z. ont informé la CPD qu'ils confirmaient leur courriers et prises de position antérieurs et renonçaient à formuler des remarques supplémentaires.

Y. Par courrier du 30 juin 2011, le SDI a adressé une prise de position finale, en concluant au rejet des requêtes, sous réserve de leur recevabilité. La prise de position du SDI était accompagnée de 4 pièces justificatives.

En substance, le SDI se réfère à l'article 146 lit. a DOGA qui lui confère le mandat légal de la responsabilité du traitement électronique de l'information. A ce titre, le SDI serait responsable de l'intégrité du système informatique de l'Etat, notamment sous l'angle de la sécurité. De plus, le réseau informatique est commun pour l'administration centrale et la justice. L'activité du SDI antérieurement à la saisie des autorités disciplinaires se serait limitée à la recherche de la cause des dysfonctionnements constatés et non à des mesures de surveillance individuelle. Les premières analyses faites avec les moyens limités de l'époque n'auraient pas permis d'identifier précisément les personnes concernées. Le SDI aurait été limité au simple réseau des Services (adresse IP). En effet, l'attribution d'une adresse IP via le serveur DHCP serait faite de façon dynamique. De plus, le SDI n'aurait pas eu les moyens techniques pour analyser l'historique de ce système. Il aurait donc été impossible de s'assurer de l'attribution de l'IP concernée à un poste précis au moment des faits. C'est la raison pour laquelle le SDI aurait été obligé de faire appel à une société de services externe. En sus, lors de la lecture des résultats, M. A. aurait relevé que certains des noms de sites à connotation pornographique mentionnés semblaient faire allusion à des sites pénalement répréhensibles. Il aurait ainsi pris contact avec M. C., Officier au sein de la Police judiciaire en charge de la répression de la cybercriminalité, afin d'obtenir conseil et d'établir si, pour ces sites, il y avait lieu de penser qu'ils hébergeaient du contenu pédopornographique. M. C. lui aurait répondu en confirmant qu'un certain nombre de ces sites était effectivement susceptible d'héberger ce type de contenu, en plus de pornographie dite « classique ». En parallèle, M. A. se serait renseigné de manière informelle auprès de l'Office central de la Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC) pour plus de précisions sur la marche à suivre. Les réponses qui lui auraient été données l'auraient incité à aller de l'avant et de mandater une société tierce pour la poursuite du dossier.

La société SCRT a fourni un premier rapport du 19 décembre 2008 exclusivement basé sur les journaux de trafic réseau du « proxy » Internet. Ce rapport mentionne au point 3.1 le nombre de hits illicites par machines. Vu le nombre élevé de hits, il était insoutenable de ne donner aucune suite à une telle information. Une liste anonyme de 56 adresses IP a été relevée lors de l'étude des journaux. Cette liste aurait procuré une liste de lieux, mais non une liste des postes de travail. Selon le chiffre 5 du courrier du 30 janvier 2009 du Président de la CPD, le SDI aurait pu dresser une liste nominative destinée à l'autorité disciplinaire, cela afin d'accomplir correctement ses tâches légales. Ainsi, il aurait appartenu au SDI de retrouver l'information permettant de relier de manière fiable et exhaustive les adresses IP mentionnées à des numéros de postes de travail.

Le SDI aurait alors continué les recherches par le biais de la gestion d'inventaire des postes de travail. Le SDI consigne en effet des informations relatives à l'ensemble de son parc informatique dans un logiciel. Les extractions effectuées au moyens des systèmes « Invmat » et « PS'Soft » auraient permis de fournir bien plus de détails que lors de la tentative précédente auprès du serveur DHCP. Malheureusement, certaines informations au sein des deux bases auraient été contradictoires, voire fausses. Le SDI n'aurait dès lors pas eu d'autre choix que d'aller vérifier, pour chaque poste référencé par son adresse IP, que les informations obtenues par l'analyse des journaux réseau « proxy Internet » correspondaient effectivement aux adresses IP concernées. L'objectif de cette vérification aurait donc été de confirmer que les adresses IP relevées par SCRT via l'analyse réseau correspondaient bien à des postes de travail identifiables et qui pourraient par la suite faire l'objet d'une saisie éventuelle, tout en veillant dans le même temps à ce qu'aucune erreur ne puisse être commise et qu'un poste de travail non concerné soit exclu. En effet, les aléas d'identification liés au mode de fonctionnement du serveur DHCP en place à ce moment, ainsi que les incohérences d'inventaire liées à la migration, alors en cours, de l'outil d'inventaire des postes, auraient appelé une confirmation. La saisie à tort de postes non concernés par l'affaire aurait été traumatisante pour leurs usagers, et le SDI, dans un esprit de respect et d'éthique, aurait souhaité limiter au maximum ces effets, en ne poursuivant la démarche que sur les postes réellement concernés. La nature précise de la démarche ne pouvait être divulguée. En effet, d'une part, il aurait pu s'agir de postes partagés et une telle information aurait donc consisté à apprendre à un tiers non concerné la présence de traces d'accès à des sites pornographiques. En second lieu, il y aurait eu un taux d'erreur et des risques que certaines des adresses IP suspectées n'aient plus de traces correctement exploitables, à cause de l'écoulement du temps (les ordinateurs pouvant effacer eux-mêmes des traces anciennes en fonction de leurs besoins en espace sur le disque dur). Dès lors, il aurait été hasardeux d'annoncer oralement aux personnes ayant permis l'accès au poste que la recherche portait sur la présence de traces d'accès à des sites pornographiques, dès lors que ces traces pouvaient ne plus être exploitées ou se révéler infondées. Enfin, dans le cas où la personne contactée au téléphone aurait été effectivement l'auteur de ces accès à des sites pornographiques, le fait de lui annoncer qu'une vérification sur la présence de sites pornographiques allait être réalisée à distance aurait permis à celle-ci d'agir de différentes manières simples et à la portée de quiconque pour altérer ou supprimer les traces de manière définitive.

S'agissant du processus exposé lors de l'entretien téléphonique du 29 janvier 2009 entre le Président de la CPD et M. A., l'ensemble des points décrits dans la procédure de contrôle des accès à Internet auraient été expliqués et validés un à un par les deux interlocuteurs. Concernant la prise en main à distance des postes visés, à aucun moment il n'aurait été clairement signifié à M. A. que cette méthode ne pouvait pas être utilisée. En outre, la lettre de validation du Président qui a suivi le lendemain, notamment la phrase « De manière générale, le protocole de l'opération m'apparaît conforme aux directives et aux processus préconisés par la doctrine », ne pouvait

raisonnablement être interprétée comme une désapprobation de la méthode, y compris la détention d'une liste nominative avant l'ouverture de procédures disciplinaires. En outre, le SDI se réfère à l'avis de la Commission d'enquête présidée par le Juge fédéral Baechler, confirmant la licéité du processus suivi. Le traitement du dossier se serait ainsi fait dans le respect des dispositions légales et notamment des directives gouvernementales applicables en la matière (Directives du 13 mars 2001 aux magistrats, fonctionnaires et employé-e-s de la République et canton du Jura, concernant les modalités d'utilisation d'Internet) qui ont été agréées par la CPD.

<u>En droit</u> :

1. En vertu de l'article 50 al. 2 lit a LPD, la CPD s'assure d'office que les dispositions légales et réglementaires concernant le traitement des données à caractère personnel sont observées. Elle est saisie sur demande des personnes concernées ou du responsable du fichier. Elle agit également d'office (art. 51 LPD).

L'article 36 al. 1 LPD dispose que toute personne concernée par un traitement de données à caractère personnel, qui estime que le traitement porte atteinte de manière illicite à ses intérêts, peut intervenir auprès de l'autorité de surveillance pour faire interdire le traitement (lit. a), faire cesser le traitement et faire détruire les données déjà recueillies (lit. b), ou encore faire constater l'illicéité du traitement (lit. c).

La recevabilité de la requête de Z. en constatation du traitement illicite de ses données est contestée par le Gouvernement, celui-ci estimant que le requérant ne peut se prévaloir d'un intérêt encore actuel à un tel constat.

Il est exact qu'aux termes de sa jurisprudence (RJJ 1996, p. 305), la CPD fait dépendre la recevabilité d'une action en constatation, au sens de l'article 36 al. 1 lit. c LPD, de l'existence d'un intérêt digne de protection que le requérant doit prouver (art. 92 al. 2 CPA) et qui doit, en principe, être actuel et concret.

En l'espèce, lors de son audition du 2 mars 2010, le Chef du SDI a indiqué à la CPD que les données collectées préalablement à la saisie des disques durs, en particulier celles obtenues au moyen de la prise en main à distance des postes informatiques des collaborateurs concernés, étaient conservées par le SDI, respectivement par M. A.. Celles obtenues par l'analyse des fichiers journaux du mois de novembre 2008 ont été reproduites dans les rapports forensiques. Or, dans la mesure l'article 2 al. 4 LPD assimile la conservation de données à caractère personnel à un traitement de données, force est de constater que le requérant Z., ainsi d'ailleurs que le requérant Y., disposent encore d'un intérêt actuel à faire constater l'éventuelle illicéité de ce traitement, toujours en cours, de données qui les concerneraient.

En sus et d'une façon générale, pour qu'un intérêt digne de protection soit retenu en procédure administrative, il ne doit pas nécessairement affecter la situation juridique du

requérant. Il peut s'agir aussi d'intérêts de fait, par exemple économiques, ou d'intérêts de nature esthétique, idéale ou morale (G. BOINAY, La procédure administrative et constitutionnelle du canton du Jura, art. 120 N 9). En l'espèce, vu la couverture médiatique qui a entouré l'affaire dite du « pornogate », née de la surveillance informatique des ordinateurs des collaborateurs de l'Etat et des magistrats, couverture médiatique dont les effets perdurent encore à ce jour, l'on devrait de toute manière reconnaître aux requérants un intérêt, à tout le moins idéal mais encore actuel, à faire constater le caractère éventuellement illicite de la surveillance dont ils ont fait l'objet et qui est à l'origine de l'affaire qui les a concernés.

Enfin, une procédure d'office a été ouverte par la CPD, conformément aux articles 50 et 51 al. 2 LPD, en vue de contrôler la validité de la collecte de données effectuée par le SDI dans le cadre de la surveillance informatique des membres de la fonction publique. Cette procédure a été jointe à celles introduites sur requêtes. Il s'ensuit que la CPD serait de toute manière habilitée à examiner les griefs des requérants dans le cadre de son pouvoir de surveillance d'office.

Pour le surplus, l'intérêt actuel de X., actuellement en procédure de recours auprès de la Cour administrative, à requérir le constat du traitement illicite de données dont il aurait fait l'objet, respectivement l'interdiction à l'avenir d'un tel traitement et la destruction de données recueillies éventuellement de manière illicite, au sens de la LPD, est manifeste et n'est pas contesté.

Les requêtes sont donc recevables et il convient d'entrer en matière. Comme exposé ci-dessus, il appartiendra également à la CPD d'examiner d'office, d'une façon générale et au-delà des cas particuliers des requérants, la licéité des traitements de données intervenus lors de la surveillance de la navigation Internet des membres de la fonction publique.

2. Selon l'article 5 LPD, consacrant le principe de la légalité, des données personnelles peuvent être traitées si une base légale matérielle le prévoit ou si le traitement sert à l'accomplissement d'une tâche légale. Les données sensibles ne peuvent être traitées que si une base légale formelle le prévoit ou si l'accomplissement d'une tâche légale l'exige absolument (art. 5 al. 2 lit. a LPD) ou encore si la personne concernée a donné expressément son accord (art. 5 al. 2 lit. b LPD).

A l'instar des normes spécifiques de la Loi fédérale sur la protection des données (ci-après LFPD) au sujet des traitements de données effectués par les organes fédéraux, la LPD cantonale conditionne ainsi tout traitement de données effectué par les organes de l'Etat au respect du principe de la légalité, cela dans un but de prévisibilité et de transparence de l'activité étatique, d'égalité dans l'application de la loi et de respect des exigences de l'article 36 Cst. féd., respectivement de celles de l'article 13 CJU, puisqu'il en va d'une atteinte au droit fondamental à l'autodétermination en matière

informationnelle tiré de l'article 13 Cst. féd. (P. MEIER, Protection des données, Fondements, principes généraux et droit privé, Berne 2011, p. 146 et réf. citées).

Il convient dès lors d'examiner en premier lieu si, dans le cadre de la surveillance informatique des connexions Internet des collaborateurs de l'Etat, respectivement de magistrats, le SDI a traité des données personnelles, la nature de ces données, et si un tel traitement était conforme au principe de la légalité tel que défini par l'article 5 LPD.

2.1 En vertu de l'article 2 al. 1 LPD, les données à caractère personnel sont toutes les informations qui se rapportent à une personne identifiée ou identifiable. Selon l'article 2 al. 2 lit. a et h LPD, les données sensibles sont toutes les informations relatives, notamment, à la sphère intime et aux modes de comportement. L'article 2 al. 4 LPD précise quant à lui que le traitement des données à caractère personnel consiste en toute opération portant sur de telles données, notamment la collecte, la conservation, l'utilisation, la modification, la communication et la destruction.

2.1.1 Il résulte de la définition ci-dessus que doit être considérée comme une donnée personnelle toute information, dès lors que celle-ci peut être mise en rapport avec une personne identifiée ou identifiable. La notion est large : hormis les pures données matérielles, presque toutes les données peuvent être mises en relation avec une personne et devenir des données au sens de la loi (D. ROSENTHAL, Handkommentar DSG, art. 3 N 14 ; P. MEIER, op. cit., p. 197). Les données peuvent être des données objectives (une expérience professionnelle, une maladie, une condamnation pénale, une habitude de consommation) ou des données subjectives (un jugement de valeur, par ex. l'appréciation portée sur un travailleur, un pronostic de guérison, l'évaluation de la solidité financière d'un emprunteur ; P. MEIER, op. cit., p. 198 et réf. citées). Le caractère exact ou non de l'information n'est pas un critère de la définition, dans la mesure où la loi envisage expressément que la donnée soit inexacte, en en permettant la rectification (art. 37 LPD ; D. ROSENTHAL, Handkommentar DSG, art. 3 n 8 ; P. Meier, op. cit., p. 198). Il n'est pas nécessaire que les données soient intégrées, ou destinées à être intégrées, à un fichier ou à une banque de données, ni qu'elles soient classées de manière logique ; seules certaines dispositions spécifiques de la loi sont applicables aux fichiers comme tels (28 ss LPD ; P. MEIER, op. cit., p. 198 et réf. citées). La forme des données est indifférente (ATF 125 II 473 = JT 2001 I 324, consid. 4b ; ATAF 2009/44, consid. 1.2.1 ; P. MEIER, op. cit., p. 198s et réf. citées) : la donnée peut être constituée de caractères alphabétiques, d'une image photographique ou audiovisuelle (image d'une webcam ou d'une caméra de surveillance), d'un son, d'un chiffre ou d'un signe (analogique, digital, numérique ou alphanumérique), d'un dessin ou d'une autre représentation graphique, d'une odeur, d'une suite ou d'une combinaison de tels éléments (photographie avec légendes, numéro de téléphone, adresse électronique, bande vidéo avec enregistrement sonore et sous-titres, etc.), de caractéristiques biométriques (par ex. empreinte digitale) ou biologiques (par ex. prélèvement sanguin) ; le type de support ne joue pas de rôle non plus (papier, film,

support optique, audio ou numérique : CD-rom, clé USB, etc.). Il importe peu notamment que l'information soit immédiatement perceptible (photographie) ou nécessite au contraire la mise en œuvre d'un outillage technique (insertion d'un CD-rom dans un ordinateur ; lecture du gabarit d'empreintes digitales).

Pour qu'elle soit soumise à la LPD, une donnée doit pouvoir être mise en rapport avec une personne identifiée ou identifiable. Une personne (physique ou morale) est identifiable lorsque, par corrélation indirecte d'informations tirées des circonstances ou du contexte (notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique culturelle ou sociale), il est possible de l'identifier avec les moyens technologiques disponibles (Arrêt du TAF A-3144/2008 du 27 mai 2009, consid. 2.2.1 ; P. Meier, op. cit., p. 202). Il y a identification même si les données se rapportent à plusieurs personnes possibles au sein d'un groupe restreint (D. ROSENTHAL, Handkommentar DSG, Art. 3 N 33 ; P. Meier, op. cit., p. 203). L'anonymisation des données peut empêcher l'identification ou la ré-identification. Dans un tel cas, la donnée échappe à la LPD (P. MEIER, op. cit., p. 202ss et réf. citées). L'estimation du degré d'anonymisation requis dépend d'abord des connaissances complémentaires que le détenteur ou le destinataire des informations possède ou peut acquérir relativement aisément. Si la ré-identification est possible par l'ajout de telles connaissances complémentaires ou la comparaison avec d'autres données provenant d'autres sources, on ne parlera plus de données anonymisées. L'appréciation se fera ensuite par rapport à l'importance (en technologie, en temps, en coût, en personnel) des moyens à mettre en œuvre pour être en mesure de ré-attribuer les données à une personne déterminée. Les moyens de recherche faciles et efficaces que l'on trouve dans les suites bureautiques ou sur Internet doivent naturellement être pris en compte, en plus des moyens particuliers dont peut disposer l'intéressé (par ex. banque de données interne permettant de procéder à des recoupements ; Arrêt du TAF A-3144/2008 du 27 mai 2009, consid. 2.2.1 ; P. MEIER, op. cit, p. 204s et réf. citées). Entreront également en ligne de compte la durée de la conservation : plus elle sera brève avant la destruction irréversible des données, plus le risque ou la possibilité d'identification seront faibles. On tiendra compte également de l'intérêt propre de celui ou de celle qui pourrait chercher à ré-identifier la personne (D. ROSENTHAL, Handkommentar DSG, Art. 3 N 25 ; P. MEIER, op. cit., p. 205). Cet intérêt influe en effet directement sur la volonté de mettre en œuvre les moyens requis pour la ré-identification. C'est par conséquent la théorie relative de la ré-identification que l'on appliquera : seules les connaissances, moyens et possibilités, ainsi que l'intérêt propre de l'auteur (potentiel) du traitement doivent être pris en compte pour déterminer si la ré-identification doit être envisagée (P. MEIER, op. cit., p. 206 et réf. citées).
S'agissant d'une adresse IP (numéro d'interface avec le réseau d'un matériel informatique connecté à un réseau d'information utilisant l'Internet Protocol, en particulier le numéro de l'ordinateur relié à Internet), la jurisprudence suisse admet en l'état que les adresses IP doivent être considérées comme des données personnelles, cela qu'elles soient statiques (fixes) ou dynamiques, en raison de la possibilité

technique de ré-identification (arrêt A-3144/2008 du TFA du 27 mai 2009, confirmé sur ce point par l'arrêt du TF 1C_285/2009 du 8 septembre 2010 publié au RO 136 II 508). La question demeure toutefois discutée en doctrine, s'agissant des adresses dites dynamiques, une partie de celle-ci refusant de qualifier systématiquement ces données connexes à la communication électronique de données personnelles (P. MEIER, op. cit., p. 208ss et réf. citées). Selon ces auteurs, si le fournisseur d'accès, qui a attribué l'adresse, peut être identifié aisément, il n'en va pas de même de l'ordinateur à qui l'adresse dynamique a été attribuée pour le court laps de temps d'une navigation. Pour l'exploitant du site Internet visité, l'adresse IP ne permet donc pas l'identification et ne constitue pas une donnée personnelle si elle n'est pas accompagnée d'autres indications (par ex. des données identifiantes dans l'ouverture d'un compte utilisateur sur le site, ou un cookie permettant d'identifier un utilisateur par son ordinateur, malgré le changement d'adresse IP à chaque nouvelle session). L'identification est en revanche possible pour le fournisseur d'accès lui-même (ne serait-ce que pour des raisons de facturation), ainsi que pour les autorités, mais seulement en relation avec une enquête policière ou une procédure judiciaire.

En résumé, la doctrine retient que, dans l'hypothèse où un tiers n'est pas en mesure, hors enquête policière ou judiciaire, d'identifier le titulaire de l'adresse IP dynamique et que par ailleurs cette identification est complexe, la théorie relative paraît faire obstacle à qualifier une adresse IP dynamique comme telle de donnée personnelle (D. ROSENTHAL, Handkommentar DSG, Art. 3 N 27 ; P. MEIER, op. cit., p. 210). En revanche, à partir du moment où il est possible, par l'utilisation d'autres éléments, de faire un lien avec un usager déterminé, l'adresse devient identifiante (P. MEIER, op. cit., p. 211).

En l'espèce, il résulte des éléments versés au dossier, notamment le rapport « Analyse trafic réseau » de la société SCRT, tel qu'il a été produit auprès de la Cour administrative dans le cadre de la procédure de recours de X., qu'à fin 2008, en présence d'indices de navigation Internet sur des sites à caractère pornographique, le SDI a décidé de procéder à l'analyse des fichiers journaux du mois de novembre 2008 des collaborateurs de la fonction publique jurassienne. Il a mandaté l'entreprise spécialisée SCRT à cette fin. Le but déclaré de l'analyse était de déterminer les machines d'où provenaient les flux, la teneur de ces flux et le volume échangé. Cette première phase a permis d'identifier notamment les adresses IP de 56 postes informatiques de collaborateurs ayant fait plus de cent appels vers un site contenant des mots clés à connotation sexuelle et le nombre de hits effectués. Pour 31 postes informatiques, les informations collectées ont également porté sur le recensement des sites les plus consultés, la répartition horaire des consultations sur le mois, le nombre de hits à une heure d'une date donnée, classé par jour (Rapport SCRT « Analyse réseau », p. 7ss, ch. 3 « Résultats »).

En vue de vérifier l'exactitude des informations déjà récoltées au moyen de l'analyse des fichiers journaux, d'obtenir les preuves des consultations illicites (Rapport SCRT

« Analyse trafic réseau », p. 99ss, Tableau du ch. 4), d'écarter certains postes dont l'implication pouvait provenir de doublons et de déterminer l'utilisateur impliqué dans les cas où le poste informatique était partagé, le SDI et SCRT ont, par la suite, contrôlé les fichiers « index.dat » situés sur le disque C: des postes informatiques des membres de la fonction publique et l'historique Internet Explorer de ceux-ci pour déterminer s'ils contenaient des traces d'accès à des sites problématiques (Courrier du 29 janvier 2009 de M. A., p. 2, ch. 10 et Rapport SCRT « Analyse trafic réseau », p. 99). A cette fin, le SDI a pris contact par téléphone avec la personne connectée sur le poste à contrôler et lui a demandé l'autorisation de prendre le poste en question en télémaintenance, sans pour autant expliquer la nature exacte de cette opération (Courrier du 29 janvier 2009 de M. A., p. 2, ch. 9). Les informations collectées à distance au moyen de cette prise en main ont été sauvegardées et analysées. Au moyen de cette analyse, le SDI et SCRT ont établi une liste de 29 machines, à nouveau référencées au moyen de leurs adresses IP, dont il était prouvé qu'elles présentaient des traces d'accès à des sites pornographiques (Rapport SCRT « Analyse trafic réseau », p. 99ss, tableau du ch. 4).

Au vu des principes doctrinaux et jurisprudentiels rappelés ci-dessus, les collectes et les analyses effectuées par le SDI ou par SCRT sur mandat du SDI, lors des deux phases susmentionnées, doivent bien être considérées comme un traitement de données personnelles, cela même avant l'établissement d'une liste nominative.

En effet, déjà au stade de la phase d'analyse des fichiers journaux, le fait de recenser les postes informatiques de membres de la fonction publique, désignés par leurs adresses IP, ayant effectué des consultations de sites pornographiques, avec les horaires de connexion, les noms des sites les plus consultés, etc., revient à collecter des informations pouvant être mises en rapport avec des personnes, conformément à la jurisprudence du Tribunal fédéral et du Tribunal administratif fédéral citée ci-dessus au sujet des adresses IP, que celles-ci soient statiques ou dynamiques.

Certes, ladite jurisprudence fait l'objet de critiques en doctrine en ce qui concerne les adresses IP dynamiques. Cependant, à l'examen du Tableau figurant sous ch. 4 du rapport SCRT « Analyse trafic réseau », page 99ss, on constate que l'ensemble des adresses IP au 15 janvier 2009 des 33 postes informatiques contrôlés au moyen de la prise en main à distance étaient strictement les mêmes que celles obtenues lors des analyses des journaux du mois de novembre 2008, désignées par la mention « IP initiale », de telle sorte que l'éventualité et la fréquence du changement des adresses IP des postes de travail des collaborateurs du canton, mise en exergue par le SDI et SCRT lors de leurs auditions et prises de positions, semblent avoir été fortement exagérées.

En outre, le fait que certains postes informatiques, identifiés au moyen de leurs adresses IP, étaient partagés par plusieurs utilisateurs, voire qu'une adresse IP d'origine ait pu, dans certains cas, correspondre à plusieurs machines (rapport SCRT « Analyse trafic réseau », p. 99), n'implique pas que les informations collectées ne

puissent pas être tenues pour des données personnelles, dans la mesure où la doctrine précitée considère qu'il y a identification même si les données se rapportent à plusieurs personnes possibles au sein d'un groupe restreint. De plus, étant donné que l'analyse des fichiers journaux effectuée par le SDI ou SCRT a permis d'établir les dates et heures des connexions aux sites problématiques, il était donc possible par la suite, au moyen des plans horaires de travail des collaborateurs, de retrouver parmi l'éventuelle pluralité d'utilisateurs celui impliqué dans la consultation de sites pornographiques. Enfin, il convient de relever que la question des postes de travail partagés, de même que les remplacements de certains postes ou des postes itinérants, ne s'est posée que dans un certain nombre de cas (Courrier du 29 janvier 2009 de M. A., p. 2, ch. 8). Pour les autres, notamment lorsque les collaborateurs disposaient d'un ordinateur personnel dont ils étaient les seuls utilisateurs, l'adresse IP était manifestement identifiante. On pense en particulier aux deux magistrats ayant fait l'objet de la surveillance, dont le requérant Y., ainsi que le Secrétaire du Parlement, à savoir le requérant Z.

On mettra encore en évidence certaines mentions des responsables du SDI et de SCRT figurant au dossier. Ainsi, aux termes de son courrier du 29 janvier 2009, p. 2, ch. 7, M. A. relevait que les adresses IP associées aux noms des sites permettaient au mandataire (SCRT) et au SDI de retrouver les noms des services et plus précisément l'identifiant (numéro d'inventaire) pour grande partie des postes informatiques ayant servi à commettre ces abus. Aux termes de son rapport « Analyse trafic réseau », p. 99, ch. 4 « Utilisateurs potentiels des machines », SCRT déclarait que, pour les machines les plus incriminées, des suppositions avaient été faites quant à l'utilisateur de ladite machine lors de la première phase de l'enquête. Toujours à la p. 99 de son rapport, SCRT mentionnait également que, sur la base de l'état au 7 janvier 2009, soit après l'analyse des fichiers journaux, l'association entre la machine et l'utilisateur avait pu être réalisée pour un certain nombre de cas.

En tout état de cause, le déroulement des faits atteste que les utilisateurs ayant consultés des sites pornographiques ont pu être identifiés par le SDI, puisque ce dernier a finalement fourni une liste nominative au Gouvernement en février 2009. Il a donc été possible, sur la base des adresses IP et par l'utilisation d'autres éléments ou bases de données, de faire un lien avec un usager déterminé, de telle sorte que lesdites adresses recensées lors de l'analyse des fichiers journaux doivent être considérées comme identifiantes au cas particulier, conformément à la jurisprudence et à la doctrine précitée.

Enfin, le fait que des erreurs, doublons ou faux positifs soient apparus dans certains cas est irrelevant, dans la mesure où, comme cela a été rappelé ci-dessus, une information mise en rapport avec une personne est tenue pour une donnée personnelle quand bien même ladite information serait fausse. Dans le même sens, il n'est pas pertinent de savoir si la donnée collectée pouvait être sans autre utilisée comme moyen de preuve dans le cadre d'une procédure ou si celle-ci devait faire l'objet d'une

vérification ou d'une confirmation pour acquérir force probante en justice ou dans le cadre d'une procédure disciplinaire. La définition d'une donnée personnelle n'est pas limitée aux informations destinées à servir de moyens de preuve.

En ce qui concerne les données obtenues au moyen de la prise en main à distance, dans la mesure où une telle prise en main nécessitait que le SDI prenne contact par téléphone avec l'utilisateur du poste informatique pour que celui-ci accède à la demande de télémaintenance, il va de soi que les données collectées à cette occasion pouvaient être mises en relation avec une personne déterminée ou déterminable. De plus, il convient de relever que les fichiers « index.dat » ne sont pas seulement des fichiers de gestion technique, mais qu'ils contiennent une partie de l'historique de l'utilisateur et sont bien à ce titre des informations représentant des données personnelles.

Il s'ensuit que toutes les informations mises en rapport avec les adresses IP des postes informatiques des membres de la fonction publique du canton, collectées lors de l'analyse des fichiers journaux et de la prise en main à distance par le SDI ou SCRT sur mandat du SDI, doivent être tenues pour des données personnelles avant même l'établissement d'une liste nominative.

2.1.2 En vertu de l'article 2 al. 2 litt. a LPD, sont des données sensibles celles qui relèvent de la sphère intime. Hormis les données relatives à la santé, on songe essentiellement aux préférences et activités sexuelles (P. MEIER, op. cit., p. 221 et réf. citées). Il peut s'agir également des informations relatives aux modes de comportement et aux habitudes de consommation (art. 2 al. 2 lit h LPD). Parmi ceux-ci, la doctrine et la jurisprudence citent, entre autres exemples, l'ensemble des références lectures dans une bibliothèque ou un profil de navigation sur Internet (P. MEIER, op. cit., p. 228 et réf. citées).

D'une manière générale, il est admis que certaines données relatives aux communications, tels que les fichiers journaux (log files) qui indiquent notamment quand et depuis quel ordinateur une page Web a été consultée, peuvent être sensibles et leur analyse peut permettre de constituer des profils de la personnalité (Message du Conseil fédéral du 27 novembre 2009, FF 2009 7695). S'agissant d'employés en particulier, la doctrine retient également que l'analyse de l'activité de navigation Internet de ceux-ci par l'employeur est susceptible de porter sur des traits essentiels de la personnalité et du comportement du travailleur, qui se manifestent par ses choix de navigation, et donc sur un profil de la personnalité (P. MEIER, op. cit., p. 713).
Enfin, dans une décision du 1er septembre 2004, l'autorité de céans a tenu pour sensibles des informations et appréciations sur le comportement des collaborateurs d'un service de l'Etat, pouvant donner lieu à des reproches et engager la responsabilité disciplinaire de ceux-ci (RJJ 2004, p. 230, consid. 3.2.1).

Au cas d'espèce, d'une part, la nature des sites recensés relève manifestement de la sphère intime. D'autre part, dans la mesure où le contrôle a porté sur un mois durant, sur les horaires de connexion, les sites les plus fréquentés par chacun des utilisateurs, etc., et que ces analyses ont permis d'établir les modes de comportement de certains membres de la fonction publique pouvant engager leur responsabilité disciplinaire, les données collectées par le SDI à cette occasion doivent être considérées comme sensibles.

Dès lors, c'est à la lumière des exigences accrues de l'article 5 al. 2 LPD que doit être examiné le traitement de données effectué par le SDI, ayant consisté à collecter des informations sur les sites consultés par les membres de la fonction publique cantonale et les auteurs desdites consultations, cela au moyen de l'analyse des fichiers journaux du proxy permettant l'accès à Internet, respectivement des fichiers « index.dat » dont l'accès sur le disque C: a été obtenu au moyen d'une prise en main à distance des postes informatiques.

2.2 En vertu de l'article 5 al. 2 LPD, les données sensibles ne peuvent être traitées que si une base légale formelle le prévoit ou si l'accomplissement d'une tâche légale l'exige absolument ou encore si la personne concernée a donné expressément son accord.

2.2.1 Dans le canton du Jura, le Gouvernement a édicté une directive, le 13 mars 2001, relative aux enregistrements et à la surveillance informatique. Cette directive prévoit notamment qu'en cas d'abus intolérables s'agissant d'accès à Internet par les collaborateurs, abus qui seraient décelés préalablement au moyen d'un contrôle ne se rapportant pas à des utilisateurs spécifiques, les employés faillibles seront repérés personnellement et subiront des sanctions disciplinaires.

Cette directive est inspirée des exigences posées par la doctrine en matière de droit privé du travail et des recommandations du Préposé fédéral à la protection des données et à la transparence (ci-après PFPDT), telles qu'elles ressortent de son Guide de décembre 2007 relatif à la surveillance de l'utilisation d'internet et du courrier électronique au lieu du travail, à l'attention des administrations publiques et de l'industrie privée. Il est en effet admis en droit du travail que l'employeur peut exercer une surveillance de la navigation Internet de ses employés à certaines conditions. A cet égard et pour satisfaire les principes de la bonne foi, de la reconnaissabilité, ou encore du devoir d'information conditionnant une telle surveillance, un règlement est indispensable si l'employeur entend procéder à des contrôles nominaux sans avoir à donner une information spécifique individuelle à chaque fois (Guide du PFPDT, op. cit., p. 18 ; P. MEIER, op. cit., p. 713 et réf. citées). En outre, l'employeur doit ensuite se conformer au principe de proportionnalité s'agissant des modalités du contrôle, en respectant les différents stades d'analyses retenus par la doctrine : journalisation de la navigation des collaborateurs sur Internet ; contrôles anonymisés ne se rapportant pas aux personnes (analyse statistique des fichiers journaux effectués par ex. selon le critère des pages web les plus consultées) ; contrôles pseudonymisés (analyses non

nominales se rapportant aux personnes), en cas de soupçons sur un service ou un groupe de personnes ; enfin, en cas de soupçon concret de violation du règlement d'utilisation, un contrôle nominatif est dès lors admissible pour autant qu'il soit prévu par le règlement (P. MEIER, op. cit., p. 713ss ; Guide du PFPDT, op. cit., p. 21). Il convient de relever que la doctrine retient qu'à partir du stade des contrôles pseudonymisés, les analyses doivent être décidées par la direction de l'entreprise ou le service des ressources humaines et ne peuvent être laissés à la compétence des seuls services informatiques (P. MEIER, op. cit., p. 715). D'autre part, la même doctrine considère, au sujet des contrôles pseudonymisés, qu'un nom d'utilisateur (USERID) ou une adresse IP statique ne constituent pas des pseudonymes suffisants (Guide du PFPDT, op. cit., p. 21 ; P. MEIER, op. cit., p. 715). Il y a encore lieu de mentionner que, toujours selon la doctrine, en cas de soupçons d'infractions pénales ou d'atteinte grave aux intérêts de l'entreprise, l'employeur peut procéder à une surveillance même s'il n'a pas informé le personnel spécifiquement ou globalement (par un règlement de surveillance), dans la mesure où il serait alors en mesure de se prévaloir d'un intérêt privé, voire public, prépondérant au sens de l'article 13 al. 1 LFPD (P. MEIER, op. cit., p. 715ss)

Respectant les différentes étapes prévues par la doctrine, la directive du 13 mars 2001, bien que d'une rédaction très compliquée et parfois contradictoire, permet ainsi de répondre aux exigences en matière de proportionnalité, de reconnaissabilité ou encore de bonne foi qui s'appliquent à un traitement de telles données par un employeur. A cet égard, on relèvera que ladite directive avait été approuvée par l'autorité de céans, lors de son adoption par le Gouvernement.

En revanche, d'une part, la directive du 13 mars 2001 ne contient aucune indication quant à l'autorité compétente pour ordonner et procéder à de tels contrôles. D'autre part, elle ne représente manifestement pas une base légale formelle permettant au SDI de traiter des données personnelles sensibles, au sens de l'article 5 al. 2 litt. a LPD. A cet égard, il est rappelé que l'on considère comme une loi au sens formel tout acte que le législateur a adopté selon la procédure législative ordinaire (A. AUER / G. MALINVERNI / M. HOTTELIER, Droit constitutionnel suisse, Berne 2006, Vol. I, p. 516). En droit jurassien, une loi au sens formel est l'acte législatif qui est adopté par le Parlement après deux lectures (art. 83 al. 3 CJU) et qui est assujetti au référendum facultatif en vertu de l'article 78 litt. a CJU (J. MORITZ, La loi en droit constitutionnel jurassien, CJE 2007, p. 29 N 78).

En outre, il ne faut pas perdre de vue que les recommandations du PFPDT, de même que les exigences de la doctrine en matière de droit du travail, autorisant l'employeur à exercer une surveillance de la navigation Internet de ses employés sur la base d'un simple règlement d'entreprise, ne valent principalement qu'en matière de rapports de travail de droit privé. En effet, d'une part, le traitement de données personnelles ordinaires ou sensibles par des personnes de droit privé, régis par la LFPD, n'est pas soumis à l'exigence d'une base légale formelle ou matérielle par la loi précitée, celle-ci

n'imposant le respect d'une base légale qu'aux traitement de données effectués par les organes fédéraux (art. 17 LFPD). D'autre part et contrairement à ce qui prévaut pour les organes de l'Etat, les mêmes employeurs privés peuvent se prévaloir de motifs justificatifs, au sens de l'article 13 LFPD, permettant notamment de justifier, par un intérêt prépondérant de l'auteur, un traitement de données portant atteinte à la personnalité de la personne concernée. Dès lors, au sein d'une administration publique cantonale ou communale, l'adoption d'un règlement ou de simples directives autorisant une surveillance de la navigation Internet des collaborateurs ne suffirait que dans les cantons qui ne seraient éventuellement pas soumis, dans le cadre de leur propre législation, à l'exigence d'une base légale formelle en matière de traitement de données sensibles.

Il s'ensuit que la directive du 13 mars 2001 relative aux enregistrements et à la surveillance informatique ne permet pas, à elle seule, l'enregistrement, l'analyse et l'utilisation des données sensibles que représentent les fichiers journaux d'accès Internet ou « index.dat » mis en rapport avec les postes informatiques des collaborateurs du canton ou leurs adresses IP.

Dès lors qu'il s'agissait de contrôler le respect de la directive du 13 mars 2001 concernant les modalités d'utilisation d'Internet par les collaborateurs de la fonction publique et de leurs devoirs de service en général, respectivement d'établir les violations de tels devoirs et d'en identifier les auteurs, c'est uniquement dans le cadre d'une procédure d'enquête disciplinaire au sens de l'article 32 aLStFM, en vigueur à l'époque des faits, ou 68 LOJ, qu'une telle analyse et utilisation des fichiers journaux, permettant d'identifier les auteurs de connexions à des sites pornographiques, pouvait être réalisée en respectant le principe de la légalité. En effet, une procédure disciplinaire aboutissant à une décision au sens de l'article 2 CPA, le Code de procédure administrative lui était applicable (RJJ 1995, p. 339 ; RJJ 1998, p. 146 ; RJJ 1998, p. 241). Notamment, les articles 58ss CPA, subsidiairement 168ss CPC ou 210ss aCpcj par renvoi de l'article 69 CPA, relatifs à l'établissement des faits et les moyens de preuve pouvant être ordonnés par l'autorité administrative, s'appliquent à la procédure d'enquête disciplinaire (RJJ 1998, p. 74s). En particulier, l'article 59 al. 1 lit. a CPA prévoit que l'autorité procède aux investigations nécessaires en recourant s'il y a lieu aux titres, rapports, livres et autres documents officiels et privés. Or, il est admis en doctrine que les termes « autres documents » permettent de prendre en compte les nouveaux moyens résultant de l'évolution des progrès techniques (B. BOVAY, Procédure administrative, Berne 2000, p 188). Dans le même sens, l'article 177 CPC, auquel l'article 69 CPA renvoie, définit expressément les fichiers électroniques et les données analogues comme des documents constituant des titres pouvant servir de moyens de preuve. Il s'ensuit que les articles 59ss CPA, applicables dans le cadre d'une procédure décisionnelle, telle qu'une enquête disciplinaire, représentaient une base légale formelle suffisante pour un traitement de données sensibles comme une analyse nominative ou identifiante de fichiers journaux d'accès Internet des postes de travail de collaborateurs de la fonction publique.

Cependant, il appartenait à l'autorité disciplinaire, à savoir le Gouvernement, respectivement le Conseil de surveillance de la magistrature, de décider de l'ouverture d'une telle procédure. Surtout, en vertu de l'article 50 CPA et sous réserve de l'article 50 al. 2 CPA, c'était à l'autorité disciplinaire de diriger l'enquête, notamment en ordonnant les moyens de preuve nécessaires à établir les faits et identifier les auteurs éventuels de violations de devoirs de service.

En d'autres termes, dès la découverte d'indices sérieux de violation des devoirs de services, tels qu'ils ressortaient de la toute première analyse des fichiers journaux ayant permis au SDI d'identifier le problème de saturation du réseau, il appartenait à celui-ci de saisir le Gouvernement, respectivement le Conseil de la magistrature, qui seuls étaient habilités à ordonner que soient effectuées par le SDI (art. 50 al. 2 CPA) les analyses des fichiers journaux mis en relation avec les adresses IP des postes de travail des collaborateurs de la fonction publique, respectivement à mandater une société externe pour effectuer de telles analyses (art. 50 al. 3 CPA).

2.2.2 Le fait que certains sites consultés laissaient à penser qu'un délit pénal aurait pu être commis par certains collaborateurs n'autorisait pas non plus le SDI à procéder lui-même aux analyses des fichiers journaux mis en relation avec les adresses IP des postes informatiques des collaborateurs.

En effet, en 2008 et 2009, les mesures de surveillance de connexions Internet, en temps réel ou rétroactives, destinées à élucider une infraction pénale, relevaient de la LSCPT. Or, en vertu de l'article 193 aCppj, c'est au Juge d'instruction qu'il aurait appartenu d'ordonner une telle surveillance de télécommunications. Il convient, en outre, de relever que la décision d'un Juge d'instruction dans ce sens aurait dû être approuvée, dans les 5 jours, par la Chambre d'accusation (art. 194 et 195 aCppj). Suite à l'entrée en vigueur du Code de procédure pénal fédéral, une telle surveillance est désormais ordonnée par le Ministère public et approuvée par le Juge des mesures de contraintes (art. 269 et 274 CPP).

Il y a lieu de rappeler que, contrairement à ce qui prévaut en matière de rapports de travail de droit privé, l'Etat ou ses services ne peuvent invoquer un motif justificatif au sens de l'article 13 LFPD, de telle sorte que les principes dégagés par la doctrine au sujet du droit de l'employeur de procéder à une surveillance en cas de soupçons d'infractions pénales (ch. 2.2.1 de la présente décision) ne lui sont pas applicables.

Bien plus, en vertu des règles de la procédure pénale à ce sujet, de telles preuves réunies de façon illicite par un organe de l'Etat auraient vraisemblablement été écartées du dossier de l'instruction pénale (CR CPP – J. BENEDICT / J. TRECCANI, art. 141 N 4), créant ainsi le risque de ne pas pouvoir poursuivre l'auteur de l'infraction.

Il résulte de ce qui précède qu'en présence d'indices laissant supposer que certains collaborateurs aient consultés des sites de nature pornographique au sens de l'article 197 CPP, il appartenait au SDI, respectivement sa hiérarchie, de dénoncer les faits aux autorités pénales, seules compétentes pour ordonner une surveillance rétroactive des connexions Internet des collaborateurs du canton en vue de collecter les preuves permettant d'établir l'infraction éventuelle.

Au demeurant, il convient encore de relever que la directive du 13 mars 2001 prévoyait expressément cette obligation, en disposant que, « lors d'indices d'une infraction pénale commis au moyen d'Internet, seules les autorités de poursuite pénale interviendront. Ces dernières décideront de la procédure à suivre et des mesures de surveillance idoines ».

2.2.3 En vertu de l'article 5 al. 2 lit. a 2ème phrase LPD, des données personnelles sensibles peuvent être traitées, en dépit de l'inexistence d'une base légale formelle, si l'accomplissement d'une tâche légale l'exige absolument.

A cet égard, il y a lieu de relever que les conditions permettant à une autorité de traiter des données sensibles en vertu de cette disposition sont les mêmes que celles auxquelles la communication de données à caractère personnel à une autre autorité ou à d'autres organes publics est subordonnée en application de l'article 13 LPD. Or, l'article 13 litt. b LPD, selon lequel des données à caractère personnel peuvent être communiquées à des autorités ou à d'autres organes publics lorsque le requérant établit qu'il en a absolument besoin pour l'exécution de ses tâches légales, vise une hypothèse qui supplée à l'absence d'une base légale formelle. Selon la jurisprudence constante de l'autorité de céans, la communication ne peut intervenir, sur la base de l'article 13 litt. b LPD, que si le destinataire des informations n'est pas en mesure d'accomplir une tâche légale, clairement définie, sans la connaissance des données pertinentes. La communication doit répondre, pour lui, à une nécessité absolue (RJJ 2008, p. 93 consid. 5.2 et réf. citées ; RJJ 1999, p. 106ss, consid. 2 et réf. citées). Cette jurisprudence est aussi applicable, mutatis mutandis, au traitement des données sensibles prévu à l'article 5 al. 2 LPD lorsque le traitement est exigé par l'accomplissement d'une tâche légale. Autrement dit, on doit admettre que ce n'est qu'à la condition que l'autorité ne soit pas en mesure d'accomplir une tâche légale, clairement définie, sans les données dont elle a absolument besoin, qu'elle peut traiter des données sensibles en l'absence d'une base légale formelle.

En l'espèce, les tâches légales du SDI sont définies par l'article 146 DOGA. Il s'agit de la responsabilité du traitement électronique de l'information, le conseil aux organes de l'administration en matière d'automation et d'informatique, la coordination des efforts tendant à introduire le traitement électronique de l'information dans l'administration et toute autre attribution conférée par la législation.

En tant que responsable du traitement électronique de l'information en particulier, il appartient bien au SDI, en face d'un problème d'accès Internet, d'identifier le problème en question et de le résoudre, pour autant que la solution à un tel problème soit d'ordre technique. En revanche, face à un constat d'abus dans l'utilisation d'Internet, le SDI ne pouvait tirer aucune compétence de l'article 146 DOGA s'agissant d'en identifier les auteurs et de réunir les preuves exploitables en vue de la conduite d'une procédure disciplinaire, cette attribution étant réservée par la loi au Gouvernement, respectivement au Conseil de surveillance de la magistrature.

Il s'ensuit que le SDI n'est pas en mesure de se prévaloir d'une tâche légale qui l'aurait autorisé à analyser les fichiers journaux en vue d'identifier les auteurs des connexions à des sites problématiques ou simplement les postes de travail de ceux-ci ou de réunir les preuves de telles connexions. En outre, dans la mesure où il ressort du ch. 2.2.1 de la présente décision qu'il eût été possible que de telles analyses soient ordonnées, en toute légalité, par le Gouvernement ou le Conseil de surveillance de la magistrature, le traitement de ces données par le SDI de sa propre initiative n'apparaissait de toute manière pas indispensable à l'accomplissement d'une tâche légale au sens de la jurisprudence précitée.

2.2.4 Conformément à l'article 5 al. 2 litt. b LPD, des données sensibles peuvent encore être traitées, en dépit de l'inexistence d'une base légale formelle, si la personne concernée a donné expressément son accord. L'exigence d'un consentement exprès exclut tout accord tacite, par actes concluants ou encore hypothétique.

Au cas particulier, un tel accord exprès des membres de la fonction publique quant au traitement de données relatives à leurs connexions Internet fait manifestement défaut.

2.2.5 La question de la nécessité d'une base légale formelle pour traiter les données personnelles liées à l'utilisation de l'infrastructure électronique de l'administration dans le canton du Jura peut être, dans une large mesure, rapprochée de la situation qui prévalait au sein de l'administration et des tribunaux fédéraux jusqu'à l'adoption des modifications du 1er octobre 2010 de la Loi fédérale sur l'organisation du gouvernement et de l'administration (ci-après LFOGA), de la Loi sur le Tribunal fédéral, de la Loi sur le Tribunal administratif fédéral, de la Loi fédérale sur l'organisation des autorités pénales et de la Loi sur le Tribunal fédéral des brevets.

En effet, l'article 17 LFPD qui s'applique aux organes fédéraux, dispose que ceux-ci ne sont en droit de traiter des données personnelles que s'il existe une base légale (art. 17 al. 1 LFPD). En vertu de l'article 17 al. 2 LFPD, des données sensibles ou des profils de la personnalité ne peuvent être traités que si une loi au sens formel le prévoit expressément ou si, exceptionnellement : a) l'accomplissement d'une tâche clairement définie dans une loi au sens formel l'exige absolument ; b) le Conseil fédéral l'a autorisé en l'espèce, considérant que les droits des personnes concernées ne sont pas menacés ; c) si la personne concernée y a, en l'espèce, consenti ou a rendu ses

données accessibles à tout un chacun et ne s'est pas opposée formellement au traitement. Cette disposition présente des similitudes manifestes avec l'article 5 de la LPD cantonale jurassienne.

Or, aux termes de son message du 27 novembre 2009 (FF 2009 7693), le Conseil fédéral relevait que les données relatives aux communications, c'est-à-dire les données générées par l'utilisation de l'infrastructure électronique, sont conservées un certain temps au moins. Ce sont en particulier les fichiers journaux (log files), qui indiquent notamment quand et entre quelles personnes une communication téléphonique a eu lieu ou quand et depuis quel ordinateur une page web a été consultée. Or, selon le Conseil fédéral, les données relatives aux communications mais aussi celles relatives au contenu de ces dernières peuvent faire l'objet d'une analyse se rapportant aux personnes. Or, certaines de ces données personnelles sont sensibles et leur analyse peut permettre de constituer des profils de la personnalité (FF 2009 7697). A cet égard, le Conseil fédéral constatait qu'il n'existait pas de base légale pour la conservation de ces données par les organes fédéraux et proposait de mettre en place la base légale formelle nécessaire pour traiter les données personnelles liées à l'utilisation de l'infrastructure électronique de l'administration, tout en réservant l'existence de règles spéciales autorisant déjà le traitement de ces données personnelles à de strictes conditions, telles que les règles de la procédure disciplinaire permettant la « perquisition » de telles données (25 LFPers et 98 OFPers renvoyant aux art. 12 et 19 PA), de la procédure pénale (LSCPT ou CPP) ou encore d'autres lois spéciales (LTC, LMSI, LIFD, etc.), qui continueront à s'appliquer.

Ainsi, le 1er octobre 2010, l'Assemblée fédérale a adopté plusieurs modifications de la LFOGA. Notamment, le nouvel article 57l litt. b ch. 3 LFOGA prévoit que les organes fédéraux peuvent enregistrer les données personnelles liées à l'utilisation de leur infrastructure électronique pour contrôler le respect des règlements d'utilisation. L'article 57m LFOGA dispose que les données enregistrées peuvent être analysées sans rapport avec des personnes dans les buts mentionnées à l'article 57l LFOGA. L'article 57n LFOGA permet une analyse en rapport avec des personnes mais de manière non nominale, par sondage, dans le but de contrôler l'utilisation de l'infrastructure électronique ou le temps de travail du personnel. Enfin, l'article 57o al. 1 lit. a et b LFOGA autorise l'analyse des données enregistrées en rapport avec des personnes et de manière nominale dans le but d'élucider un soupçon concret d'utilisation abusive ou poursuivre un cas d'utilisation abusive ou d'analyser les perturbations électroniques, y remédier ou parer aux menaces concrètes qu'elle subit. La Loi sur le Tribunal fédéral, sur le Tribunal administratif fédéral, sur l'organisation des autorités pénales et sur le Tribunal fédéral des brevets ont été modifiées dans le même sens. Ces dispositions n'ont toutefois pas encore été mises en vigueur.

Dès lors, vu les similitudes entre l'article 5 LPD et 17 LFPD, il convient de s'inspirer des considérations émises par le Conseil fédéral quant à la nécessité d'une base légale formelle pour les traitements des données personnelles liées à l'utilisation de

l'infrastructure électronique de l'administration, notamment ceux destinés aux contrôles du respect des règlements d'utilisation, et de constater que le droit cantonal jurassien ne prévoit pas une base légale formelle permettant d'effectuer de telles analyses ou contrôles à des conditions plus larges ou par d'autres autorités que celles prévues par la procédure disciplinaire ou par les nouvelles procédures de la LPers dont il sera question ci-dessous.

2.2.6 Aux termes de son courrier du 30 janvier 2009 adressé à M. A., le Président de la Commission de protection des données a admis, d'une manière générale, la validité du traitement de données effectué par le SDI. Cependant, d'une part, il mettait clairement en doute la conformité de la collecte de données opérée au moyen de la prise en main à distance des postes informatiques sans en indiquer le motif exact à l'utilisateur concerné. D'autre part, il convient de relever que sous ch. 3 de son courrier précité, le Président déclarait : « L'opération étant ponctuelle, elle n'a, en principe pas à être validée par la Commission cantonale de la protection des données. Cette opération est en effet menée à la demande et sous la responsabilité de l'autorité exécutive, c'est-à-dire qui détient le pouvoir de surveillance sur l'administration et le personnel de l'Etat, en application des directives susmentionnées qui ont reçu l'approbation de la CPD ». En d'autres termes, lors de son avis du 30 janvier 2009, le Président de la CPD partait expressément du principe que les contrôles menés par le SDI étaient effectués sur instruction de l'autorité disciplinaire. Ce n'est qu'à réception des courriers du 10 juin 2009 du Conseil de surveillance de la magistrature et du 7 juillet 2009 du Gouvernement qu'il s'est avéré que les autorités disciplinaires en question n'avaient pas ordonné ou autorisé de telles analyses.

En tout état de cause et comme le Président de la CPD l'annonçait lui-même expressément aux termes de son courrier précité, l'avis qu'il fournissait sous la forme d'un conseil, au sens de l'article 50 al. 2 litt. g LPD, ne lie pas la CPD dans le cadre de la présente procédure.

Enfin, il résulte du rapport « Analyse trafic réseau » de SCRT qu'au moment où l'avis du Président de la CPD a été requis, respectivement donné, l'ensemble du traitement de données avait déjà été réalisé par le SDI, sous réserve de l'établissement d'une liste nominative (ch. 13 à 15 du processus décrit aux termes du courrier du 29 janvier 2009 de M. A.). En particulier, il ressort de ce document que l'enregistrement des données au moyen de la prise en main à distance des postes de travail a été effectué jusqu'au 15 janvier 2009 (rapport SCRT « Analyse réseau », p. 99ss, tableau du ch. 4). Par conséquent, au 29 janvier 2009, le processus décrit par M. A. était déjà accompli au moins jusqu'à son étape no 12. L'avis donné par le Président de la CPD à l'époque n'a donc, de toute manière, eu aucune incidence sur un traitement de données déjà effectué par le SDI et dont celui-ci requérait une validation a posteriori.

2.3 Au vu de ce qui précède, la CPD aboutit à la conclusion que, tant et aussi longtemps que les autorités compétentes n'avaient pas ouvert formellement des procédures

disciplinaires et ordonné elles-mêmes une telle collecte de données, les informations recueillies par le SDI, sur la base de l'analyse des fichiers journaux d'accès Internet ou « index.dat », et mises en relation avec les adresses IP des postes informatiques des membres de la fonction publique ou leurs utilisateurs, l'ont été sans base légale suffisante au sens de l'article 5 LPD. Il appartient donc à la CPD d'en constater l'illicéité.

3. En vertu de l'article 7 al. 2 LPD, des données à caractère personnel ne peuvent être traitées dans un but qui, selon les règles de la bonne foi, serait incompatible avec celui qui avait motivé leur collecte. En outre, l'article 12 LPD prévoit que la collecte de données à caractère personnel se fait en principe auprès de la personne concernée. La base légale et le but du traitement lui sont communiqués.

Le principe de la bonne foi exige que l'autorité s'abstienne de tout comportement propre à tromper les administrés ou contradictoire. Il s'agit à la fois d'un principe constitutionnel (art. 5 al. 3 Cst féd.) et d'un droit fondamental (art. 9 Cst. féd. ; A. AUER / G. MALINVERNI / M. HOTTELIER, op. cit., Vol. I, p. 755 N 2149 et réf. citées, et Vol. II, p. 472 N 1003). En vertu de l'article 26 al. 1 CPA, l'autorité administrative doit agir conformément au principe de la bonne foi. Cette obligation résulte également des articles 9 Cst. féd. et 56 al. 1 CJU. Il est notamment admis que l'autorité administrative viole son obligation de bonne foi lorsqu'elle donne à un administré des renseignements inexacts ou trompeurs (G. BOINAY, La procédure administrative et constitutionnelle du canton du Jura, Porrentruy 1993, art. 26 N 2).

Le principe de la bonne foi tient une place centrale dans le droit de la protection des données, en tant que clause générale. Il implique une exigence de transparence dans le traitement des données à caractère personnel (BSK DSG – U. MAURER-LAMBROU / A. STEINER, Art. 4 N 8). En droit jurassien, le principe de la spécificité du but, selon lequel le traitement de données à caractère personnel doit viser un but déterminé à l'avance (art. 7 al. 1 LPD) en découle. La doctrine en matière de protection des données retient expressément qu'un traitement de données effectué clandestinement constitue une violation du principe de la bonne foi, même lorsqu'aucune norme particulière n'est violée. C'est le cas de l'obtention d'informations en indiquant une fausse identité ou un faux but (ROSENTHAL/JÖHRI, Handkommentar zum Datenschutzgesetz, 2008, n. 14 ad art. 4). Lors de la procédure d'adoption de la LFPD du 19 juin 1992 et aux termes de son message du 23 mars 1988 (FF 1988 II 457), commentant l'article 4 du projet de la LFPD, le Conseil fédéral relevait : « à côté des dispositions générales s'opposant à la collecte qui peuvent le cas échéant trouver application, un principe revêt ici une importance particulière : les données doivent être traitées conformément à la bonne foi. Les données ne doivent pas être collectées à l'insu de la personne concernée ou contre sa volonté. Celui qui recueille des données en trompant intentionnellement la personne concernée – par exemple en se présentant sous une fausse identité ou en donnant de fausses indications quant au but du traitement – transgresse le principe de la bonne foi (cf. art. 28 CO). Il en va de même de celui qui collecte des données clandestinement, par exemple en écoutant les

conversations ou en épiant des personnes, ou encore en manipulant les programmes d'un système de communication interactif (vidéotex). Remarquons au passage qu'une telle collecte peut en outre constituer une infraction pénale ».

Au cas d'espèce, on doit constater que le principe de la bonne foi a été violé. En s'infiltrant subrepticement dans les postes des fonctionnaires et magistrats suspectés de consultations illicites de sites Internet, notamment en indiquant à ces personnes ou en leur laissant accroire que le motif de cette intervention relevait de la télémaintenance, alors qu'en réalité il s'agissait de recueillir des preuves des consultations de sites pornographiques, le SDI a utilisé un procédé déloyal, contrevenant ainsi à un principe essentiel régissant l'activité des organes de l'administration.

S'agissant des motifs invoqués pour justifier la prise en main à distance, il ressort des réponses adressées, le 23 juillet 2010, par SCRT à la Cour administrative dans la procédure de recours de X., qu'il n'existait en réalité aucune impossibilité technique à ce que les preuves nécessaires à l'établissement des faits soient réunies d'une façon conforme au droit, à savoir par une saisie des disques durs ordonnée par l'autorité disciplinaire. Les seuls motifs mis en évidence par SCRT aux termes des réponses précitées, à savoir la question du temps et du coût lié à l'analyse de 54 disques durs au lieu de 30, ne permettent manifestement pas de déroger au principe du respect de la bonne foi par les organes de l'Etat, pour autant qu'une telle dérogation au moyen d'une pesée des intérêts ait pu être envisagée à ce sujet.

Il en va de même du prétendu effet traumatisant pour les collaborateurs de l'Etat qui aurait pu être visés à tort par la saisie de disques durs et que la prise en main à distance aurait permis d'écarter. Il est rappelé qu'une enquête disciplinaire peut être ordonnée dès qu'il existe des indices précis faisant admettre la probabilité d'une violation des devoirs de fonctions. (RJJ 1998, p. 71). Il n'est pas requis que les faits soient établis à suffisance de preuve déjà au stade de l'ouverture de l'enquête, dans la mesure où c'est l'enquête en question qui aura pour but d'établir les faits permettant de confirmer ou d'infirmer les soupçons pesant sur le collaborateur, avec naturellement l'éventualité qu'une violation des devoirs de fonction ne soit, en définitive, pas confirmée. En d'autres termes, soit les indices sont suffisamment sérieux et crédibles pour qu'une enquête disciplinaire soit ouverte contre le collaborateur soupçonné, soit il convient d'y renoncer. Face à certains cas litigieux, il appartenait à l'autorité disciplinaire de décider, notamment en fonction des indices existant et du risque que ceux-ci ne soient finalement pas confirmés, de l'opportunité d'une enquête dans les cas problématiques. En aucun cas, cette situation n'autorisait le SDI à procéder à une recherche de preuves sur les ordinateurs des collaborateurs, en obtenant leur autorisation quant à une prise en main à distance au moyen d'un subterfuge.

Il appartient donc également à la CPD de constater l'illicéité de la recherche et de l'enregistrement par le SDI des données contenues dans les fichiers « index.dat »

situés sur le disque C: des postes informatiques des membres de la fonction publique, obtenues par une prise en main à distance des postes tout en cachant la nature exacte de cette opération ou en prétextant un motif de télémaintenance.

4. En vertu de l'article 2 al. 4 LPD, l'utilisation et la conservation de données personnelles représentent des traitements au sens de la LPD. A ce titre, la CPD peut ordonner la cessation du traitement, ainsi que la destruction des données déjà recueillies, cela sur requête (art. 36 al. 1 litt. b LPD) ou d'office (art. 50 al. 1 et 2 litt. a LPD).

4.1 En ce qui concerne les données collectées illicitement par le SDI au moyen de l'analyse des fichiers journaux, celles-ci ont été par la suite administrées dans le cadre des procédures disciplinaires (cf. rapports forensiques) et demeurent conservées au sein des dossiers en question.

Comme exposé sous chiffre 2.2.1 de la présente décision, l'établissement des faits par l'autorité disciplinaire et la collecte des preuves par celle-ci sont régis par le CPA. Or, il est admis en procédure administrative que l'utilisation de preuves obtenues par des moyens illégaux ne peut intervenir que si les preuves en question auraient pu être recueillies d'une façon légale (ATF 99 V 12 ; B. BOVAY, Procédure administrative, Berne 2000, p. 190 et réf. citées ; B. KNAPP, Précis de droit administratif, Bâle 1991, p. 419 N 2020 et réf. citées). En sus, une partie de la doctrine admet également l'utilisation de preuves illégales si un intérêt public important le justifie (P. MOOR / E. POLTIER, Droit administratif, Berne 2011, Vol. II, p. 297 et réf. citées).

En l'espèce, la CPD constate qu'il eût été juridiquement possible pour l'autorité disciplinaire, en présence d'indices de navigation Internet abusive par des collaborateurs, de procéder ou de faire procéder, dans le cadre d'une enquête préalablement ouverte, aux analyses anonymes ou pseudonymes des fichiers journaux permettant de confirmer ou d'infirmer les soupçons, puis, en cas de confirmation, aux analyses nominatives en vue d'identifier les auteurs des abus en question, conformément à la directive du 13 mars 2001, aux recommandations du PFPDT et à la doctrine en la matière (Meier, op. cit., p. 714ss). Comme cela a été exposé sous ch. 2.2.1 précité, les articles 59 ss CPA représentent la base légale formelle nécessaire à un tel traitement de données. L'existence d'un intérêt privé de l'employeur, respectivement public lorsque l'employeur est une administration, à effectuer de tels contrôles en vue du respect de ses directives en matière de navigation Internet, intérêt mis en rapport avec la sécurité du réseau informatique, le temps de travail, la capacité de stockage et la bande passante du réseau, ou encore la réputation de l'employeur, n'est pas contesté en doctrine (cf. notamment le Guide du PFPDT, op. cit., p. 6). Le suivi des étapes d'analyse (anonyme ou pseudonyme, puis nominative) des fichiers journaux permet, en outre, de respecter le principe de proportionnalité posé par l'article 6 LPD dans le traitement de telles données (MEIER, op. cit., p. 713ss). De plus, la finalité disciplinaire du traitement effectué dans le cadre de l'enquête étant prévu par la loi elle-même (art. 32 LStFM), il n'aurait pas été

nécessaire de respecter, en sus, le principe de reconnaissabilité (MEIER, op. cit., p. 277).

Dès lors, quand bien même les données collectées par le SDI au moyen des analyses de fichiers journaux, fin 2008 et début 2009, l'ont été de manière illicite, les mêmes données auraient pu valablement, au sens de la LPD, être réunies par l'autorité disciplinaire elle-même. Celle-ci était donc en droit de les utiliser a posteriori dans le cadre des enquêtes disciplinaires ouvertes à l'encontre des collaborateurs, conformément au principe admis en jurisprudence et en doctrine sur l'utilisation de moyens de preuve obtenus par des moyens illégaux. Il n'y a donc pas lieu d'ordonner leur destruction.

Il en va de même des données collectées par l'autorité disciplinaire elle-même, au moyen de la saisie et de l'analyse des disques durs. D'une part, une telle collecte est intervenue conformément à la loi (art. 59 al. 1 litt. a et 51 al. 1 et 2 CPA). D'autre part, elle aurait pu, en pratique, porter sur l'ensemble des postes impliqués par l'analyse des fichiers journaux, de telle sorte qu'elle ne dépendait pas, pour être ordonnée, d'une analyse illicite effectuée préalablement au moyen d'une prise en main à distance par le SDI des postes informatiques. En effet, contrairement aux déclarations des représentants de SCRT ou du SDI auprès de la Cour administrative pour tenter de justifier la prise en main à distance des postes informatiques, la CPD arrive à la conclusion qu'il aurait été possible pour l'autorité disciplinaire de saisir et d'analyser les 54 disques durs des postes impliqués au moyen de l'analyse des fichiers journaux. Notamment, le surplus de coût et de temps qu'aurait entraîné une analyse de 54 disques durs au lieu de 29, mis en exergue par le SDI et SCRT, ne permet pas à la CPD de conclure à l'impossibilité pratique d'une telle administration de preuve par l'autorité disciplinaire. S'agissant du temps en particulier, il ressort du rapport d'enquête de la Commission présidée par le Juge Baechler que la saisie des disques durs est intervenue à partir du 5 mars 2009. Les rapports forensiques résultant de l'analyse des disques durs ont été remis à la Commission d'enquête, au fur et à mesure de leur élaboration, que peu de temps avant les auditions des collaborateurs qui se sont tenues du 20 mars au 24 avril 2009. Il s'ensuit que l'analyse et la rédaction des rapports forensiques portant sur la trentaine de disques durs saisis ont duré un peu moins de deux mois, sous réserve des compléments d'analyse requis par la Commission d'enquête. Même si l'on part du principe qu'une analyse de 54 disques durs aurait pris le double de temps, à savoir 4 mois, il ne s'ensuit pas une impossibilité pratique de procéder de cette manière. Surtout, il eût été possible, avant de procéder à toutes les analyses nécessaires à l'établissement des rapports forensiques, telles qu'elles sont décrites sous page 7 et 21ss du rapport final de la Commission d'enquête, de procéder sur les disques durs saisis à la même recherche de mots clés dans les fichiers « index.dat » au moyen du programme X-Ways Trace que celle effectuée lors de la prise en main à distance ayant permis d'écarter rapidement les utilisateurs non-concernés. En d'autres termes, la même recherche et analyse limitée, mais permettant d'exclure les postes ou utilisateurs non concernés, effectuée par la

prise en main à distance préalablement à la saisie des disques durs, pouvait être réalisée sur les disques durs une fois saisis. La saisie et la copie des disques durs elles-mêmes impliquaient 1 à 2 heures par disque (Déclarations de M. B., procès-verbal de la séance du 2 mars 2010, p. 6). On ne comprend donc pas l'impossibilité, alléguée par le SDI et SCRT en rapport au coût et au temps, de procéder par la saisie des disques durs au lieu de la prise en main à distance.

4.2 S'agissant des données obtenues illicitement au moyen de la prise en main à distance des postes de travail des collaborateurs, celles-ci sont conservées par le SDI (Déclarations de M. B., procès-verbal de la séance du 2 mars 2010, p. 4). Elles n'ont pas été versées dans les dossiers disciplinaires, ce que confirme l'examen du dossier de première instance de la procédure disciplinaire ouverte à l'encontre du requérant X..

Dans la mesure où, d'une part, la détention de telles données sensibles par le SDI ne repose notamment sur aucune base légale et que, d'autre part, elles ont été obtenues de façon illicite, leur conservation représente ainsi un traitement contraire à la LPD. Il convient donc d'en ordonner la destruction.

4.3 Ce qui a été exposé sous ch. 4.1 et 4.2 doit faire l'objet d'une réserve s'agissant du requérant X., dans la mesure où la procédure disciplinaire ouverte à son encontre est toujours pendante devant la Cour administrative intervenant comme autorité de recours.

A cet égard, il y a lieu de relever que la LPD ne s'applique en principe pas aux procédures judiciaires pendantes. Cela découle, a contrario, de l'article 23 LPD qui dispose que « la présente loi ne s'applique aux procédures civiles, pénales et de juridiction administrative que si : a) les dispositions de procédure ne garantissent pas une protection équivalente des données à caractère personnel ; b) ces procédures conduisent à la création de fichiers destinés à perdurer au-delà du jugement ou de la décision » (RJJ 1999, p. 121 consid. 1b ; RJJ 2008, p. 97s, consid. 2.1). Le but de l'inapplicabilité de la LPD aux procédures judiciaires pendantes est d'éviter de perturber, en raison d'une application trop stricte des principes posés dans la loi, l'administration de la justice dans une procédure qui exige parfois que des données sensibles soient collectées auprès de tiers (Message du Gouvernement, Journal des Débats 1986, no 6, p. 138). Les différents codes de procédure jurassien garantissent les droits des justiciables. En assurant la protection juridique des parties, ils visent, par là même, au respect des droits de la personnalité. Comme au plan fédéral, on peut dès lors considérer que le but de la clause d'exclusion de l'article 23 est d'éviter un concours objectif de normes, en ce sens que la LPD ne doit pas intervenir dans le déroulement d'une procédure judiciaire, notamment pénale. En droit jurassien, ce n'est que si les dispositions de procédure n'offrent pas une protection équivalente que la loi sur la protection des données peut trouver application, ce qui ne peut être décidé qu'au vu d'une situation spécifique (Message du Gouvernement, ibidem ; RJJ 1999, p. 122, consid. 1baa). Dans ce sens, saisie d'une requête tendant au constat de l'illicéité de la

production de pièces dans le cadre d'une procédure pendante devant la juge administrative, l'autorité de céans a considéré qu'il convenait de faire preuve de retenue dans l'examen des griefs du requérant, puisqu'il appartenait en principe au juge, dans une procédure judiciaire soumise à la maxime d'office (art. 58 CPA), de décider quels moyens de preuve étaient nécessaires pour établir les faits et trancher le litige (RJJ 2006, p. 90 consid. 1.1).

Dans le même sens, le Tribunal fédéral retient que, lorsqu'une question relative à la protection des données apparaît dans le cadre d'une procédure qui a pour objet principal d'autres prétentions que celles découlant spécifiquement de la loi sur la protection des données, elle doit être tranchée dans le cadre de la procédure principale et suivre les voies de droit prévues à cet effet (ATF 128 II 328, consid. 8.4).

Il appartient donc à la Cour administrative de se prononcer elle-même, dans le cas concret du requérant X., sur les preuves qu'elle entend administrer ou écarter, en application des règles de la procédure administrative, subsidiairement de la protection des données dans l'hypothèse où elle considérerait que les dispositions du CPA ne garantissent pas une protection équivalente. Ainsi, elle n'est pas liée par la présente décision admettant le principe de l'utilisation par l'autorité disciplinaire de preuves obtenues illicitement par le SDI.

5. Sur la base de l'article 36 al. 1 lit. a LPD, un requérant peut demander à la CPD de faire interdire à l'avenir un traitement de données illicite. En l'espèce, une telle mesure est requise par le requérant X.. En outre, la CPD peut également prononcer une telle interdiction en vertu de ses compétences d'office en matière de surveillance, au sens de l'article 50 al. 1 et al. 2 litt. a LPD.

5.1 Depuis les faits intervenus en 2008 et 2009, la législation sur les rapports de service a été modifiée. Il convient donc d'examiner à quelles conditions actuelles des mesures de surveillance pourrait intervenir au sujet de la navigation Internet des membres de la fonction publique cantonale.

5.1.1 En date du 22 septembre 2010, le Parlement jurassien a adopté une nouvelle Loi sur le personnel de l'Etat (ci-après LPers), abrogeant la LStFM. Cette loi est entrée en vigueur le 1er janvier 2011. Aux termes de l'article 28 al. 4 LPers, relatif aux instruments de travail, le Gouvernement édicte les dispositions réglant la surveillance de l'utilisation des outils de communication, notamment aux fins d'éviter les abus. Les principes régissant la loi sur la protection des données doivent être respectés.

L'article 41 de l'Ordonnance du Gouvernement sur le personnel de l'Etat du 29 novembre 2011 (ci-après OPers), entrée en vigueur le 1er janvier 2012, décrit l'usage par l'employé du matériel et des instruments de travail. En particulier, l'employé est tenu de signer la charte informatique de l'Etat (art. 41 al. 3 litt. a OPers), de respecter en tout temps les normes de sécurité édictées par le Service de l'informatique et de

s'abstenir de consulter, de télécharger, d'enregistrer et de diffuser des documents à caractère pornographique, pédophile, raciste ou violent, au moyen du matériel mis à sa disposition par l'employeur. L'article 175 OPers charge le Service des ressources humaines, avec l'accord du chef du Département auquel il est rattaché ou sur demande de ce dernier, de procéder aux investigations nécessaires en cas de soupçons d'abus ou de violation de la législation sur le personnel de l'Etat. De plus, le Gouvernement peut mandater le Service des ressources humaines, un autre service ou un tiers afin d'effectuer une enquête ou un audit au sein d'une unité administrative (art. 175 al. 2 OPers).

Tel que posé, l'article 28 al. 4 LPers contient une délégation législative en faveur du Gouvernement. Or, en matière de restrictions aux droits fondamentaux, dont fait partie la protection des données (art. 13 al. 2 Cst. féd.), une telle délégation est admissible pour autant que le droit cantonal ne l'exclue pas d'emblée, qu'elle soit limitée à un domaine déterminé et qu'elle figure dans une loi au sens formel, qui contient elle-même les grands traits de la réglementation restrictive. Le Tribunal fédéral interprète ces conditions strictement (ATF 128 I 113 ; 122 I 61 ; 118 Ia 305 = JT 1994 I 630). Mais il admet que même une restriction grave à une liberté puisse se trouver dans une ordonnance fondée sur une délégation législative, pour autant que ses éléments fondamentaux figurent dans la loi (ATF 130 I 26 ; A. AUER / G. MALINVERNI / M. HOTTELIER, Droit constitutionnel suisse, Berne 2006, Vol. I, p. 633).

En l'espèce, vu l'article 5 al. 2 LPD qui soumet le traitement de données sensibles à une base légale formelle et les principes rappelés ci-dessus en matière de délégation législative, l'article 28 al. 4 LPers ne présente pas de façon suffisamment précise les lignes fondamentales de la réglementation déléguée. Il s'ensuit que l'article 28 al. 4 LPers ne peut, à lui seul, être considéré comme la base légale formelle exigée par l'article 5 al. 2 LPD. Il en va de même de l'article 175 OPers, s'agissant d'une ordonnance de substitution représentant uniquement une base légale matérielle (A. GRISEL, Traité de droit administratif, Neuchâtel 1984, Vol. I, p. 314).

La LPers a abrogé la LStFM au sein de laquelle figurait la procédure disciplinaire. En revanche, la LPers prévoit de nouvelles procédures aboutissant à une décision au sens de l'article 2 CPA, soit notamment : la procédure de mutation en raison de l'insuffisance des aptitudes de l'employé aux exigences de la fonction (art. 69 LPers) ; la procédure de licenciement pour des motifs fondés au sens de l'article 87 LPers, notamment lorsque les prestations, le comportement ou les aptitudes de l'employé ne correspondent plus aux exigences du poste (art. 87 al. 2 LPers) ; le licenciement extraordinaire, au sens de l'article 90 LPers ; la décision de suspension selon l'article 92 LPers. Dans la mesure où l'article 59 CPA s'applique aux procédures précitées, il représente la base formelle requise par l'article 5 al. 2 LPD. Il s'ensuit qu'en dehors de ces procédures et d'une instruction de l'autorité compétente pour les mener, une analyse des fichiers journaux ou index.dat en relation avec les postes informatiques

des employés du service public ou leurs adresses IP n'est pas possible, faute de base légale formelle suffisante.

5.1.2 S'agissant des magistrats de l'ordre judiciaire, ceux-ci peuvent toujours faire l'objet d'une procédure disciplinaire, cela conformément aux articles 68 ss LOJ. C'est donc uniquement dans le cadre d'une telle enquête ordonnée par le Conseil de surveillance de la magistrature et sur instruction de celui-ci qu'une analyse des fichiers journaux ou index.dat en relation avec les postes informatiques de magistrats de l'ordre judiciaire ou leurs adresses IP pourrait intervenir.

5.1.3 Au vu de ce qui précède, il convient de faire interdiction au SDI de procéder à des analyses de fichiers journaux ou index.dat pouvant être mises en relation avec des postes informatiques d'employés de l'Etat ou leurs adresses IP, en dehors d'une procédure de mutation, de licenciement ou de suspension et sur instruction de l'autorité compétente pour mener une telle procédure.

Dans le même sens, il convient également de faire interdiction au SDI de procéder à des analyses de fichiers journaux ou index.dat pouvant être mises en relation avec des postes informatiques de magistrats ou leurs adresses IP, en dehors d'une procédure disciplinaire et sur instruction de l'autorité compétente pour mener une telle procédure.

5.2 Lors de l'instruction de l'une des procédures administratives citées ci-dessus, il ne sera naturellement pas possible de collecter des données au moyen d'un subterfuge ou d'une tromperie, tel que prétexter une opération de maintenance sur le poste de travail d'un employé ou d'un magistrat pour rechercher les preuves d'un tel abus, cela en raison du principe de la bonne foi qui s'applique en général à l'activité de l'administration et en matière de protection des données en particulier (ch. 3 de la présente décision). A cet égard, il y a lieu d'interdire un tel procédé à l'avenir.

6. Les requérants Y. et Z. requièrent de la CPD qu'elle constate le caractère illicite de la communication et la diffusion de l'information effectuée par le Gouvernement au sujet de l'enquête dont ils ont fait l'objet.

Le Gouvernement a produit, en cours de procédure, ses communiqués de presse des 6 mars et 29 juin 2009.

Aux termes du communiqué du 6 mars 2009 et en résumé, le Gouvernement informe de l'ouverture d'enquêtes disciplinaires à l'encontre d'une trentaine de collaborateurs, en raison de la consultation par ceux-ci de sites non-professionnels, notamment à contenu pornographique, consultations mises en évidence par des investigations intervenues suite à différents problèmes techniques rencontrés sur le réseau informatique cantonal. Il convient de relever qu'aucun nom de collaborateur n'était divulgué. La fonction des membres de la fonction publique ou les services concernés n'étaient pas non plus révélés.

Lors de son communiqué du 29 juin 2009, le Gouvernement a donné connaissance du résultat des enquêtes disciplinaires. En substance, il relatait que des sanctions disciplinaires, allant de graves à légères, avait été prises, sous réserve de trois cas pour lesquels il avait été renoncé à prononcer une sanction. Aucun collaborateur n'avait dû être dénoncé à la justice pénale. Parmi les cas les plus graves, trois collaborateurs avaient déjà quitté ou allaient quitter sous peu l'administration. A l'instar du communiqué du 6 mars 2009, aucun nom, service ou fonction n'étaient cités.

En vertu de l'article 4 al. 1 de la Loi cantonale sur l'information et l'accès aux documents officiels (ci-après LInf), les autorités ont l'obligation de communiquer régulièrement et spontanément des informations sur leurs activités et leurs projets. Dans une décision du 1er septembre 2004 de l'autorité de céans, il a été considéré qu'un rapport d'audit mettant en évidence les disfonctionnements d'un service étatique était un document soumis à la LInf, la notion d'information se rattachant à l'accomplissement d'une tâche publique devant être comprise dans un sens large, à savoir dès lors qu'elle se rapporte à l'organisation, au fonctionnement ou aux activités des administrations et services publics (RJJ 2004, p. 228, consid. 3.1.1). Dès lors, le principe de la communication par le Gouvernement au sujet des disfonctionnements intervenus, fin 2008 et début 2009, au sein de la fonction publique, en rapport avec la navigation Internet d'une trentaine de collaborateurs, et des mesures disciplinaires qui s'en sont suivies trouve donc sa base légale dans l'article 4 LInf précité.

S'agissant des modalités d'une telle communication, dans sa décision du 1er septembre 2004, la CPD a relevé que le droit à la protection des données primait le droit à l'information et à la consultation des documents officiels. En particulier, la communication ne doit pas contenir des informations et des appréciations concernant des personnes déterminées, citées par leurs noms ou identifiables en raison des références aux fonctions qu'elles assument, ainsi qu'au sujet du comportement de celles-ci. Dans le cas du rapport d'audit traité par la CPD, l'autorité de céans avait ainsi nié le droit d'obtenir, sur la base de l'article 5 al. 4 LInf, la production du rapport en question. En revanche, il avait été tenu pour admissible au regard de la LPD que le contenu essentiel du rapport d'audit soit communiqué dans les limites prévues à l'article 4 al. 2 LInf, permettant à l'autorité de fournir des renseignements écrits sous forme anonymisée pour pallier l'interdiction ou l'impossibilité de publier le document (RJJ 2004, p. 231 ss consid. 3.2.1 et 3.2.2).

Au cas d'espèce, force est de constater que les communiqués des 6 mars et 29 juin 2009 du Gouvernement respectent les principes dégagés par la jurisprudence précitée, notamment en ne citant aucun nom, ni les fonctions des personnes impliquées, et se limitant à donner les lignes essentielles de l'affaire disciplinaire de grande ampleur dont il était saisi, ainsi que du résultat de celle-ci. Il en va de même, d'ailleurs, de la communication interne du 6 mars 2009.

Au demeurant, toujours aux termes de sa décision du 1er septembre 2004, la CPD a retenu que, lorsqu'il s'agit de personnes occupant des fonctions officielles importantes, la mise en cause de celles-ci pouvait tomber dans la sphère publique (RJJ 2004, p. 232, consid. 3.2.2) et il n'était pas déterminant que ces personnes aient pu être identifiées en dépit de l'anonymisation des renseignements donnés. Le principe dégagé par la jurisprudence de la CPD à ce sujet pourrait s'appliquer aux deux requérants, vu les fonctions de magistrat et de secrétaire du Parlement qu'ils occupaient.

Enfin, s'agissant des informations parues dans la presse en sus des renseignements fournis par le Gouvernement dans ses communiqués, notamment celles publiées dans l'édition du « Matin » du 12 mars 2009 révélant les noms des trois magistrats impliqués, de même que les informations dont disposaient apparemment des tiers avant même que l'affaire ne soit rendue publique par le Gouvernement, celles-ci résultent vraisemblablement de fuites qui peuvent représenter la violation d'un secret de fonction, au sens de l'article 320 CP, et non d'une communication par un organe étatique au sens de la LPD. Il n'appartient pas à la CPD d'instruire dans ce sens.

7. En vertu de l'article 46 LPD, il n'est pas perçu de frais ni émolument dans le cadre d'une procédure devant la CPD.

Dans la mesure où la CPD intervient en qualité d'instance spéciale de la juridiction administrative (art. 4 al. 2 litt. c CPA) et les requérants obtenant gain de cause sur l'essentiel de leurs requêtes, il y a lieu d'allouer une indemnité de dépens aux requérants représentés par un mandataire professionnel, conformément à l'article 224 CPA (RJJ 2006, p. 94s, consid. 5).

PAR CES MOTIFS

La Commission cantonale de la protection des données

constate

1. que les analyses des fichiers journaux d'accès Internet et index.dat des postes informatiques des membres de la fonction publique, dont ceux des trois requérants, en vue d'identifier les postes informatiques ou leurs utilisateurs à l'origine de connexions à des sites Internet à caractère pornographique, respectivement le nom des sites consultés par les membres de la fonction publique, le nombre et les horaires de connexions de ceux-ci, analyses effectuées fin 2008 et début 2009 par le Service de l'informatique ou la société SCRT sàrl sur mandat du Service de l'informatique, sont intervenues avant que les autorités compétentes ordonnent l'ouverture d'enquêtes disciplinaires et sans instruction des mêmes autorités ; que ce traitement de données était illicite, le Service de

l'informatique de la République et Canton du Jura n'étant pas compétent pour décider de placer les membres de la fonction publique sous surveillance informatique ;

2. que la recherche et l'enregistrement des preuves des consultations de sites à caractère pornographique dans les fichiers index.dat, effectués au moyen d'une prise en main à distance des postes informatiques des membres de la fonction publique suspectés d'utilisation abusive d'Internet, dont ceux des trois requérants, tout en cachant la nature exacte de cette opération à l'utilisateur ou en prétextant un motif de télémaintenance, contrevenaient au principe de la bonne foi ; que cette recherche et cet enregistrement de données étaient de ce fait illicites au sens de la LPD ;

ordonne

la destruction par le SDI de toutes les données collectées, fin 2008 et début 2009, au moyen de la prise en main à distance des postes informatiques des membres de la fonction publique, dont ceux des trois requérants ;

ordonne

1. l'interdiction de toute analyse des fichiers journaux ou des fichiers index.dat pouvant être mise en relation avec des postes informatiques des membres de la fonction publique ou leurs adresses IP qui n'interviendrait pas dans le cadre d'une procédure de mutation, de résiliation ou de suspension au sens de la Loi sur le personnel de l'Etat, respectivement d'une procédure disciplinaire au sens de la Loi d'organisation judiciaire s'agissant de magistrats de l'ordre judiciaire, et sur instruction de l'autorité compétente pour mener de telles procédures ;
2. l'interdiction de toute collecte de données qui serait effectuée au moyen d'une prise en main à distance des postes informatiques des membres de la fonction publique, sans qu'il soit indiqué à la personne concernée la finalité exacte du traitement de données ;

rejette

pour le surplus, les conclusions des requérants ;

dit

que la procédure est gratuite ;

alloue

1. au requérant Z. une indemnité de dépens par Fr 4'593.05 TTC, à verser par l'Etat ;
2. au requérant X. une indemnité de dépens par Fr 6'904.60 TTC, à verser par l'Etat ;

informe

les parties du fait que la présente décision est susceptible de recours auprès de la Cour administrative du Tribunal cantonal (art. 45 LPD), dans les 30 jours dès sa notification (art. 121 CPA). Le recours contiendra des conclusions, des motifs ainsi que les moyens de preuve et les titres éventuels seront joints, conformément aux articles 126ss CPA.

ordonne

la notification de la présente décision :

- au requérant Z., par son mandataire, Me Alain Schweingruber, avocat à Delémont ;
- au requérant Y. ;
- au requérant X., par son mandataire, Me Jean-Marie Allimann, avocat à Delémont ;
- au Gouvernement de la République et Canton du Jura, Hôtel du Gouvernement, 2800 Delémont ;
- au Service de l'informatique, Route de Moutier 109, 2800 Delémont ;
- à la Cour administrative du Tribunal cantonal, Le Château, 2900 Porrentruy.

Porrentruy, le 29 mars 2012

AU NOM DE LA COMMISSION CANTONALE DE LA PROTECTION DES DONNEES

Le président a.h. :	**La secrétaire :**
Olivier Vallat	Gladys Winkler Docourt