REQUERIMENTO DE INFORMAÇÕES

Relacionadas aos dados pessoais coletados e tratados pelos meios telemáticos de comunicação e ensino, bem como sobre medidas de segurança de informação adotadas por esta Universidade.

1. Considerações preliminares

Ainda que a Lei de Acesso à Informação seja assente na desnecessidade de justificar-se o pedido de informações, a requerente compreende que importa tecer algumas considerações preliminares. Com a ocorrência da pandemia de Covid-19, notoriamente a universidade passou a adotar medidas de ensino à distância, com a realização de classes virtuais e grande fluxo de informações sendo transacionadas via plataformas cibernéticas.

Nesse aspecto, informações de interesse público não restaram devidamente publicizadas, obstando a realização de controle social sobre a Administração Pública no aspecto. Isso porque os atos e decisões administrativas que consignaram a respeito dos procedimentos da modalidade remota de educação não são transparentes, carecendo de informações fundamentais para a averiguação do respeito às garantias dos servidores e alunos da instituição. Especificamente, a Universidade deixou de dar publicidade para questões referentes aos protocolos de proteção de dados pessoais e de segurança de informações científicas.

Assim, deve-se ter em vista que a Lei de Acesso à Informação prevê, em seu art. 1º, parágrafo único, inciso II, que as Autarquias submetem-se ao regime de Acesso à Informação. Nesse ínterim, considerando que não foram alcançadas informações sobre os serviços e plataformas que intermedeiam as aulas virtuais, bem como sobre as formas de tratamento das informações pessoais e científicas, faz-se necessário o presente pedido de acesso a informações, com fulcro nos arts. 10 e 11 da Lei 12.527/2011.

Os requerimentos levam em consideração a necessidade de observância da realidade que se impõe, de fluxo e captação de dados pessoais consoante prediz a Lei Geral de Proteção de Dados, cujas disposições merecem desde já observância, considerando que os contratos referentes a plataformas e serviços virtuais, bem como o manejo de dados coletados agora na universidade, perdurarão até sua entrada em vigor. Nesse sentido, espera-se que as respostas levem em consideração os conceitos trazidos pela LAI, pelo Marco Civil da Internet e pela Lei Geral de Proteção de Dados, no que toca o tipo de dados, a titularidade dos mesmos, o tratamento, o descarte, os princípios, as responsabilidades do controlador e operador do tratamento, entre outros, conforme requerido.

2. Dos requerimentos

Isso exposto, a Associação dos Docentes da Universidade de São Paulo – ADUSP solicita saber:

2.1 No que toca às plataformas usadas para aulas virtuais e outras formas de comunicação entre docentes e alunos:

Dos agentes de coleta e tratamento de Dados:

1) Qual(is) programa/software(s) é(são) utilizado(s) para qual tipo de atividade remota (realização de aulas por meio telemático, troca de emails, entre outros);

A STI privilegia uma diversidade de ferramentas para uso pela comunidade USP e as Unidades têm completa autonomia para escolha e uso de ferramentas de apoio.

Em relação ao apoio e suporte ao ensino a distância podemos citar o e-disciplinas (Moodle), o Classroom e Sistema de Aprendizado Eletrônico – AE USP. Para reuniões (e também aulas online): Google Meet, Conferência Web (Mconf), Microsoft Teams, Webex, Zoom, Jitsi Meet. O domínio @usp.br e os domínios de algumas unidades utilizam o correio eletrônico do Google For Education.

Mais informações sobre as ferramentas podem ser conseguidas em http://faq.sti.usp.br.

2) Qual(is) empresa(s) é(são) fornecedora(s) dos serviços, com indicação se as mesmas são nacionais ou estrangeira;

Entre os fornecedores de serviços estão a Google LLC (estrangeira), a Microsoft Corporation (estrangeira), a WebEx Communications Inc. (estrangeira) e a Zoom Video Communications, Inc. (estrangeira). O Moodle, o MConf e o Jitsi são aplicações de software livre.

3) O inteiro teor do contrato com a(s) empresa(s) prestadora(s) dos serviços e se houve licitação, incluindo indicação do valor e duração dos serviços contratados;

Vide processo 16.1.55.84.8 (enviar cópia do processo em anexo).

4) Se é necessário cadastro individual dos usuários docentes e alunos para utilização dos serviços;

Para serviços que têm suporte direto da USP, há integração do serviço de login e senha da Universidade com as diversas plataformas para acesso e uso quando necessário.

5) Se há avisos sobre a política de privacidade e proteção de dados e possibilidade de opção op out, com uso do serviço mesmo em desacordo de alguma cláusula;
6) o teor integral da política de privacidade e proteção de dados da empresa operadora/prestadora do serviço;

5-6) Cada prestador de serviço possui suas próprias políticas que normalmente são disponibilizadas quando do acesso aos serviços.

7) se a Universidade investe em servidores próprios e quanto;

Sim. As Unidades têm autonomia para manter seus parques computacionais. Apenas na STI, para 2021, há previsão orçamentária de R $3.000.000,00 (três milhões de reais) para a interNuvem (Nuvem USP). Informações adicionais sobre o histórico de aquisição de servidores próprios podem ser encontradas no processo 2012.1.15615.1.8. Além disso, informações sobre a interNuvem USP podem ser encontradas em: http://www.sti.usp.br/competencias/internuvem/

8) Especificamente no caso dos e-mails funcionais, a caixa postal dos professores, técnicos e estudantes da USP é administrada por alguma empresa privada; se os servidores de e-mail da universidade estão hospedados nas dependências da USP ou em servidores de empresas privadas; em não sendo na USP, onde e com quais protocolos de segurança;

As Unidades têm autonomia para gerir seus próprios domínios de correio eletrônico. No caso do domínio @usp.br e domínios de algumas unidades que utilizam o correio eletrônico do Google For Education administrado em conjunto com a Superintendência de Tecnologia da Informação, os procedimentos seguem o contrato estabelecido com a Google Inc.

Da coleta de dados, do tipo de tratamento e do armazenamento:

9) Se a universidade possui o levantamento de quais tipos de dados e concernentes a quais titulares são coletados e tratados no processo de aulas virtuais, de troca de e-mails e outros, se houver; se sim, quais são;

10) Qual a finalidade da coleta e tratamento, e se é observado o princípio da minimização;

11) quais as bases legais para cada finalidade de tratamento;

12) Se esses dados são usados por terceiros – ou compõem base de dados sobre o qual terceiro tem acesso; Se sim, quem é o terceiro; Se sim, o terceiro usa para qual finalidade e com fulcro em qual base legal;

13) Quais são os protocolos de segurança de informação usados pelo sistema e pelo servidor do controlador e do operador do tratamento de dados pessoais;

14) Qual é o período de armazenamento de cada tipo de dados e o porquê do estabelecimento de cada período indicado;

15) Onde e como os dados são armazenados e se é possível a portabilidade dos dados para outra empresa/servidor, caso a universidade deseje;

16) Se os dados são tratados ou armazenados em no Brasil ou em território estrangeiro;

17) Se há política de descarte de dados, e se o titular do dado pode requerer a retificação ou o descarte;

18) se houve análise de risco sobre o processo de coleta e tratamento de dados;

19) quais medidas e mecanismos voltados a mitigar os riscos identificados, por parte do controlador e do operador de dados;

20) como é feito o processo de tratamento de dados pessoais que podem gerar riscos aos titulares e que possam impor restrições não previstas em lei aos usuários de serviços públicos, conforme previsto na LGPD e decorrente do sistema normativo protetor dos consumidores e dos usuários de serviços públicos (art. 6º, I e III, do CDC; Art. 5º, inc. IV,CDUSP; art. 7º, V, da Lei Estadual 10.294/1999;

21) se o controlador e o operador de dados possuem um protocolo de acesso com graus de privilégios de acesso;

22) se e como é feita a anonimização e a guarda dos dados pessoais;

23) Se há análise sobre o impacto financeiro de eventuais falhas e vazamentos na atividade de troca de informações e armazenamento de dados, considerando como potencialmente afetados os membros da comunidade acadêmica e o desenvolvimento científico do país;

24) como é feita a governança do banco de dados decorrente dos tratamentos realizados;

25) qual a forma e frequência de atualização de referido banco de dados;

26) quem tem acesso aos dados pessoais coletados e quais são os graus de privilégios de acesso, tanto em relação ao controlador, ao operador e a terceiros, se houver;

27) Como é feita a anonimização dos dados pessoais;

9-27) Dado a relevância, o impacto e a abrangência da nova Lei Geral de Proteção de Dados, a Universidade, já há tempo preocupada com o tema, está envidando esforços em diversos sentidos visando adequar-se à nova realidade. Entre outras medidas, está em andamento a criação da Agência USP de Proteção e Divulgação de Dados (AUPD). Um Grupo de Trabalho foi criado pela Portaria do Reitor (430) de 10-12-2020, publicada no DO em 11/12/2020,

Desta forma, os questionamentos de 9 a 27 deverão ser submetidos à Agência para análise detalhada.

2.2 Sobre as informações funcionais dos docentes:

28) que tipo de informações dos docentes são coletadas pela universidade e onde são armazenadas (servidores próprios ou de empresas contratadas);

29) se as bases de dados que armazenam informações pessoais e funcionais, informações de pesquisas científicas e informações de comunicações virtuais entre docentes e discentes são operadas e controladas pela universidade ou por outros;

30) em sendo por terceiros, quem são e qual o teor dos contratos com a prestadora do serviço;

31) se, além do prestador de serviço, as bases de dados são acessadas por terceiros para alguma finalidade específica;

32) quais informações dos alunos compõem a base de dados;

33) se as informações de cunho de propriedade intelectual, científica e de patente possuem qual processo de tratamento específico;

34) qual a forma e frequência de atualização de referido banco de dados; 35) se há um protocolo de acesso com níveis de privilégios de acesso, tanto em relação ao controlador, ao operador e a terceiros, se houver;

36) como é feita a anonimização dos dados pessoais;

37) se os docentes e discentes têm acesso às suas informações, e se podem realizar a retificação e solicitar o descarte das mesmas; quais são os procedimentos para tanto;

38) Se há análise sobre o impacto financeiro de eventuais falhas e vazamentos na atividade de troca de informações e armazenamento de dados, considerando como potencialmente afetados os membros da comunidade acadêmica e o desenvolvimento científico do país;

39) como é feita a governança do banco de dados de informações científicas;

40) quem é o controlador dos dados? Quais critérios de segurança do armazenamento, usos, formas de acesso e mecanismos de controle social da sua utilização com fundamento e base legal nas finalidades indicadas;

41) Se há compartilhamento da base de dados com outras entidades estatais e/ou privadas; se sim, quais;

42) se há parâmetros de confiabilidade da segurança de informação usados pelo sistema e pelo servidor do controlador de dados e do operador;

28-42) Como apontado acima, o tratamento de dados pessoais, mormente os dados funcionais de docentes, é questão de grande relevância para a Universidade, que está avançando na criação de uma agência específica para tratamento de dados e informações, a quem caberá a análise e adequação dos processos existentes aos preceitos da nova Lei Geral de Proteção de Dados.

Assim, os questionamentos de 28 a 42 deverão ser encaminhados à Agência USP de Proteção e Divulgação de Dados (AUPD) para análise detalhada.