

Relatório de participação

Reunião: Comitê de Políticas para a Economia Digital (CDEP) da OCDE

Data e local: Paris, 15 a 19 de maio de 2017

Participante: Ministro Carlos da Fonseca (Ministério das Relações Exteriores)

Realizaram-se, em Paris, entre 15 e 19 de maio passado, as reuniões semestrais do Comitê de Políticas para a Economia Digital (CDEP) da OCDE e seus respectivos grupos de trabalho (SPDE, CISP e MADE). O Brasil foi representado pelo Ministro Carlos da Fonseca, do Ministério das Relações Exteriores.

GRUPO DE TRABALHO SOBRE SEGURANÇA E PRIVACIDADE NA ECONOMIA DIGITAL (SPDE) - 15 de maio

a) DIGITAL ECONOMIC OUTLOOK (DEO) 2018/19

2. O GT discutiu a renovação do DEO, que se dá a cada dois anos, especialmente no que se refere aos temas de segurança e privacidade. Salientou-se a dificuldade para obtenção de informações detalhadas, por parte dos países membros, no que tange a incidentes de segurança digital. Para paliar o problema, o secretariado desenvolveu novo modelo de questionário ("survey"), que simplifica aquele utilizado em edições anteriores, e que será aplicado para a próxima edição do DEO.

3. Quanto ao resultado do último "survey", conduzido ao longo de 2016, o secretariado realizou apresentação sobre desdobramentos recentes nos países membros em matéria de segurança e privacidade. O foco central da enquete disse respeito às estratégias de segurança digital, concluídas ou em elaboração.

4. 33 dos 35 países membros da OCDE responderam ao questionário. Desses, 29 já possuem uma estratégia nacional para segurança cibernética, estando os demais em fase final de formulação. Em paralelo, 28 países possuem políticas de incentivo à produção de soluções técnicas para segurança cibernética pela indústria nacional. No que se refere à importância da cooperação internacional, alguns países já estabeleceram a figura do "embaixador para segurança

digital", e a maioria prioriza atividades conjuntas de "capacity building" e gestão de segurança.

5. No que tange à privacidade, 34 países responderam ao questionário, dos quais 25 afirmaram possuir políticas públicas específicas, e 30, uma legislação nacional exclusiva. Apenas 16 informaram possuir estratégias nacionais em matéria de privacidade, ao passo que nove outros afirmaram encontrar-se em estágio preparatório. 33 países disseram possuir uma agência nacional para aplicação de medidas em prol da privacidade de dados. No que se refere a essas medidas, destacaram-se aquelas voltadas para educação, conscientização, transparência e "empoderamento" do usuário, por meio da portabilidade de dados.

6. Capítulo específico do DEO (5º) trata do impacto da confiança digital no comércio digital. Pesquisas conduzidas pela Comissão Europeia, com apoio da OCDE, dão conta de que 60% dos cidadãos da UE se dizem preocupados com o ambiente digital (na Alemanha, 80%). 50% declararam haver deixado de realizar transações no último ano em razão de falta de segurança digital. 30% das empresas entrevistadas declararam que, pelas mesmas razões, não utilizam computação em nuvem. Em Portugal, essa proporção chega a 45%.

7. Entre os consumidores, a relação de desconfiança é proporcional ao nível de educação. Número maior de incidentes é identificado entre usuários com maior nível de escolaridade, o que se pode explicar pela maior intensidade do uso da rede. Da mesma forma, a notificação de incidentes de segurança é maior no caso de empresas de grande porte. Há poucas notificações por parte de PMEs, o que não significa necessariamente um número menor de incidentes; poderia, antes, refletir ausência de políticas específicas para gestão de privacidade e segurança digital.

8. A pesquisa relacionou o nível de confiança e a intensidade de uso comercial da Internet à capacidade de o usuário controlar seus próprios dados, o que ocorre com maior frequência em países da Europa Ocidental. Entre os países pesquisados, a Turquia foi o que apresentou piores resultados nesse quesito.

9. Finalmente, a pesquisa detectou aumento significativo na demanda dos usuários por treinamento e/ou serviços relacionados à gestão de riscos de privacidade e segurança digital, em níveis muito superiores à capacidade de oferta de tais serviços.

10. O representante brasileiro comentou acerca dos efeitos dos ataques do crypto-ransomware "WannaCry", iniciados em 12 de maio, especialmente no que diz respeito às empresas de telefonia móvel, que geraram grande insegurança nos usuários, pelo fato de, potencialmente, ameaçarem os serviços de dados móveis. O secretariado do SPDE ponderou que, de modo geral, os ataques geram externalidade negativa em confiança digital que atinge todos os usuários, mesmo quando o ataque não afeta diretamente o consumidor. Usando como exemplo o roubo de cartões de crédito "online", salientou que a reação do usuário é de desconfiar de todos os cartões, inclusive os que não sofreram ataques. A situação apresentaria desafio de ordem sistêmica, uma vez que ataques pontuais tendem a gerar efeitos generalizados de desconfiança na rede.

b) REVISÃO DA RECOMENDAÇÃO SOBRE PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS DE INFORMAÇÃO (CIIP)

11. Em 2016, teve início processo de revisão da Recomendação, adotada em 2008, de forma a alinhá-la com o conteúdo da "Recomendação sobre Gestão de Segurança de Risco Digital" (2014). Na prática, isso significa agregar, ao documento de 2008, conceitos como os de "transformação digital da sociedade" e "gestão de risco de segurança digital", além de acrescentar referências às melhores práticas adotadas nos últimos anos em termos de proteção de CIIP. Para tanto, novo questionário, ora em elaboração, deverá abordar questões como as novas regulamentações nacionais em matéria de segurança de infraestruturas críticas.

12. O secretariado do SPDE organizou mesa redonda sobre o tema, com participação de representantes da Agência Internacional de Energia e dos governos francês e alemão, que informaram sobre as iniciativas adotadas em ambos os países.

c) REVISÃO DA RECOMENDAÇÃO DO CONSELHO SOBRE CRIPTOGRAFIA (1997)

13. O Secretariado da OCDE tem-se empenhado, há alguns anos, em promover revisão da Recomendação, que data de 1997 e cujo teor prevê reavaliação a cada cinco anos - o que nunca aconteceu, em boa medida, por oposição dos Estados Unidos.

14. Durante as discussões sobre o instrumento, o representante brasileiro destacou que, embora o País já tenha decidido aderir a série de Recomendações da OCDE na área digital, no caso da Recomendação em tela, a adesão não poderia ser confirmada, no momento, em razão da inclusão de dispositivos que versam sobre matéria controversa, ainda não pacificada internamente.

d) PROJETO DE RECOMENDAÇÃO EM MATÉRIA DE SEGUROS PARA RISCO DIGITAL

15. Os membros do SPDE foram convidados a discutir projeto de Recomendação sobre apólices de seguro para incidentes de segurança digital ora sob consideração do Comitê de Finanças.

16. A questão de fundo de que tenciona tratar o instrumento é a contribuição a ser oferecida pelo mercado de seguros para a gestão de risco de segurança digital. Entre os aspectos destacados, estão: (a) troca de experiências e melhores práticas; (b) incentivo a investimentos em tecnologias de segurança digital, associados a uma proporcional redução dos prêmios de seguro pagos por empresas que realizem tais investimentos; e (c) levantamento sistemático do risco digital em empresas, com potenciais consequências em termos de elevação dos prêmios de seguro.

17. O projeto de Recomendação, que ainda não tem data para aprovação, oferece uma classificação tanto dos incidentes cibernéticos como das perdas cibernéticas ("cyber losses"). Há quatro categorias de incidentes: violação da confidencialidade de dados; mau funcionamento dos sistemas; ataque à integridade de dados; e atividade criminosa ("malicious activity").

18. Entre os principais problemas que enfrenta o setor estão: (a) o custo das apólices, em geral mais caras do que no mercado de seguro tradicional (até 6 vezes mais do que prêmios pagos por seguros sobre propriedades); (b) os novos desafios que representam desenvolvimentos como a Internet das Coisas e a computação em nuvem, em termos de multiplicação das vulnerabilidades "online"; e (c) a dificuldade de avaliação dos prêmios de seguro, que podem variar substancialmente, a depender do serviço oferecido pela empresa segurada. No exemplo apresentado, uma empresa de serviços de saúde com plataforma digital pagaria seguro muito mais elevado do que uma empresa de vendas "online", em razão

da quantidade e sensibilidade das informações por ela controlada, e do potencial de violação de dados.

19. Os membros do SPDE poderão contribuir para a elaboração da Recomendação sobre Seguros para Risco Digital até o final de setembro próximo, quando uma primeira versão do instrumento será submetida à avaliação do Comitê de Finanças.

GRUPOS DE TRABALHO SOBRE SEGURANÇA E PRIVACIDADE NA ECONOMIA DIGITAL (SPDE), MEDIÇÃO E ANÁLISE NA ECONOMIA DIGITAL (MADE) E CONECTIVIDADE E INFRAESTRUTURA (CISP) - 16 de maio

a) REUNIÃO CONJUNTA SPDE/MADE

Workshop sobre aprimoramento de métricas aplicadas a incidentes de segurança digital ("improving measurement of digital security incidents")

20. O seminário teve como principal objetivo discutir o desenvolvimento e o aprimoramento de métricas aplicáveis à análise de incidentes de segurança cibernética, com foco na elaboração de pesquisas ("surveys") e nas políticas voltadas à notificação de incidentes por parte de empresas. Participaram, como palestrantes, representantes do governo do Reino Unido e da "International Conference of Data Protection and Privacy Commissioners" - ICDPPC.

Debate e estudo da OCDE sobre Estratégias Nacionais em privacidade

21. O estudo da OCDE teve como base: (1) diretrizes ("guidelines") definidas em 2013; (2) mandato determinado pela Declaração de Cancún, de 2016; e (3) questionário conduzido em 34 países, também em 2016. Dos 34 países respondentes, 18 ainda não possuem estratégia nacional sobre privacidade e 9 encontram-se em fase de elaboração. 36. As diretrizes de 2013 estabeleceram as bases conceituais prescritas pela OCDE para a elaboração das estratégias. Entre os aspectos mais importantes, a Organização destaca: (1) a necessidade de definir em que nível de governo se estabelecerá a estratégia; (2) a importância de contar com

órgão de supervisão e aplicação, na forma de uma "autoridade nacional" sobre privacidade e proteção de dados ("Data Protection Authority"); (3) a utilidade de se adotarem medidas em matéria de conscientização digital ("digital privacy awareness"); (4) o imperativo de contar com mecanismos de cooperação internacional na matéria, tendo em vista que a maior parte dos incidentes de "privacy breach" ocorre de forma transfronteiriça; (5) e a conveniência de preservar, no estabelecimento de políticas e regras sobre privacidade, equilíbrio entre a abertura de dados, que gera ganhos econômicos, e a privacidade, que gera "ganhos sociais".

Estratégias de proteção e privacidade de dados: Chile e Reino Unido

22. Representante do Chile - país com maior penetração de Internet na América Latina - informou sobre o lançamento, em 27 de abril de 2017, pela Presidente Michelle Bachelet, de "Agenda digital" com medidas de médio e longo prazos (2017-20), entre as quais o estabelecimento de uma estratégia de segurança de dados. Foi criada, na sequência da aprovação da estratégia, agência de proteção de dados e privacidade, vinculada à Presidência da República. Em 20/04, o país havia ratificado a Convenção de Budapeste - o terceiro país da região a fazê-lo.

23. Representante do Reino Unido informou que a Estratégia de "data protection and privacy" britânica, elaborada por entidade independente, seria lançada oficialmente em 25 de maio. Os objetivos principais seriam: (1) incrementar a confiança pública no ambiente digital, por meio da criação de um "accountability framework"; (2) aperfeiçoar os padrões e práticas em matéria de fluxo de informação digital, por meio do desenvolvimento do conceito de "privacy by design" (por oposição a "privacy by default"); (3) elevar o perfil britânico no debate internacional sobre privacidade e segurança de dados; (4) fomentar o desenvolvimento de soluções tecnológicas para segurança digital, especialmente por meio do incentivo à pesquisa em tecnologias emergentes, como o "big data"; e (5) criar instituições para aplicação das novas leis e regras na matéria (agência de privacidade e segurança de dados).

b) REUNIÃO DO GT MADE

Workshop organizado pela UNCTAD sobre indicadores de comércio eletrônico

24. Torbjörn Fredriksson, Chefe da Seção de Análise de TICs da UNCTAD, fez apresentação sobre o tema, ponderando que, no momento em que cresce a pressão em diferentes foros, como a OMC e a OCDE, para discussão do "comércio digital", inclusive na forma de novos acordos de acesso a mercados, a carência de indicadores dificulta uma avaliação sobre os eventuais impactos de tais acordos. Em vista disso, a UNCTAD lançou, durante a "e-Trade Week", em 27 de abril último, iniciativa que visa à produção de métricas harmonizadas voltadas para o comércio eletrônico, em especial as transações B2C e transfronteiriças.

25. A referida iniciativa teria como principais objetivos: (1) promover debate internacional acerca de uma definição comum para "comércio digital"; (2) incentivar o estabelecimento de metodologia aceita internacionalmente para a geração de indicadores e métricas na matéria; (3) incentivar a produção, nos planos doméstico e internacional, de estatísticas detalhadas e confiáveis sobre a proporção de operações comerciais realizadas por meio de dispositivos digitais; e (4) estimular a produção, nos planos doméstico e internacional, de metodologias e indicadores que permitam aferir o volume de operações transfronteiriças de comércio digital. Maiores informações sobre a iniciativa encontram-se no site: <http://unctad.org/en/pages/MeetingDetails.aspx?meetingid=1323>.

c) REUNIÃO CONJUNTA GTs MADE/CISP

Projeto para estabelecimento de indicadores de IoT

26. O secretariado recordou mandato estabelecido pela Declaração de Cancún (2016) para que os GTs MADE/CISP iniciassem projeto com vistas ao estabelecimento de métricas comparáveis para aplicação no ecossistema de IoT. Para tanto, propôs-se discussão inicial, de cunho metodológico, centrada em definições e modelos estatísticos aplicados à IoT, que fossem compatíveis no plano internacional. Com base nesse trabalho inicial, os GTs propoem primeira versão de termos de referência e "survey" para levantamento de informações

sobre os diferentes ecossistemas de IoT no mundo. O trabalho será desenvolvido durante o biênio 2017/19.

27. De forma a ilustrar a importância do tema "IoT metrics", o secretariado promoveu debate com participação de representantes da "IoT UK Nation database" (banco de dados sobre o ecossistema de empresas de IoT no Reino Unido), da "Thingful.net" (instrumento de busca voltado para IoT) e do GSMA.

28. Após as apresentações, as delegações presentes iniciaram debate em torno dos temas e metodologias apresentados. O representante brasileiro questionou aspectos relativos à privacidade de dados e autorização para seu uso, em particular no que se refere aos meios disponíveis para o detentor dos dados para assegurar consentimento bem informado por sistemas como o "Thingful.net".

29. Representantes da Alemanha, Itália e Reino Unido somaram-se ao questionamento, ponderando a dificuldade em aferir se a autorização para uso dos dados deu-se na forma de "active consent" ou "passive consent", ou seja, se o detentor dos dados de fato autorizou o uso ou apenas absteve-se de se manifestar a respeito.

30. Ao final do debate, o Secretariado do Comitê informou que elaborará, até a próxima reunião do CDEP, os termos de referência do projeto, bem como primeira proposta de questionário para o "survey", que levarão em conta os questionamentos acima. Os países membros do Comitê foram convidados a manifestar formalmente o interesse em participar da iniciativa.

COMITÊ DE POLÍTICAS PARA A ECONOMIA DIGITAL (17 A 19 de maio de 2017)

a) REVISÃO DO PROCESSO DE REFORMA MEXICANA EM TELECOMUNICAÇÕES

31. O processo de "peer review", conduzido pelo secretariado do CDEP (GT sobre Conectividade e Infraestrutura - CISP), baseou-se em estudo encomendado pelo governo mexicano, em 2012, que deu origem à reforma do setor de telecomunicações, promovido pelo governo de Enrique Peña Nieto a partir de 2013. Nessa nova revisão, iniciada em 2016, o secretariado

analisou os resultados da reforma. A execução do estudo segue o seguinte cronograma: (1) elaboração de questionário específico (agosto/16); (2) "fact finding mission" ao México (setembro/16); (3) "follow up mission" (dezembro/16); (4) apresentação do "peer review" ao GT CISP (maio/17); (5) elaboração do primeiro rascunho de relatório (junho/17); e (6) divulgação do relatório (setembro/17).

b) REVISÃO DAS ATIVIDADES DOS GRUPOS DE TRABALHO

Agenda SPDE

32. O Comitê aprovou os trabalhos conduzidos durante a reunião do GT SPDE, em especial a análise dos capítulos sobre segurança e privacidade do "Digital Economic Outlook" (DEO); a revisão da Recomendação sobre Proteção de Infraestruturas Críticas de Informação (CIIP), o processo de revisão da Recomendação do Conselho sobre Criptografia, de 1997; e a apresentação do projeto de Recomendação em matéria de "Seguros para Risco Digital". No que se refere à revisão do projeto de Recomendação sobre "Acesso aprimorado a dados" ("Enhanced access to data"), o secretariado do CDEP informou sobre a realização, na Dinamarca, nos dias 30 e 31 de outubro próximo, de reunião para finalização de relatório preliminar e início da redação de uma proposta de revisão formal do instrumento.

Agenda MADE

33. O Comitê aprovou os trabalhos conduzidos durante a reunião do GT MADE, em especial a análise do conteúdo relativo a indicadores e métricas do DEO; os resultados do Workshop sobre aprimoramento de métricas aplicadas a incidentes de segurança digital ("improving measurement of digital security incidents"); os resultados da discussão sobre indicadores de comércio eletrônico, inclusive a sugestão da UNCTAD, acatada pelo Comitê, de criação de um GT interinstitucional para propor metodologias de consolidação estatística e construção de um sistema de métricas aplicável, de maneira global, ao comércio digital; além das conclusões do relatório sobre "Determinantes e Impactos da Automação" na indústria e no emprego ("Determinants and Impact of Automation"), apresentado em reunião anterior do GT MADE.

Agenda conjunta MADE/CISP

34. O Comitê aprovou os trabalhos conduzidos durante a reunião conjunta dos GTs MADE e CISP, em especial a proposta de estudo sobre indicadores e métricas para IoT. O delegado brasileiro reiterou sua preocupação quanto à necessidade de incorporar-se ao projeto uma dimensão de privacidade/segurança de dados, em especial no que se refere à questão da autorização prévia para uso de informações geradas por equipamentos de IoT. Sugeriu, nesse sentido, fosse o GT SPDE somado ao projeto, de forma a que a metodologia a ser definida incluísse aspectos e temas de sua competência. O Presidente do CDEP reconheceu a importância dessas questões e informou que os três GTs deverão reunir-se para deliberar sobre a melhor maneira de incorporá-las ao projeto.

c) PROJETO "GOING DIGITAL"

35. O secretariado informou o Comitê acerca da evolução do projeto, anunciado, como se recorda, durante a reunião do CDEP de novembro de 2016 (à época, intitulava-se "Horizontal Project: Seizing the Benefits of Internet for Growth and Well Being"). O lançamento oficial do "Going Digital" ocorreu em Berlim, em 12 de janeiro de 2017, durante a primeira reunião da Força Tarefa sobre Economia Digital do G20, em seminário que contou com presença de 250 pessoas. Desde então, várias atividades foram realizadas, com destaque para a primeira reunião do "Grupo de Especialistas", em 5 de abril. Sobre a governança do projeto, informou-se que o "Grupo de Amigos", que já manteve dois encontros, será liderado por México e Reino Unido. O "Steering Committee", por sua vez, será encabeçado por Japão e Portugal, e deverá reunir-se em 20 de novembro. Como resultados do "Going Digital", espera-se que um primeiro relatório contendo conclusões nos três pilares propostos seja apresentado na reunião do Conselho de Ministros, de 2018. Ademais, estão previstas a elaboração de um "toolkit", a organização de mesas redondas nacionais e regionais, com vistas a apoiar o desenvolvimento de estratégias digitais, além da formulação de uma ou mais Recomendações do Conselho da OCDE em matéria de transformação digital.

36. Na sequência, o secretariado propôs discussão acerca dos vetores de análise a serem empregados na metodologia do "Pilar 1" ("Framework for analyzing digitalisation"). O primeiro vetor ("scale without mass") diz respeito à questão da concentração de mercados na economia digital, distorção provocada pelo peso econômico do "fluxo de dados" (bens intangíveis). Empresas como o WhatsApp, por exemplo, possuíam, no momento de sua compra pelo Facebook, 300 milhões de usuários e uma movimentação de mensagens da ordem de 50 bilhões por dia, com uma equipe de apenas 55 funcionários. Da mesma forma, o Netflix conta um faturamento de quase US\$ 9 bilhões anuais e somente 3500 funcionários. Já o Dropbox soma 500 milhões de usuários, 1,2 bilhão de documentos arquivados e apenas 1200 empregados. Tais circunstâncias apresentariam enormes desafios para os governos nacionais, especialmente em termos de políticas de concorrência.

37. O segundo vetor ("soft capital") diz respeito à possibilidade tecnológica de equipamentos de IoT, associados a dispositivos analógicos, passarem a gerar dados, dos quais se podem extrair informações, com valor econômico específico. Assim, por exemplo, tratores já não cuidariam apenas de arar a terra, passando a reunir em seus sensores conjunto de informações essenciais sobre condições do solo, regime pluviométrico, etc. Novos modelos de automóveis, por sua vez, já reuniriam dezenas de sensores, com potencial para produzir informações sobre condições de trânsito, movimentação do usuário (controlada por GPS), qualidade de ruas e estradas, etc. Esse cenário, no qual bens e serviços tendem a confundir-se, apresenta desafios aos formuladores de políticas públicas em termos de privacidade e segurança de dados, mas oferecem também oportunidades para o uso dos dados gerados em políticas sociais.

38. O terceiro vetor ("intelligence at the edges") diz respeito à crescente tendência à desconcentração do acesso a notícias e informações. Contrariamente ao modelo tradicional de mídia ("one to many"), no qual um veículo transmitia notícias para muitos leitores, no sistema atual ("many to many"), as chamadas mídias sociais distribuem de forma descentralizada, e muitas vezes sem nenhum tipo de controle, notícias de qualidade duvidosa a uma massa cada dia maior de leitores acríticos. A intensificação dos casos de "fake news" é apenas um dos desdobramentos dessa situação.

d) REVISÃO DA RECOMENDAÇÃO DO CONSELHO SOBRE TICs e MEIO

AMBIENTE

39. Graham Vickery, consultor do Comitê, apresentou relatório preliminar sobre a evolução de políticas públicas em matéria de TICs e meio ambiente, desde a aprovação da Recomendação, em 2010, bem como modelo de questionário para ensejar eventual revisão do instrumento. Foi solicitado ao Comitê deliberar sobre ambos os documentos.

40. O instrumento de 2010 elenca dez recomendações específicas, entre as quais: coordenação de políticas públicas em matéria de energia, meio ambiente e TICs; adoção de perspectivas de ciclo de vida; apoio a P&D em tecnologias e serviços "verdes"; desenvolvimento de habilidades em TICs ("ICT skills") com foco ambiental; estímulo à conscientização pública em relação ao papel ambiental das TICs; adoção de melhores práticas em tecnologia e meio ambiente, tanto por parte de empresas como dos governos ("leading by example"); e aperfeiçoamento das políticas públicas em matéria de compras governamentais, de forma a que contribuam para a contratação de tecnologias e serviços ambientalmente neutros.

41. Ao avaliar resultado de pesquisas realizadas junto aos membros da OCDE, Vickery salientou os seguintes bons resultados, associados à aplicação das recomendações do Instrumento: (1) o papel das TICs é cada vez mais reconhecido pelos governos como contribuição para suas políticas públicas ambientais; (2) observa-se um envolvimento crescente de autoridades de diferentes áreas de governo, (econômicas, C,T&I, desenvolvimento e meio ambiente); (3) nota-se, por outro lado, uso crescente das novas tecnologias em "smart applications", com consequências positivas em termos ambientais (sensores de qualidade do ar, aplicativos para uso em "smart cities" e "smart agriculture", etc).

42. Como próximas etapas do cronograma, o secretariado propôs o mês de junho para envio de comentários ao novo questionário; o mês de setembro para envio de respostas ao novo questionário; a próxima reunião do CDEP para apresentação das conclusões preliminares; o mês de fevereiro de 2018, para apresentação do relatório-síntese, sugerindo (ou não) a revisão do instrumento; e a reunião de CDEP de maio de 2018, para a discussão final sobre a revisão da Recomendação.

43. As próximas reuniões dos GTs SPDE, MADE e CISP estão previstas para ocorrerem na semana de 30 de outubro a 3 de

novembro de 2017. Excepcionalmente, o próximo encontro do Comitê não se dará na sequência dos GTs, e sim nos dias 21 e 22 de novembro próximo.