GUIA DE ESTUDOS

ORGANIZAÇÃO INTERNACIONAL DE POLÍCIA CRIMINAL

STSC

SÃO PAULO

2016

SUMÁRIO

CARTA DE APRESENTAÇÃO

Caros representantes,

Quando o comitê da Interpol foi escolhido durante as reuniões do Secretariado, admito que fiquei com muita vergonha por não ter pesquisado mais a fundo o tema sugerido. Originalmente, o tópico a ser debatido era referente à inconstitucionalidade da espionagem política no Artigo 3º da Constituição (parece até que estou falando grego). Mal nós sabíamos que essa questão é complexa demais para dois dias de debate e praticamente foi resolvida algumas décadas atrás. Porém, levando em consideração os recentes acontecimentos da mídia internacional, acreditamos ser muito proveitosa a questão do gerenciamento de dados pessoais por governos e empresas.

Atualmente, a segurança pública, especialmente no espaço virtual, gera muitas dúvidas à medida que novas tecnologias surgem e desenvolvem-se. Biometria, scanners, criptografia, inteligências artificiais e outras invenções podem parecer coisas de ficção científica, mas a maioria delas já são mais do que realidade, são cotidianas. Apesar da proteção virtual e a segurança de dados terem sido de grande auxílio para instituições, programas governamentais e indivíduos, estas características são vistas hoje mais como um obstáculo do que como um suporte.

Em abril de 2016, a comunidade internacional observou de perto as tensões entre a Apple Inc. e a Federal Bureau of Investigation (FBI) enquanto esta última tentava hackear um aparelho portado pelo suspeito de um ato homicida no estado da Califórnia. No final, a investigação continuou com os agentes invadindo o software mesmo sem o auxílio da empresa e sem maiores repercussões. Episódios como este nos levam a pensar se realmente estamos protegidos e, ainda mais importante, em quem devemos confiar. Seriam as corporações e conglomerados multinacionais os protetores das informações cedidas de bom grado para seu uso? Ou será que estamos mais seguros se o governo tivesse acesso a essas informações e usasse em cortes de justiça e investigações?

Seguindo esta linha de pensamento, gostaríamos de dar as boas vindas a todos para a simulação da comissão extraordinária da Assembleia Geral da Organização Internacional de Polícia Criminal (OIPC/Interpol) da terceira edição da Simulação Interna Santa Clara, que abordará a temática “Gerenciamento de Dados Privados e a Cooperação da Iniciativa Privada”! Partindo para a apresentação dos lindos e maravilhosos diretores deste belíssimo comitê, temos:

- Bruno Fiorelli Barbosa, atualmente cursa o 3º ano do E.M. no Colégio Santa Clara, pretende fazer algo relacionado à Filosofia ou Geografia e gosta muito de fazer fóruns e ler revistas em quadrinhos;
- Fernanda Fernandes Boscariol, atualmente cursa o segundo semestre de Medicina Veterinária na Faculdade Anhembi Morumbi e gosta muito de cachorros;

- Victor Miyano, atualmente cursa o quarto semestre de Relações Internacionais na USP-SP e já estudou húngaro (világos mindem?);
- Mateus Oliveira de Andrade, atualmente cursa o segundo semestre de Direito na FGV-SP e gosta de participar em eventos vitorianos.

Estes diregatos estarão acompanhando vocês no que der e vier, sempre prontos para ajudar e tirar dúvidas. Estaremos disponíveis a qualquer momento tanto por e-mail quanto por telefone/mensagem (depois passaremos nossos contatos). Não vamos colocar especificidades do comitê nesta seção, mas atentem às observações gerais do comitê. Fora isso, esperamos que todos se divirtam e estudem com muita dedicação para tornar este um dos melhores debates já realizado na história da SISC!

Um abraço, e até a Interpol!

Atenciosamente,
Bruno Fiorelli, Fernanda Boscariol, Victor Miyano e Mateus Oliveira

HISTÓRICO DA ORGANIZAÇÃO

A Organização Internacional de Polícia Criminal (OIPC), ou somente Interpol, é um organismo intergovernamental que age no intuito de facilitar a investigação e prevenção de crimes internacionais por meio da cooperação entre agências policiais ao redor do globo. Suas origens remontam desde antes da Grande Guerra, em 1914, durante o Primeiro Congresso Internacional de Polícia Criminal, em Mônaco. Nesta reunião, os representantes de algumas poucas polícias nacionais estabeleceram 12 pontos a serem desenvolvidos (*the 12 wishes*), que podem ser resumidos na implementação de uma metodologia unificada de atuação.

No entanto, foi somente em 1923 que a Interpol deixou de ser uma ideia e tornou-se um embrião. Por iniciativa de Johannes Schober, presidente da polícia de Viena, foi criada a Comissão Internacional de Polícia Criminal (CIPC), sediada no país austríaco. A comissão atuou plenamente por 15 anos, expandindo suas centrais e atividades até o tráfico internacional, falsificações e chegou a criar uma rede de rádio independente para uso único e exclusivo de policiais. Em 1938 a Alemanha, sob controle de Adolf Hitler, anexou o país e tomou controle integral da organização em 1942, movendo sua sede para Berlim. Entre 1938 e 1946, a CIPC foi oficialmente considerada inativa (e por outros até morta ou falida) até que as nações francesa e belga mediram esforços para reconstruí-la após o término do conflito.

Até 1955, havia mais de 50 agências policiais oficialmente afiliadas e, finalmente, em 1956 foi promulgada a vigente constituição, que alterou o nome da comissão para o acrônimo atual. A partir deste ano, a Interpol tornou-se economicamente independente em 1958, estabeleceu sua sede em Lyon, França, em 1989, e adaptou-se à era digital em 1990 com o lançamento e desenvolvimento do sistema de comunicação entre centrais X400 (que evoluiu para o I24/7).

Em 1949, a recém-criada Organização das Nações Unidas (ONU) concedeu à CIPC o status consultivo de organização não governamental (ONG). Mas em 1971, esta situação mudaria com o reconhecimento da Interpol como uma organização intergovernamental. Outras entidades, como por exemplo a União Europeia (UE), promoveram um relacionamento saudável nas últimas décadas que resultou em um massivo desenvolvimento e, no caso, a criação da Europol.

Atualmente, a Interpol aparenta ter desaparecido do cenário internacional, mas é exatamente o contrário. Nos últimos anos, um complexo de inteligência e inovação foi estruturado em Singapura, capacitando maior coordenação de treinamentos especiais e a detecção de novas ameaças, além de ter um foco voltado para os cyber crimes. Campanhas como “Turn Back Crime” que possuem repercussão mundial, auxiliaram no desenvolvimento de políticas para áreas pouco conhecidas, como os crimes ambientais e os crimes esportivos.

Jackie Chan, ator e figura pública, em um painel da Interpol

A OIPC possui diversos comitês essenciais para seu funcionamento, mas o mais importante é sem dúvida a Assembleia Geral, que reúne representantes de mais de 190 nacionalidades. Existem outras cúpulas como o Secretariado Geral e o Comitê Executivo, mas a Assembleia pode, em casos extraordinários, criar uma comissão para análise de uma questão específica. Os membros da Interpol não são as representatividades de cada governo, e sim os representantes das polícias federais (ou nacionais) de cada país membro, justamente por serem as agências mais abrangentes. As polícias são uma instituição estatal que possui o monopólio da violência legítima e está vinculado ao poder judiciário de cada governo, mudando sua forma e comportamento de país para país.

CRIPTOLOGIA

Considerando a enorme bagagem técnico-conceitual que esta reunião tratará, é importante esclarecer alguns princípios relacionados ao tema central. Desta maneira, esta seção foi pura e simplesmente estruturada para desenvolver tudo aquilo que não está diretamente relacionado com as negociações, somente os conceitos fundamentais a serem tratados na discussão.

Introdução

Desde o início da vida na Terra, os seres vivos desenvolveram meios e artifícios para comunicação entre a própria espécie. Até o surgimento da civilização, a maioria das informações era baseada em proteínas, feromônios e até mesmo código genético. A língua escrita começou a surgir na Mesopotâmia, a mais de 6000 anos atrás, com o formato cuneiforme, mas foi somente na Grécia Antiga e no apogeu do Império Romano que as cifras viriam a ser utilizadas.

Criptografia (do grego *kriptos* – escondido; e *grafia* – escrita) é a ciência e a arte de tornar secreta uma mensagem ou uma linha de comunicação entre interlocutores. Atualmente, muitas pessoas possuem um senso comum muito errôneo sobre esta área do conhecimento. A **Criptologia** é o ramo mais abrangente, dentro desta existe a Criptografia, Criptoanálise, Codificação e muitas outras ciências. Apesar de serem ramificações distintas, o objeto de estudo é, na maioria das vezes, o mesmo. Existem três componentes que se encontram no centro de todos os sistemas e paradigmas: a Cifra, o Código e a Chave.

Os **códigos**, como a maioria das pessoas conhece, são mensagens que sofreram o processo de codificação. Este processo somente é possível por meio de uma informação capaz de transformar o

texto original em um texto ou linguagem diferente (código), e o nome atribuído a esta informação (ou algoritmo) de transformação é **chave**. Alguns dos códigos mais conhecidos são o Código Morse, o QR Code, o Código Vitoriano das Flores, o Alfabeto Fonético da OTAN, o Código de Barras e afins. O objetivo dos códigos (assim como o de cifras) é impedir (ou somente retardar) que a mensagem possa ser lida por terceiros, justamente por que a mensagem só poderá ser lida caso seja única e especificamente traduzida pela devida chave.

As **cifras**, diferente dos códigos, possuem uma chave de conhecimento somente dos interlocutores, e de mais ninguém. Códigos, apesar de demorarem, podem ser facilmente traduzidos, pois possuem uma chave de conhecimento geral. Já para uma cifra, decriptar é praticamente impossível sem o conhecimento da chave, e este processo é conhecido como **criptoanálise.** A criptografia pode ser realizada de acordo com inúmeras configurações de chave, sendo que as mais conhecidas são a criptografia simétrica e a assimétrica.

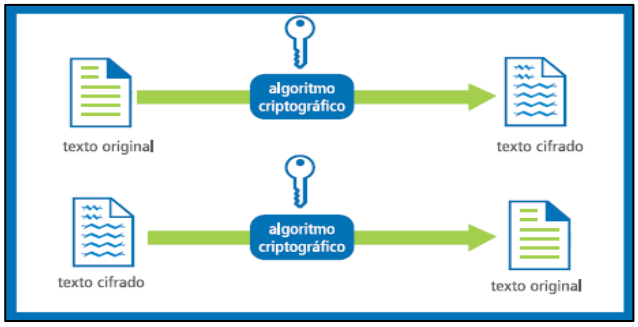

Imagem simplificando o processo de encriptografia e decriptografia

Criptografia Simétrica

Esta forma de criptografia é sem dúvidas a mais simples e a menos utilizada em sistemas de dispositivos tecnológicos. A criptografia simétrica é baseada na premissa de que existe uma chave para a comunicação secreta de um par de interlocutores. Este criptossistema é extremamente eficiente quando se trata de um mínimo grupo de pessoas ou a comunicação de ordens entre pessoas de alto escalão. No entanto, à medida que o número de pessoas cresce dentro da rede de sigilo, o número de chaves cresce, e a segurança destas torna-se exponencialmente alarmante.

Imagine que uma pequena empresa de 1000 empregados possui uma rede interna de comunicação. Cada indivíduo necessitaria de 999 chaves diferentes para conversar com cada um de seus companheiros de trabalho. Desta maneira, seriam necessárias 499,500 chaves diferentes neste criptossistema[1]. Para tanto, nos anos 70, dois engenheiros de software criaram uma solução simples para um problema complexo, a criptografia de chave pública, mais conhecida como criptografia assimétrica.

[1] Este Exemplo foi ilustrado no artigo de Criptologia da Encyclopedia Britannica

Criptografia Assimétrica

Esta forma de criptossistema é extremamente difícil de imaginar, mas muito simples de colocar em prática. Para facilitar a visualização, utilizar-se-á um exemplo que ilustra quatro interlocutores diferentes.

Antes de pensar neste sistema, é preciso especificar que existem dois processos criptográficos diferentes, a encriptografia (transformar o texto em cifra) e a decriptografia (transformar a cifra em texto). Estas operações podem ser divididas em duas chaves diferentes, uma que funcione para encriptar e outra para decriptar. A ideia de ter uma criptografia assimétrica é de tornar uma destas chaves pública, enquanto a outra permanece sigilosa.

Imagine que Fulano quer estabelecer uma comunicação segura com Sicrano. A princípio, eles utilizam uma criptografia simétrica, pois não é necessário um sistema maior. Até que então, Beltrano e Outrano decidem envolver-se nas conversas, e Fulano e Sicrano querem estabelecer uma comunicação secreta com eles também. Para não transformar a conversa em um código (onde todos possuem uma única chave comum) e evitar a manutenção da segurança de mais chaves caso mais pessoas envolvam-se, os quatro decidem utilizar uma criptografia assimétrica.

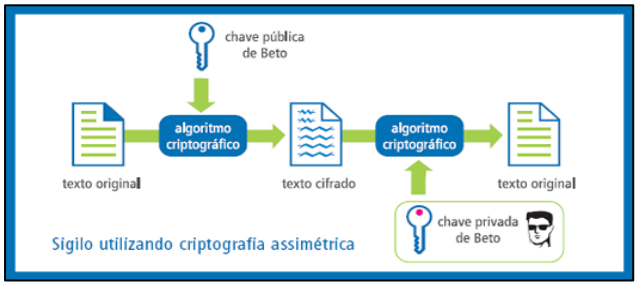

Ilustração do processo de criptografia assimétrica com dois interlocutores

Cada um dos indivíduos reparte suas operações em duas chaves. Agora, cada um possui a sua própria chave de encriptografia e decriptografia. Fulano então pede para todos deixarem as chaves de encriptografia em um lugar acessível e público. Caso alguma das pessoas deseje enviar uma mensagem pra qualquer um, basta processar o texto na chave pública para encriptar e a pessoa conseguirá ler após decriptar com uma chave pessoal. Desta maneira, a segurança restringe-se a somente uma chave e para estabelecer contato com determinada pessoa da rede, basta requisitar sua chave pública.

Criptoanálise

Outra ramificação da criptologia é a criptoanálise, a arte e ciência de compreender um criptossistema sem pertencer a este. Esta área do conhecimento pode ser segmentada em três gêneros diferentes, sendo classificados de acordo com a informação a qual o analista possui acesso. A maioria das metodologias lida com a frequência de letras da língua encriptada e a frequência de repetições sequenciais na cifra. O renomado matemático Friedrich Gauss (1777-1855) uma vez acreditou ter criado uma cifra impossível de ser decifrada, mas nem ele foi capaz de ocultar as repetições das letras na língua alemã.

Atualmente existem companhias especializadas em criptoanálise e decodificação que destacam-se ao prestarem serviços para o governo assim como para empresas. Uma das mais renomadas, a Cellebrite Company de Israel, trabalha com extração, decodificação e análise. A empresa já foi considerada a melhor companhia de recuperação forense de dados em celulares e possui suporte para softwares como iOS, Android, LG, Mycrosoft Mobile, BlackBerry e outros.

DEFINIÇÃO DO TEMA

Apple x FBI

Próximo ao natal de 2015, Syed Rizwan Farook, trabalhador do sistema de saúde pública de São Bernardino, EUA, realizou um atentado que ficou conhecido como "San Bernardino Shooting". Totalizando mais de 20 pessoas feridas e 14 mortos, este ataque continha com um diferencial exclusivo: foram encontrados dispositivos que aparentavam serem bombas implantadas na cena do crime. Após a perícia concluir que os acontecimentos foram planejados e havia possível envolvimento de células terroristas, a investigação logo foi tratada como um caso de terrorismo.

Assim como na maioria dos países, após ser tratado como um ato terrorista, a investigação foi entregue para as autoridades federais do país, a Federal Bureau of Investigation (FBI). As autoridades, considerando que as possíveis bombas ainda poderiam ser ativadas e havia a possibilidade de outras bombas existirem, confiscaram o celular do suspeito, um modelo de Iphone. Apesar do mandato de confisco ser para o celular, o dispositivo eletrônico físico, as informações contidas nele eram protegidas por senha e somente seria possível acessá-lo com a ajuda dos produtores ou com uma operação de *by-pass* (contornar o acesso por senha).

A FBI logo apelou para a Apple Inc. fornecer uma *backdoor* para entrada. No entanto, considerando que esta *backdoor* não seria algo único e exclusivo daquele dispositivo, e sim algo que poderia ser utilizado em toda a linha de Iphones daquele modelo, a empresa recusou, mas continuou cooperando com as investigações da maneira que pôde. O escândalo tornou-se cada vez mais aparente à medida que os atritos entre os dois organismos tornaram-se mais fortes. A dúvida que restou na maioria das cabeças foi "A Apple fez a coisa certa?".

Eventualmente, o FBI conseguiu hackear o Iphone contratando um grupo de hackers independentes, diferentemente do esperado. O episódio causou uma repercussão política, que se refletiu em um processo levado à corte. No entanto, caso a Apple tivesse cooperado ou concedido as informações do cliente, possível terrorista, toda a investigação não seria retardada e a preocupação das autoridades seria sanada em questão de dias, e não semanas. Felizmente, a informação de que os dispositivos na cena do crime eram bombas foi desmentida.

No entanto, toda a conduta deliberada pelos representantes da empresa condizem com sua política de privacidade e proteção de informações, que por sinal, caso fosse agredida, receberia retaliação do mercado consumidor e do nicho de mercado em si, sem contar nas possíveis repercussões judiciais. Assim que a agência desbloqueou o celular, a companhia rapidamente lançou atualizações de sistema para reforçar a segurança e ainda por cima desenvolveu um nova linha de produtos com propriedades diferentes das dos modelos anteriores.

O jornal "The Washington Post", em uma notícia sobre a questão sobre Privacidade X Segurança, elencou duas possibilidades que a Casa Branca anda analisando para compartilhamento de dados para investigações. Um infográfico sobre o tema pode ser acessado no link abaixo:

http://apps.washingtonpost.com/g/page/world/encryption-techniques-and-the-access-they-give/1665/

Os Emails de Hillary Clinton

A atual candidata democrata à presidência dos EUA, Hillary Diane Rodham Clinton, está envolvida em um escândalo que remonta desde 2012, mas somente tornou-se relevante no último ano por conta de sua conta de email. Hillary, até 2013, atuava no cargo de Secretária de Estado do país, realizando a manutenção de diversos assuntos políticos externos e internos durante o mandato de Barack Obama.

Em 2012, um ataque à embaixada estadunidense em Benghazi na Líbia matou 4 pessoas, incluindo o embaixador Chris Stevens, que morreu por inalação de fumaça dos escombros. Os responsáveis pelo ataque foram membros de uma guerrilha islâmica radical, sem aparentes relações com uma célula maior, mas que planejaram cautelosamente o atentado. Autoridades do país rechaçaram tais atos e Obama e Hillary prometeram trazer os radicais à justiça por seus atos.

Muito tempo depois, durante a campanha eleitoral da Ex-Primeira Dama, Hillary causou uma enorme polêmica quando foi relatado que seu email pessoal era utilizado para troca de mensagens relativas a seu cargo. De acordo com a lei federal, toda mensagem expedida oficialmente pelo Secretário de Estado é propriedade da União, fazendo com que as mensagens presentes no email pessoal de Hillary tornassem-se propriedade governamental. A problemática complicou-se ainda mais quando a candidata entregou as 55 mil páginas de emails para o Departamento do Estado sem dar acesso a seu email, possivelmente ocultando trocas de mensagens e informações dos olhos do Estado.

Muitas teorias de conspiração depois, foi encontrado em meio aos emails recolhidos que havia uma possível ligação de Hillary com os ataques de 2012, estipulando-se que a Secretária possuía pleno conhecimento do atentado antes deste acontecer. O Departamento de Justiça, realizaou então uma audiência para averiguar não só o escândalo dos emails, mas também incluiu a negligência de Clinton durante seu mandato.

Atualmente, a candidata foi escolhida como candidata definitiva do Partido Democrata na convenção nacional e ruma para as eleições do país para concorrer com Donald Trump. Nenhuma investigação foi realizada por nenhuma parte em qualquer momento para revelar a verdade por detrás deste episódio.

Brasil X Whatsapp

No final da noite do dia 16 de Dezembro de 2015 o Brasil inteiro observou relatos de usuários do aplicativo WhatsApp, pertencente à empresa Facebook, que o aplicativo estava fora do ar. O que ocorreu foi uma decisão da Justiça Federal, gerado na 1ª Vara Criminal de São Bernardo do Campo, no ABC paulista. De acordo com o Tribunal de Justiça, o WhatsApp não atendeu uma determinação judicial em Julho de 2015, que foi reiterada em Agosto do mesmo ano, aplicando juntamente uma multa. Em nenhum dos casos a ordem foi realizada.

Devido a tal feito, o Ministério Público requisitou o bloqueio do aplicativo por 48 horas, baseado na lei do Marco Civil da Internet. Este foi o primeiro grande bloqueio no país. O presidente da companhia Facebook, Mark Zuckerberg fez um pronunciamento a respeito da ação brasileira "Este é um dia triste para o país. Até hoje, o Brasil tem sido um importante aliado na criação de uma internet aberta. (...) Estou chocado que a nossos esforços em proteger dados pessoais poderiam resultar na punição de todos (...)".

Mas supreendentemente, esta não foi a primeira vez que o bloquei do aplicativo é cobrado pela justiça brasileira. Em Fevereiro, também de 2015, um juiz de Teresina determinou a suspensão temporária do aplicativo, alegando que o mesmo recusava-se a fornecer informações a uma investigação policial em processo desde 2013.

Em Maio de 2016, a Justiça de Sergipe, pelo não comprimento da decisão judicial de compartilhar informações que subsidiariam uma investigação policial, ordenou que as operadoras de telefonia bloqueassem o WhatsApp por 72 horas e, caso fosse descumprido, haveria de multa de 50 mil reais, a ordem foi cumprida por todas as empresas filiadas ao Sinditele Brasil. Como a cessão de informações foi inicialmente descumprida, o presidente do Facebook na América Latina foi preso em Março do mesmo ano.

Em todos os casos, as informações requisitadas eram relativas à investigações de redes de tráfico de drogas internacional. A sociedade internacional não tomou a situação como alarmante e teve pouca repercussão em outras regiões do mundo, mas sem dúvida este é um episódio que demonstra como a informação privada é almejada pelo governo.

Problemática e Solução

Tendo em vista os três episódios anteriormente descritos, a presente reunião da Comissão Extraordinária da Assembleia Geral da Interpol irá focar especificamente em duas questões muito presentes na metodologia de investigação criminal da atualidade: o **compartilhamento de dados privados** entre empresas e polícias e, em um segundo momento, o **gerenciamento destes dados compartilhados**. O objetivo desta seção em si é desenvolver melhor os dois temas e apresentar os principais argumentos que defendem todos os lados.

A começar pelo compartilhamento, existem diversas implicações que devem ser consideradas, principalmente o viés técnico e o conceitual. Estas vertentes levantam duas questões centrais a serem exploradas: "Mais informação significa mais segurança?" e "Como realizar estes compartilhamento de forma a evitar abusos?". O canal de vídeos do Youtube "In a Nutshell" desenvolve muito bem a primeira questão em seu vídeo "*Safe and Sorry - Terrorism and Mass Surveillance*".

Desde 2001, a luta contra o terrorismo tornou-se uma corrida tecnológica e informacional para o Ocidente. Quanto mais informação e mais analistas, maior era a chance de encontrar os líderes do terrorismo fundamentalista mundial. Filmes como "A Hora mais Escura (*Zero Dark Thirty*)", "O Homem Mais Procurado do Mundo (*Seal Team Six: The Raid on Osama Bin Laden*)" e "*Manhunt: The Story of the Hunt for Bin Laden*" demonstram como a busca por informações foi crucial para encontrar a localização do maior terrorista do mundo.

Entretanto, como bem apontado por Steve Taylor, jornalista e narrador do canal "In a Nutshell", "Se você está procurando a agulha no palheiro, adicionar mais palha não vai lhe ajudar a encontrar a agulha" (tradução livre). Possuir mais informações não significa que elas serão manuseadas e encaradas com mais cuidado. Desta forma, a coleta de informações torna-se inútil à medida que a forma de gerenciamento e utilização não é eficiente.

A outra pergunta a ser feita é a como seria realizado o compartilhamento proposto, e, caso este aconteça, haveriam limitações para alguma das partes? Como dito anteriormente, o jornal The Washington Post desenvolveu um infográfico sobre as possibilidades que a Casa Branca está analisando para facilitar este acesso. As duas ideias mais cogitadas até agora são a de "*key escrow*" e "*split keys*". A primeira funciona com a base da criptografia simétrica e determina uma chave completa para o governo e uma chave completa para o usuário, deixando a empresa de fora. Enquanto isso, a segunda, que é a mais aceita, propõe que uma chave seja dividida em duas partes para que uma fique com as empresas e outra com o governo. Desta forma, o acesso só pode ser feito quando as duas partes concordarem.

Na prática, a segunda opção é mais promissora visto que atualmente somente o usuário possui acesso a determinadas informações em seus dispositivos. Colocar o governo no encargo de proteger

chaves de acesso de todos os usuários de seu país é muito arriscado e trabalhoso, sem falar que existem cidadãos que não confiam completamente neste. Estas são algumas das soluções, mas com certeza não são as únicas.

Por último, mas não menos importante, deve ser considerado o futuro desta rede compartilhada. É importante lembrar que este tema somente será abordado caso seja de interesse comum o compartilhamento das informações e caso a rede de dados seja, de certa forma, uma rede integrada. A manutenção de dados governamentais e privados é realizada independentemente por cada uma das entidades, mas caso a rede seja compartilhada (como no caso das "*split keys*"), as questões legais ficam complicadas.

Legalmente falando, os dados compartilhados pertencem às empresas. Consequentemente, a manutenção dos dados depende da mesma, podendo ser assistida por agentes federais. A complicação surge quando a companhia decide não realizar a manutenção ou declarar falência. Todo o banco de dados, de certa forma, seria inutilizado e quem seria prejudicado seria o governo. Tendo em vista que este tem é dependente da decisão do anterior, a única observação a ser feita é que estas questões legais existem e podem ser avaliadas e superadas de formas variadas, deixando a comissão livre neste aspecto para divagar e ponderar sobre as melhores possibilidades.

É importante lembrar que qualquer resolução passada pela comissão é recomendatória, mas, em suas propostas, os delegados não devem infringir os direitos ou interferir na atuação das empresas. Todas as propostas que dizem respeito às empresas devem ter o consentimento destas.

PANORAMAS

Alphabet Incorporation

A Alphabet é uma recente empresa classificada como "holding", ou conglomerado, que comporta empresas como Google, Calico, X, Jigsaw e muitas outras. Oficialmente, a holding foi criada para gerenciar e administrar empresas as quais a Google havia comprado anteriormente, tanto que o atual CEO, Larry Page, já foi presidente desta (uma curiosidade interessante é que o link do site da empresa é http://abc.xyz). Considerando que a Google é sem dúvidas a maior empresa do conglomerado, a política de privacidade e serviços serão principalmente extraídos e resumidos desta entidade, mas reforça-se que existem sim outras empresas do conglomerado que oferecem outros serviços ainda mais diversos.

Em sua Política de Privacidade, a Google declara abertamente que utiliza tanto informações cedidas pelos usuários como informações coletadas do local de acesso, dispositivo utilizado, pesquisas recentes e afins. Todas estas informações são utilizadas para fornecimento, manutenção e proteção dos sistemas, da empresa e de seus usuários. O fornecimento de dados para terceiros dá-se

em quatro situações: com a autorização do usuário, com administradores de domínio, para processamento externo e por fins legais.

Em meio aos motivos legislativos, a maioria dos fins citados são relativos a termos de serviço ou proteção da empresa em si, contudo, existe sim o fornecimento de dados para cumprir com legislações e códigos de lei em determinados países e casos. Todas as informações coletadas são mantidas em processadores de *Big Data Storage* e os sistemas são completamente criptografados.

Apple Incorporation

A empresa Apple classifica as informações com que lida em dois tipos, as pessoas e as impessoais. As pessoais são informações que possuem uma característica única, servem como identificadores. Em contrapartida, as informações impessoais são aquelas que não definem o usuário, como fuso horário, língua, sites visitados, preferências; que são informações diferentes de nome, email, telefone, endereço, etc... Quando há a fusão dos dois tipos de informação, digamos para um perfil, a informação final é tratada como pessoal.

O objetivo da coleta de informações pessoais é evitar fraudes e incrementar produtos e serviços para agradar ainda mais os clientes. As únicas formas legislativas de ceder informação é por obrigação da lei, processo legal ou litigação. A empresa já cooperou em diversos casos com a polícia, mas nem sempre cumpriu com os requisitos desta por não ter obrigação para com as agências. A informação também pode ser cedida a terceiros para processamento e análise.

Bharti Airtel Limited

A Bharti Airtel Ltd. (BAL) é uma empresa de telecomunicação que atua em 20 países, especificamente africanos e asiáticos. Sediada em Nova Délhi, a companhia pertence à holding Bharti Enterprises e fornece serviços para mais de 305 milhões de clientes. Em sua política de privacidade, é especificado que a única informação a qual esta política aplica-se é a informação pessoal, aquela capaz de identificar o usuário.

Da mesma forma que as outras empresas, a BAL utiliza tais informações para prestação de serviços e confirmação de identidade, além de outros propósitos. É também prescrito que pode-se ceder informações para terceiros para análise e consultoria além de também cooperar com agências governamentais para fins legislativos.

Samsung Electronics Limited

A Samsung Electronics Ltd. (SEL) é uma das empresas do grupo Samsung que lida com produção de softwares e hardware. Diferente de outras companhias, a Samsung é uma das poucas

empresas que recebe e troca informação com terceiros. Obviamente, as informações somente são compartilhadas com parceiros por meio de contratos.

De origem coreana, a cooperação com as agências policiais orientais é muito mais branda do que com as de outras nações. A SEL possui âmbito internacional e atua em mercados como o de aparelhos televisivos, celulares, aparelhos caseiros, e afins. É uma das empresas que possuem maior variedade comercial no comitê e estão envolvidos em diversos tipos de serviços.

República da África do Sul (SAPS)

A África do Sul, assim como os outros países africanos em sua maioria, possuem uma visão muito próxima a respeito do tema. Os vigentes presidentes de longa data das nações desejam sim o acesso a informações por motivos de segurança nacional. Ainda é muito duvidosa a exigência das agências africanas apesar do número extremamente baixo de cyber crimes no continente e a maioria dos atentados terroristas acontecem na região do Magreb.

Alguns meses atrás, o presidente sul-africano foi acusado de espionagem política, prática extremamente presente em diversos países. O país também se encontra entrelaçado com a União Africana (UA) bloco o qual desenvolve um papel ativo.

República de Angola (NAP)

Angola é um país cuja língua oficial é o português. Devido a raízes socioculturais, o país encontra-se conectado não só com a sociedade luso-brasileira, mas também possui elementos da cultura africana. Assim como o posicionamento da África do Sul, a agência nacional de polícia busca o acesso a informações irrestrito por motivos também duvidosos. O presidente do país alerta que atentados terroristas podem acontecer a qualquer momento e a defesa nacional deve estar preparada.

Comunidade da Austrália (AFP)

A Polícia Federal Australiana é responsável não só pelos crimes cometidos em território nacional, mas também em toda a *Commonwealth* (CW). Assumindo um papel protagonista na CW, a Austrália lida com crimes internacionais como fraude, tráfico de drogas e crime organizado. Especialmente após o polêmico referendo britânico, o país vem destacando-se nos últimos anos de forma cautelosa.

A cooperação para com outras agências, assim como para a Interpol, é muito importante, apesar de não relevar à altura da Islândia e Noruega. É uma agencia que preza muito os valores de integridade e satisfação e é capaz de realizar muito bem seus trabalhos de forma independente.

República Federativa do Brasil (BFP)

A Polícia Federal Brasileira (PF) possui muitas tarefas, como estipulado na constituição do país, sendo algumas delas a proteção das extensas fronteiras, fiscalização ferroviária e rodoviária, divisão marítima, tráfico de drogas e demais atividades ilícitas. Uma das operações mais conhecidas da PF é a Operação "Lava-Jato", uma investigação de corrupção generalizada, formação de cartel e lavagem de dinheiro que começou em postos de gasolina e chegou até a empresa estatal Petrobrás.

Como colocado na seção anterior, a justiça brasileira cultiva atritos com determinadas empresas americanas. É sim interesse da PF o acesso a estas informações, pode-se dizer até que de forma desesperadora. A polícia brasileira possui intenções de coletar informações principalmente de bancos suíços e empresas de serviço de telecomunicações.

República Popular da China (PAP)

A polícia chinesa cuida não só de crimes comuns, mas também de vazamentos de informação que prejudiquem o país ou seus moradores. Apesar de muitos governos manterem informações guardadas a sete chaves, existem informações governamentais sigilosas no país capazes de assegurar pena de morte para os agentes do vazamento.

Sob a ameaça de risco de segurança pública, a Polícia Popular Armada é capaz de tomar conta de todos os canais de comunicação até que a situação seja emancipada, fazendo de tudo para garantir que informações confidencias não sejam divulgadas ou apresentadas da forma errada. Algumas das preocupações mais frequentes da polícia, como a rede de tráfico de drogas, comércio de produtos falsificados e redes de prostituição internacional, muitas vezes tomam prioridade sobre alguns crimes, principalmente por que estes problemas acabam por diminuir índices sociais e econômicos do país.

República da Colômbia (CNP)

Diferente das outras agências, a polícia colombiana é dividida em diferentes setores que atuam independentes uns dos outros. Infelizmente, por conta de falta de recursos econômicos, algumas destas divisões não são muito desenvolvidas, como é o caso da divisão de cyber crimes. Determinados crimes, incluindo o tráfico de drogas, possuem um enfoque muito forte da polícia, levando estes a crer que os dados privados possam auxiliar em investigações mais aprofundadas da rede de distribuição de maconha e coca.

O país atualmente passa por um período de grande desigualdade e problemas sociais. A administração política atual tem feito de tudo e mais um pouco para lidar com as crises atuais, mas agravantes como as Forças Armadas Revolucionárias Colombianas (FARC) e o descontrole territorial de algumas regiões no norte do país impedem uma atuação mais ampla do governo.

República da Coréia (KNPA)

A polícia coreana, assim como a japonesa, possui uma questão cultural de respeito mútuo envolvida nas relações entre o governo e a iniciativa privada. Considerado um polo tecnológico assim como muitos países asiáticos, a Coréia representa um dos principais agentes pela defesa dos direitos das empresas.

Tendo em vista a cultura extremamente liberal e receptiva da nação, a agência de polícia nacional reflete as mesmas características, sendo uma das mais abertas e auxiliadoras. Atualmente, a divisão de cyber crimes da polícia pode ser considerada uma das mais bem treinadas e efetivas da Ásia, senão do mundo inteiro.

República de Cuba (PRC)

Cuba não possui muitas empresas em seu território devido ao regime socialista imposto por Fidel Castro. Com poucas companhias estatais, o país abriu suas portas nos últimos anos para negociações com outros países, quebrando o embargo instaurado durante a Guerra Fria. Considerando a recente abertura e a política de reconciliação, a Polícia Revolucionária de Cuba possui objetivos claros, garantir que o Estado possua controle sobre os dados das empresas.

Não é surpresa reconhecer que a polícia de Cuba teria um posicionamento relativo, mas em meio à transição geopolítica na qual o país encontra-se, é necessário ter garantias mais do que promessas, principalmente quando dizem respeito ao povo e à segurança pública.

República da Eslovênia (SNP)

A agência de polícia da Eslovênia é recém-criada comparada às dos outros países. Desde 1991, com a Guerra Civil da Iugoslávia, que resultou em sua divisão em múltiplos países (e ainda não terminou), a polícia não adquiriu experiência o suficiente para lidar com o caso que o comitê apresenta. Felizmente, o país é extremamente aliciado à ideologia dos países europeus, justamente porque faz parte da União Europeia.

Considerando que a polícia eslovena é relativamente nova, no entanto, bem treinada, a agênia nacional não possui grandes preocupações neste comitê, mas procura atuar em um papel facilitador principalmente em negociações as quais a UE está envolvida.

Estados Unidos da América (FBI)

O governo estadunidense possui uma divisão específica para inteligência e espionagem (CIA) e outra ainda mais específica para interceptação e criptoanálise (NSA). No entanto, somente o FBI possui jurisdição sobre casos de infração legal dentro da federação. Operações conjuntas entre as diferentes agências pode ocorrer em casos de conflito de jurisdição, mas todas operam independentemente sem o acesso aos respectivos bancos de dados.

Para dar continuidade a uma investigação criminal, os operativos coletam provas do possível crime e encaminham para a Corte Suprema. Após avaliação da corte e do Departamento de Justiça (DoJ), os agentes recebem uma resposta positiva para continuar a investigação caso as provas sejam conclusivas. Isso significa que muitas vezes é impossível iniciar uma investigação sem acesso a informações, o confisco de um celular pode não iniciar uma investigação, mas a informação contida neste pode tornar-se uma ameaça à segurança nacional.

República Francesa (FNG)

Na França, a polícia não possui permissão para agir irrestritamente. Toda e qualquer atividade deve ser antes averiguada pelo poder judiciário, e este somente permitirá em caso de extremo perigo e ameaça da segurança pública. A metodologia de atuação assemelha-se muito a forma como o FBI atua nos EUA. O país também conta com outra organização de integração policial supranacional, a Europol, que atua principalmente quando há investigações em mais de um país do Espaço Schengen.

Uma atuação recente que marcou muito a política atual francesa foi quando houve a repressão das revoltas e greves pela não alteração do código de leis trabalhistas do país. Não houve violência letal, mas a repressão tomou proporções desnecessárias e repercutiram pelo país inteiro.

República de Gana (GPS)

Gana foi o primeiro país africano a sediar uma Assembleia Geral da Interpol (1976) e é um membro extremamente ativo da *West African Police Chiefs Committee* (WAPCC). Figurativamente, sua atuação na União Africana não é notável, mas a polícia é muito bem treinada e possui ótimos índices de alistamento, em comparação com seus vizinhos.

Infelizmente, a agência de polícia não possui departamentos para crimes online ou cyber crimes bem desenvolvidos, e muito menos um posicionamento claro frente ao assunto do comitê. No entanto, este país é visto como a voz do povo do oeste africano e já serviu de facilitador em inúmeras negociações.

República da Índia (IPS)

Devido à grande população e extensão territorial do país, a polícia indiana possui 24 subdivisões espalhadas por todas as regiões. O país, assim como a Coréia do Sul, EUA e Japão é um polo industrial e tecnológico muito forte. Muitas multinacionais, principalmente atuantes no mercado asiático e africano, concentram-se na cidade de Mumbai.

Tendo em vista o grande contingente populacional do país, foi necessário que em 1902 o governo indiano criasse a National Crime Records Bureau, pois beirava ao impossível gerenciar todos os dados e portfólios que as diferentes subdivisões da polícia detinham. A polícia indiana não possui uma posição forte referente ao tema, mas claramente beira a ser contra a obtenção dos dados visto os problemas os quais a agência já possui referentes a gerenciamento de dados.

República Islâmica do Irã (IRIP)

A pouco tempo, o Irã foi foco da comunidade internacional pois, em conversações com os EUA, França, Alemanha, Reino Unido e outros representantes, firmou um acordo multilateral para estabelecer um plano de ação para o futuro do Programa Nuclear do Irã. Frente a uma atmosfera de desconfiança, tais medidas foram vistas como necessárias para reduzir o arsenal nuclear mundial e cumprir o Tratado de Não Proliferação Nuclear estabelecido pela Organização das Nações Unidas.

A policia iraniana, muito antes deste panorama belicoso formar-se diante do mundo, já era reconhecida por contar com uma divisão de cyber crimes bem desenvolvida e possuir enorme experiência na atuação em sistemas computacionais e de rede. Felizmente, o país é muito bem protegido por sua agência de polícia nacional e possui fortes interesses nas informações privadas para facilitar inquéritos e investigações.

Estado de Israel (IP)

Apesar de Israel possui um dos mais perigosos e bem estruturados serviços de inteligência e espionagemdo mundo (Mossad), a polícia nacional é muito ocupada de tarefas uma vez que conflitos territoriais e terrorismo doméstico são frequentes. Infelizmente, não existe uma divisão de cyber crime bem desenvolvida no país, mas companhias de criptoanálise, como a Cellebrite Company citada anteriormente, são reconhecidas mundialmente.

A agência nacional de polícia israelense possui sim uma preocupação com dados privados tendo em vista que grande parte da população da Csjordânia e Gaza possui ligação com células terroristas. Os Acordos de Oslo (I e II) delimitaram áreas de jurisdição do governo israelense e da autoridade palestina, mas não por isso a polícia israelense não pode atuar na integridade do país.

Islândia (IC)

Apesar de a polícia islandesa não aparentar ter grande influência, esta é uma das únicas a qual se preocupa em deixar evidente a metodologia da polícia para com o uso e principalmente manutenção de dados pessoais durante as investigações. No site oficial do Ministério do Interior existem regulações específicas disponíveis ao público. Com um modelo de processamento e a iniciativa de cultivar relações públicas, o país é, assim como a Noruega, extremamente importante para o equilíbrio internacional.

Atualmente, muita polêmica tem girado em torno do Primeiro Ministro do país, que foi acusado de possuir empresas *off-shore* no Panamá para sonegar impostos. Todo o episódio resultou na saída do posto por pressão popular.

Japão (NPA)

A polícia japonesa possui linhas de defesa diversas, incluindo a Defesa Imperial, Defesa de Ministros, Defesa de Desastres Naturais, Defesa da População e afins. Todas estas possuem permissão governamental para atuarem da forma necessária e imediata para resolverem as ameaças iminentes.

O governo do Japão, assim como praticamente todas as agências, organizações e serviços relacionados, possui uma raiz cultural extremamente forte, baseada no respeito mútuo e na honra. Desta maneira, todas as relações nutridas pelo país refletem tais valores. A cooperação com o setor privado demonstra-se extremamente frutífera à medida que as companhias e empresas tecnológicas dão total apoio às investigações com as informações necessárias. Pode-se dizer que este é um sistema que pode não ser efetivo em outras nações devido ao fator cultural.

Reino da Noruega (NPS)

A Noruega, apesar de possuir um dos mais baixos índices de criminalidade do mundo, conta com uma polícia federal com pouco mais que 10 mil policiais. As maiores áreas de atuação são em pesquisa forense e luta contra o crime organizado.

Um dos mais importantes objetivos da polícia norueguesa é a cooperação entre agências por meio de plataformas e disseminação de conhecimento para departamentos locais. O país não é um dos destaques no progresso contra o crime e muito menos uma referência contra o cyber-terrorismo, mas é determinante para manter concisa a atuação internacional e preza muito a tolerância cultural no trabalho.

República do Panamá (NPP)

A polícia panamenha é completa e unicamente subordinada ao presidente. Toda ordem emitida pelo chefe de estado é de caráter mandatório e absoluto, sendo que uma investigação, para ter início, é necessária a aprovação deste. Sendo assim, esquemas de corrupção são incrivelmente complicados de serem investigados.

Atualmente, o Panamá recebeu muito a atenção da mídia por conta de um vazamento de informações de uma companhia do país, a Mossack Fonseca, responsável por serviços de advocacia. O escândalo, conhecido como *"The Panamá Papers"* foi um dos maiores, senão o maior, vazamento de informação confidencial e pura do mundo que envolveu figuras públicas e políticas mundialmente reconhecidas em esquemas de sonegação de impostos com a manutenção de empresas *off-shore.* A nação centro americana, sendo um dos poucos países fiscais do mundo, aparenta não demonstrar interesse em modificar sua política atual.

Federação Russa (PR)

A polícia federal russa é tratada como um departamento do Ministério do Interior do país. Relativamente nova, a ex-milícia nacional está focada em realizar mudanças estruturais em sua conduta e atuação. Mesmo após as reformas legislativas neste setor a 5 anos atrás, a Polícia da Rússia ainda possui má fama generalizada no senso comum, mas esta vem tentando provar o contrário à medida em que participa ativamente em campanhas da Interpol e possui um papel ativo na Força Tarefa do Mar Báltico sobre Crime Organizado (BSTF).

Algumas das principais tarefas da polícia é a garantia de direitos básicos à população e a luta contra o crime organizado. Ambos os objetivos ficam claros após a análise dos discursos do Ministro Vladimir Alexandrovich e da Lei Federal Nº 3-FZ. No entanto, ainda que a agência esteja disposta a atingir tais metas, ela precisa ponderar se questões como o acesso a informações privadas é algo que faria bem à imagem da entidade ou seria algo tão efetivo que garantiria mínimas repercussões.

República de Singapura (SPF)

Singapura, apesar de territorialmente diminuto e aparentemente inofensivo, representa uma das maiores potências regionais. Considerado um dos 4 Tigres asiáticos, o país é um dos países mais militarizados do mundo e mantém relações muito próximas com os EUA e Israel. Sua polícia federal não lida com crimes muito relevantes, em sua maioria acidentes de trânsito, roubos, furtos e demais crimes simples. O número de policiais, ao contrário de tropas, é relativamente pequeno, mas a divisão de cyber crimes é ultra especializada.

Nos próximos anos, Singapura irá tornar-se a capital da luta contra o crime e da luta contra crackers. Um complexo de treinamento da Interpol está atualmente em construção no país e concentrará uma diversidade de artifícios para policiais de todo o mundo. O treinamento contra cyber crimes em especial será uma novidade para muitas agências, especialmente por que auxiliará muitas delas a serem independentes de um banco de dados privado ou da boa vontade de uma empresa em ceder dados.

Confederação Suíça (FOP)

A polícia federal suíça é segmentada em diferentes departamentos, cada um com uma especialidade e conduta diferente, incluindo um Departamento de Cyber Crimes. A agência possui uma atuação quase irrestrita e costuma realizar diversas investigações internacionais, sendo um exemplo para crimes como falsificação de peças de arte, corrupção e propina.

A Suíça é internacionalmente reconhecida por comportar diversas corporações de investimentos e bancos, configurando um alvo não só da própria agência de polícia como da de muitos outros países, principalmente africanos e sul-americanos, uma vez que muitas das investigações de corrupção são originárias destes continentes. Atualmente, o acesso a contas bancárias de clientes demora alguns meses, sendo necessária a coleta de muitas evidências e provas para o inquérito e provendo mais que o necessário para a remoção e deslocamento dos bens capitais.

Ucrânia (UNP)

O governo ucraniano, muito embora parte da antiga União das Repúblicas Socialistas Soviéticas (URSS), possui uma forte ligação com o setor privado. O atual presidente do país, a partir de 1990, envolveu-se com o mercado de cacau e chegou a administrar uma das maiores empresas de confeitaria do país, a Roshen. Esta proximidade demonstra que as relações público-privadas do país são favoráveis a uma rede de compartilhamento.

No entanto, a polícia nacional ucraniana possui forte influência não só das raízes soviéticas como também dos interesses da União Europeia e da OTAN. A forte repressão que os movimentos separatistas tiveram em 2013 deve-se muito a brutalidade da polícia, principalmente da forma como os treinamentos são conduzidos.

OBSERVAÇÕES GERAIS

Nesta seção, serão especificadas algumas peculiaridades do comitê. Em primeiro lugar, o nome oficial do comitê a ser simulado neste fórum é "Comissão Extraordinária da Assembleia Geral da Interpol (CEAG-OIPC)", ou seja, um órgão subsidiário da Assembleia Geral (AG). Por ser uma comissão temporária (não duraria para sempre), este comitê possui caráter ***recomendatório***, ou seja, os delegados não podem passar uma resolução que ordene, altere, ou reconfigure qualquer aspecto da organização. Somente serão aceitas resoluções que recomendem, sugiram e incentivem determinados pontos da discussão que serão encaminhados para a AG.

Outra questão importante a ressaltar é a jurisdição de cada delegado. No panorama geopolítico atual, uma das premissas mais básicas que rege todo o sistema global é a de Soberania Nacional, que, ao pé da letra, significa que cada país deve cuidar de seus problemas e não cuidar do problema dos outros sem permissão. Da mesma forma que a polícia do país (A) não pode investigar um crime do país (B) sem permissão, uma investigação policial que envolve os países (A) e (B) não seria bem sucedida sem a cooperação mútua das duas agências. Lembrando que as polícias federais, em termos legais, geralmente só podem tratar de crimes em nível federal, que variam de acordo com a legislação de cada país. A mesma ideia vale para as empresas, elas são submetidas à lei, mas são consideradas propriedades privadas, ou seja, requerem permissão ou pode-se exigir um mandato de confisco com provas que suportam a necessidade deste.

Em termos de recursos, a Interpol não possui policiais próprios, assim como a Organização das Nações Unidas (ONU). Existem agentes especializados em determinados gêneros de crime e coordenadores regionais, mas estes raramente efetuam trabalho de campo, atuando em um papel mais administrativo. Existe um fundo monetário utilizado em projetos vigentes advindo de doações, mas não é recomendável a utilização do poderio econômico da organização (até porque iria requerer conhecimentos de comércio exterior e macroeconomia que os diretores não possuem e não se mostra necessário perante o tema em discussão).

Com relação às representações, as empresas serão representadas pelos respectivos CEOs enquanto as polícias pelos Comandantes de Polícia (ou o Ministros da Justiça, dependendo do caso). Os CEOs, para emitirem uma ordem para a empresa, precisam primeiro da aprovação da *"Board of Directors"* (Conselho Diretivo), que pode ser contatado por meio de cartas para a mesa. Já as agências, estas podem atuar livre e plenamente, de acordo com a vontade de cada delegado, sempre respeitando as jurisdições e o respeito internacional (a não ser que alguém deseje uma guerra, mas isso já vai ser explicado). Para emitir uma ordem ou enviar uma carta a qualquer representante de um governo ou instituição, pode ser enviada uma carta para a mesa com o remetente.

Em relação aos Documentos de Trabalho, a mesa irá disponibilizar um computador para uso público (dois delegados por vez) para a produção de documentos. Quando finalizados, estes devem ser previamente encaminhados para a mesa para avaliação e formatação para serem apresentados posteriormente. Em caso de documentos que pertençam a domínio público (internet), a fonte deve ser registrada. Só serão aceitos documentos escritos em português. Em caso de imagem ou vídeo, estes podem conter textos em outras línguas.

Sobre a Agenda de Trabalho, como especificado no Guia de Regras, a mesa não irá oficializar nenhum documento como sendo parâmetro para as discussões. Os delegados podem apresentar documentos elencando os tópicos que desejam-se abordar, mas a mesa não reconhecerá tal como uma agenda, e sim um documento de trabalho.

Existe ainda uma prática muito comum em simulações chamada "Intervenção" ou "Crise". Geralmente, uma crise é um momento no qual surge uma situação que requer ação imediata por parte dos delegados, colocando muito mais responsabilidades no comitê e muito mais tensão em cada ordem dada. Na realidade, é extremamente raro que uma crise de verdade atinja um comitê, ou ainda que o comitê possua jurisdição sobre esta, mas, para propósitos acadêmicos, muitos fóruns e simulações adotam a prática, seja para agitar um comitê entediante ou para causar uma pequena grande polêmica (afinal, quem não gosta de assassinar uns presidentes, hehehe). No entanto, os diretores gostariam de avisar que a Interpol pode ser sim submetida a estas eventuais crises e, caso ocorram, os procedimentos de crise serão especificados na hora.

Agora, um ponto extremamente crucial neste comitê: caso, de alguma forma, algum delegado declare oficialmente guerra a um determinado país (que não o seu) o comitê será automaticamente encerrado. Esta regra vale para todos os comitês da simulação que não lidam diretamente com um evento belicoso. A mesa diretora não se oporá a qualquer declaração do gênero, visto que é o ímpeto de uma determinada nação e a mesa deve permanecer neutra, mas tais declarações, caso sejam relevadas, também estarão sendo avaliadas de acordo com a política externa (não seria pertinente, por exemplo, o Kiribati declarar guerra ao Sudão do Sul, visto que os dois países mal mantém relações diplomáticas por falta de recursos e estão territorialmente distantes um do outro). Guerras civis serão desconsideradas, visto que muitos países ainda persistem em conflitos internos e não seria tão gritante quanto um confronto geopolítico.

Por último, mas não menos importante, os representantes das empresas não possuem voto. Apesar de serem considerados presentes ou ausentes, seu papel é meramente consultivo, ou seja, não serão contados no quórum das sessões. As empresas podem sim ser signatárias de documentos e, ao final de votações de resoluções, poderão devidamente expressar-se caso sejam favoráveis ou contra a resolução do comitê

Encerrando assim as observações, os diretores gostariam de dizer que estarão sempre à disposição para resolver dúvidas, sejam relativas às regras, Guia de Estudos, política internacional, receita de bolo, time de futebol ou novela das oito.

REFERÊNCIAS

http://brasil.elpais.com/brasil/2016/02/17/internacional/1455702891_642434.html (Acessado dia 25/07)

http://edition.cnn.com/2016/04/21/politics/san-bernardino-iphone-apple-hacking/ (Acessado dia 29/06)

http://g1.globo.com/mundo/noticia/2015/03/hillary-clinton-diz-que-usou-conta-pessoal-de-e-mail-por-razoes-praticas.html (Acessado dia 07/08)

http://g1.globo.com/sao-paulo/noticia/2016/03/policia-prende-representante-do-facebook-na-america-do-sul-em-sp.html (Acessado dia 02/08)

http://g1.globo.com/tecnologia/noticia/2015/12/estamos-trabalhando-para-reverter-bloqueio-do-whatsapp-diz-zuckerberg.html (Acessado dia 02/08)

http://g1.globo.com/tecnologia/noticia/2016/04/fbi-diz-que-desbloqueio-de-iphone-nao-funciona-em-novos-modelos.html (Acessado dia 30/07)

http://g1.globo.com/tecnologia/noticia/2016/05/usuarios-relatam-bloqueio-do-whatsapp-nesta-segunda-feira.html (Acessado dia 02/08)

http://global.britannica.com/topic/cryptology#toc25626 (Acessado dia 15/05)

http://global.britannica.com/topic/Interpol (Acessado dia 15/05)

http://kurzgesagt.org/ (Acessado dia 02/08)

http://lavajato.mpf.mp.br/lavajato/index.html (Acessado dia 02/08)

http://www.aljazeera.com/news/2016/03/fbi-breaks-iphone-dead-san-bernadino-shooter-160329041508229.html (Acessado dia 29/06)

http://www.aljazeera.com/news/middleeast/2012/09/20129112108737726.html (Acessado dia 07/08)

http://www.bbc.com/news/world-us-canada-34993344 (Acessado dia 29/06)

http://www.brasilpost.com.br/2016/07/19/bloqueio-whatsapp-brasil_n_11076150.html (Acessado dia 02/08)

http://www.cellebrite.com/ (Acessado dia 10/05)

http://www.interpol.int/en (Acessado dia 11/05)

http://www.latimes.com/local/lanow/la-me-ln-fbi-drops-fight-to-force-apple-to-unlock-san-bernardino-terrorist-iphone-20160328-story.html (Acessado dia 29/06)

http://www.mossfon.com/ (Acessado dia 02/08)

http://www.theverge.com/2016/3/18/11260488/india-ringing-bells-4-dollar-smartphone-controversy (Acessado dia 02/08)

https://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ee745911a4ff_story.html (Acessado dia 10/05)

Panoramas

https://www.google.com/policies/privacy/ (Acessado dia 07/08)

http://www.apple.com/legal/privacy/en-ww/ (Acessado dia 07/08)

http://www.airtel.in/forme/privacy-policy (Acessado dia 07/08)

http://www.samsung.com/us/common/privacy.html (Acessado dia 07/08)

http://www.saps.gov.za/ (Acessado dia 07/08)

https://www.afp.gov.au/ (Acessado dia 07/08)

http://www.interpol.int/Member-countries/Africa/Angola (Acessado dia 07/08)

http://www.pf.gov.br/ (Acessado dia 07/08)

http://eng.mod.gov.cn/ArmedForces/armed.htm (Acessado dia 07/08)

http://portal.policia.gov.co/en-us/Pages/default.aspx (Acessado dia 07/08)

http://www.police.go.kr/eng/main.do (Acessado dia 07/08)

http://www.interpol.int/Member-countries/Americas/Cuba (Acessado dia 07/08)

http://www.policija.si/eng/ (Acessado dia 07/08)

https://www.fbi.gov/ (Acessado dia 07/08)

http://www.defense.gouv.fr/gendarmerie (Acessado dia 07/08)

http://www.interpol.int/Member-countries/Africa/Ghana (Acessado dia 07/08)

http://ncrb.gov.in/ (Acessado dia 07/08)

http://cyber.police.ir/ (Acessado dia 07/08)

http://mops.gov.il/english/policingeng/police/pages/default.aspx (Acessado dia 07/08)

https://eng.innanrikisraduneyti.is/ (Acessado dia 07/08)

https://www.npa.go.jp/english/index.htm (Acessado dia 07/08)

https://www.politi.no/international/ (Acessado dia 07/08)

http://www.policia.gob.pa/inicio.html (Acessado dia 07/08)

https://en.mvd.ru/ (Acessado dia 07/08)

http://www.police.gov.sg/ (Acessado dia 07/08)

https://www.fedpol.admin.ch/fedpol/en/home.html (Acessado dia 07/08)

http://www.npu.gov.ua/en/ (Acessado dia 07/08)

Imagens

Capa - http://www.aljazeera.com/news/2015/12/san-bernardino-california-mass-shooting-151203050149707.html

Jackie Chan - http://korannonstop.com/2016/05/pakai-kaos-turn-back-crime-bisa-diancam-penjara-3-bulan/

Encriptografia (adaptadas) - http://www.rmaues.com/2015/07/criptografia-para-massa-o-que-e.html