
# Global Encryption Day – October 21 2024 - Encrypt Today to Safeguard Tomorrow: The Encryption Summit

## Artigo 45 do eIDAS: Por Trás das Cenas

**Robin Wilton - Internet Society:** Olhem para o eIDAS, Artigo 45, um tópico que tenho certeza está na mente de todos. Se você não ouviu falar do Artigo 45, não se preocupe. Vamos falar sobre isso em breve. Mas antes disso, tenho algumas notas de organização. Primeiro, essas sessões têm um código de conduta.

Portanto, certifique-se de estar ciente disso para evitar qualquer surpresa desagradável. Em segundo lugar, temos uma função de chat e uma função de perguntas e respostas. Por favor, envie suas perguntas por meio de uma dessas opções. E, por último, a interpretação está disponível em francês, espanhol e português. Você deve ver um ícone de globo na parte inferior da sua tela no Zoom para ativar a função de interpretação, se precisar.

Esses são os avisos. Temos 50 minutos para esta sessão, o que não vai parecer tempo suficiente, então não vou gastar tempo dando mini biografias de todos os palestrantes. Basta dizer que vale a pena procurar suas biografias online, pois conseguimos reunir um conjunto incrível de especialistas no assunto para isso.

Muito brevemente, eles são Alexis Hancock do projeto EFF CertBot, onde ela é a diretora de engenharia. Dennis Jackson da Mozilla, onde ele está na equipe de engenharia de criptografia. E por criptografia, não criptomoeda. E Thomas Lohninger, que é o diretor executivo do Epicenter. Então, bem-vindos ao meu painel.

Bem-vindos ao público. Estamos ansiosos por uma sessão fascinante. Para contextualizar em um nível muito alto, o Artigo 45 define parte de uma estratégia geral da União Europeia em relação à identificação digital como parte de uma iniciativa mais ampla chamada eIDAS. O foco principal do eIDAS é, historicamente, uma identidade digital para o cidadão, e evoluiu para incluir funcionalidades semelhantes a uma carteira ou, em princípio, declarações confiáveis.

de atributos individuais, como identidade, idade, qualificações profissionais, e assim por diante. O que estamos aqui para discutir hoje é uma parte muito específica disso, o Artigo 55 das regulamentações do IDS. E, acho que, Thomas, vou passar para você primeiro, se me permite, para detalhar um pouco mais essa visão geral que eu dei com uma pequena explicação do que é o Artigo 45, se puder, e depois talvez continuemos com algumas das características mais amplas do eIDAS como um esquema.

**Thomas Lohninger - epicenter.works:** Muito feliz em ajudar. Obrigado, Robin. Espero que todos possam me ouvir bem. Sim, o regulamento eIDAS é na verdade uma peça de legislação muito antiga. Foi adotado pela primeira vez em 2014. E a missão principal desta lei europeia é estabelecer uma plataforma harmonizada para identidade digital. Esta lei de 2014 nunca se concretizou totalmente porque havia razões pelas quais os estados membros nacionais, os estados membros da UE, não queriam basicamente reconhecer todos os diferentes sistemas de identidade digital de outros países. E assim, em junho de 2021, a União Europeia começou a reformar este regulamento eIDAS, e ele basicamente continha dois grandes projetos. Um era a chamada Carteira de Identidade Digital Europeia, que deveria realmente estabelecer um sistema harmonizado para identificar pessoas físicas e jurídicas, como pessoas e empresas, em relação ao setor público e privado, online e offline e em proximidade física, e também permitir a verificação de atributos sobre essas pessoas, online e offline. E isso, de forma importante, também é destinado a ser um sistema universal de propósito geral.

Portanto, deve realmente abranger desde carteiras de motorista, euros digitais, controles de fronteira, todos os diferentes tipos de sociedade, até mesmo visitas ao médico. Tudo isso acontecerá com base nesta carteira de identidade digital europeia. E a segunda parte desta reforma foi o Quox, Artigo 45, que nos traz aqui hoje, onde essa ideia de querer identificar todos também se estende aos sites.

E, como explicaremos mais adiante, estabeleceu essa ideia de ter os proprietários, as pessoas por trás de um site, autenticados para os usuários que estão usando ou visitando um site. E assim, essa ideia de ter a propriedade do domínio identificada com um certificado que os fornecedores de navegadores também são obrigados a exibir para seus usuários é, de certa forma, uma ideia antiga, mas uma ideia que a União

Europeia quer trazer de volta à mesa, talvez para entrar em alguns dos argumentos que ouvimos durante o debate, por que alguns dos estados membros acham que é uma boa ideia.

Nós, como Epicenter Works, estávamos trabalhando nessa reforma desde o primeiro dia. Tenho que dizer, nosso foco principal era a carteira, porque como uma ONG de privacidade, isso era algo onde vemos um ataque drástico à anonimidade online, aos nossos dados de identidade verificados criptograficamente pelo governo, sendo proliferados para áreas onde realmente não deveriam estar, como grandes empresas de tecnologia ou agências de pontuação de crédito, mas estávamos igualmente preocupados também com o Artigo 45 e, esse ataque à arquitetura de confiança da World Wide Web. E acho que vou deixar por aqui.

**Robin Wilton - Internet Society:** Obrigado. Aquela nota de 5 euros que te dei para a transição perfeita foi bem gasta. Porque acho que onde você parou foi, sim, existem essas potenciais implicações de privacidade em ter, o que na prática pode ser uma identidade emitida pelo governo central que é usada como base para todas essas afirmações de nível de atributo e acho que voltaremos a isso no devido tempo. Mas onde você parou foi, há essa ideia de identificar sites para o usuário final também. Então, Alexis, acho que gostaria de falar com você a seguir, se puder. A ideia de identificar sites para o usuário, isso soa familiar porque tivemos o pequeno cadeado no navegador por um tempo, e depois tivemos a barra de URL ficando verde para dizer que este site realmente é, realmente, o que você pensou que estava acessando. Estamos reinventando isso?

**Alexis Hancock - EFF:** Sim, isso foi uma repetição. Não há outra maneira eloquente de dizer isso, onde tínhamos certificados de validação estendida e abordamos essa ideia de verificar sua identidade através do TLS, que foi uma abordagem que já adotamos antes.

E não cumpriu as promessas que uma vez fez sobre ser capaz de atrair o usuário final em um site para se sentir, não apenas seguro, mas também saber que a pessoa ou entidade por trás do site é quem diz ser, usando TLS para fazer isso através de certificados de validação estendida.

Quando os certificados de validação estendida foram propostos, estávamos em uma época diferente. A web não era tão criptografada. A web era menos segura e tínhamos um ecossistema onde os certificados de validação de domínio não eram tão automatizados e não eram tão amplamente utilizados pelo usuário comum da web e pelos sistemas empresariais como são hoje.

Ser capaz de automatizar essas coisas e automatizar a segurança para serviços web, serviços por aí. Então, temos certificados EV. E passamos por esse ciclo e, por volta de 2018, acho que os navegadores em grande parte decidiram descontinuar a interface do cadeado verde porque não estava cumprindo o que se propunha a fazer.

Originalmente, foi um grande esforço. E eu quero destacar. Colocar lá fora que os certificados EV não são baratos. Eles são caros em comparação com os certificados de validação de domínio. E foi realmente a emissão de certificados de validação de domínio que ajudou a web a se tornar mais criptografada. Mais do que os certificados mais caros e mais onerosos, como a validação estendida.

Então passamos por esse ciclo. E quando vi isso, vi uma repetição de uma solução para um problema que não cumpriu os padrões que se propôs a alcançar.

**Robin Wilton - Internet Society:** Interessante. Certo. Então, os temas que acho que estamos abordando são, como você disse, o TLS, segurança da camada de transporte, que proporciona confidencialidade.

para sessões de navegador, desde que você tenha um meio seguro de troca de chaves entre o servidor e o navegador, mas esse meio seguro de troca de chaves em si significa que você precisa identificar o servidor corretamente, caso contrário, eu posso estar obtendo uma sessão segura do meu navegador, mas pode não ser para o servidor web correto.

Então, como você disse, o TLS meio que resolve esse problema tecnicamente. Mas aí você tem aquele passo procedimental de, esse é o chave pública do site pertencente à organização que diz ser dona do site? E eu acho que é esse passo procedimental. Então, Dennis, posso falar com você sobre essa parte?

Porque. e você esteve envolvido tanto na tecnologia de criptografar sessões entre navegadores e sites, mas acho que você e seus colegas também trabalharam nessa ideia de transparência de certificados. Então, como você detecta comportamentos inadequados entre os proprietários de certificados de sites?

Acho que a pergunta que quero tentar resumir é: se você quiser dizer a alguém que este site está usando um certificado falso para alegar que não é quem diz ser, o usuário final é a pessoa certa para informar?

**Dennis Jackson - Mozilla:** Obrigado, Robin. Sim, acho que essa é uma pergunta realmente interessante. Então, do ponto de vista do usuário final no navegador, como um agente de usuário, temos que decidir se as chaves que vemos, o certificado que vemos, são confiáveis para aquele site específico.

E eu acho que, como você mencionou, embora possamos tomar algumas decisões técnicas sobre isso, no final das contas, o usuário nunca estará em uma posição de estar totalmente informado sobre aquele site e suas práticas e políticas específicas, e ser capaz de entender se aquele site é a informação de autenticação correta para essa conexão em particular.

No passado, na época dos certificados EV, como Alexis mencionou, pensávamos que talvez adicionar mais informações a esse certificado poderia ajudar os usuários a tomar essa decisão, e como Alexis mencionou, essa abordagem realmente não foi bem-sucedida. Então, o que aconteceu foi que nos movemos mais em direção a um sistema de transparência pública.

E agora, quando as autoridades certificadoras emitem os certificados usados no TLS, eles precisam ser registrados publicamente com vários operadores de logs de transparência. E o valor disso é que esses logs agora são acessíveis ao público. Em particular, o proprietário do site, um pesquisador de segurança ou qualquer outra pessoa pode inspecionar esses logs e verificar os certificados que foram emitidos.

E, particularmente no caso do proprietário do site, eles podem dizer: Eu reconheço este certificado e esta chave pública porque são meus. Eu os gerei, eu os solicitei e, portanto, são seguros. Mas, se virem algo que não solicitaram, algo que não lhes pertence, mas está sendo usado para endossar uma conexão para o seu site, podem relatar isso como um problema sério e, em última análise, tomar medidas com base nisso para garantir as conexões ao seu site.

**Robin Wilton - Internet Society:** Enquanto isso, seria algo que o indivíduo realmente não pode fazer. Então, sim, dizer a eles que está errado quando não têm os meios para fazer algo a respeito pode acabar frustrando as pessoas. Dito isso, eu me pergunto quantas pessoas na audiência já viram um aviso de certificado aparecer no navegador dizendo: "Oh, o certificado deste site pode ser inválido."

E quantas pessoas realmente. ou desistem ou tentam fazer algo a respeito, em vez de simplesmente clicar e dizer, ah, eu queria chegar lá de qualquer maneira. e eu suspeito que a grande maioria provavelmente se enquadraria nessa última categoria. Thomas, quero voltar a você aqui porque, Dennis mencionou práticas e políticas de sites.

Em outras palavras, o que mais além da tecnologia você precisa para ter algum nível de garantia de que o certificado de um determinado site realmente pertence àquela organização? E Alexis falou um pouco antes sobre os certificados EV, que envolvem, por exemplo, alguém da organização fornecendo uma prova de identidade muito mais forte e prova de seu papel na organização para obter esse certificado.

Mas, então, a parte específica sobre a qual eu queria te perguntar é, e isso se aproxima muito mais do Artigo 45 aqui, qual é a diferença entre os certificados previstos pelo Artigo 45, os chamados QOCS, Certificados de Autenticação Web Qualificados, qual é a diferença entre esses e os certificados TLS que Alexis mencionou, que afinal de contas são a base para aquela sessão criptografada entre o seu navegador e o site?

**Thomas Lohninger - epicenter.works:** Obrigado, Robin. Essa é uma ótima pergunta e, na verdade, uma que discutimos extensivamente nos três anos e meio desde que essa lei foi proposta. E você ouviria coisas diferentes dos legisladores e também dos

provedores de serviços de confiança, que são as empresas que têm a ganhar economicamente com o Artigo 45.

E alguns deles diriam que são realmente duas coisas diferentes. Quarks são apenas outra palavra para Certificados de Validação Estendida (EV) que têm o objetivo de identificar o proprietário de um site para os usuários e seguem essa ideia europeia de que tudo deve ser identificado. Temos um forte impulso em várias legislações setoriais, como a Lei de Serviços Digitais, onde a verificação de idade é uma questão importante.

Espaço Europeu de Dados de Saúde, você vê isso surgir em todos os lugares hoje em dia, a UE parece estar bastante decidida a erradicar o anonimato online, o que vemos como um grande problema. E, a propósito, também temos o direito à pseudonimidade no eIDAS no Artigo 5, que tenta mitigar esse risco.

E o Artigo 45, claro, tem uma função dupla. Então, algumas pessoas, e conseguimos convencer a maioria no Parlamento Europeu a seguir essa interpretação, que QUOX não são certificados TLS. QUOX deve ser separado. QUOX deve apenas fazer a parte de identificação e separar a criptografia de ponta a ponta via TLS do certificado QUOX seria o caminho certo a seguir.

no conselho, então quando os 27 novos estados membros tiveram que chegar a um acordo sobre essa lei, essa distinção não estava tão clara. E os provedores de serviços de confiança geralmente estão bastante próximos de seus governos, são organizações nacionais. Houve um esforço para que os provedores de serviços de confiança fossem reconhecidos por todos os fornecedores de navegadores.

E às vezes você ouvia argumentos como, sim, mas é tão oneroso entrar na lista da Apple ou do Google ou de qualquer fornecedor de navegador e no seu repositório de certificados raiz. E se o governo diz que é seguro e é seguro o suficiente para o estado, então também deve ser seguro o suficiente para essas grandes empresas de tecnologia.

Esse é um argumento que ouvimos muito nas negociações. E talvez também para voltar a onde estamos legalmente. Então, em maio deste ano, a União Europeia aprovou o regulamento eIDAS, que já está em vigor. Mas existem os chamados atos de implementação que detalham as obrigações na lei.

E há também um ato de implementação no Artigo 45, mas não vimos isso. No total, há cerca de 28. pelo menos 28 Atos de Implementação, às vezes você pode ver vários para uma única disposição legal e apenas cinco foram submetidos à consulta até agora. A consulta terminou no início de setembro e, na verdade, amanhã será a votação desses cinco que dizem respeito apenas à carteira.

Na verdade, temos trabalhado nisso de perto e parece que eles podem falhar. Você pode ler no Amlaks político e na mídia alemã que há uma grande agitação entre os estados membros sobre se esses cinco atos de implementação sequer serão aprovados. Isso significa que teremos que esperar bastante tempo até obtermos os detalhes técnicos sobre como os quarks são realmente implementados e, a Etsy, que é uma organização de padrões que também trabalha em parte com vigilância.

padrões e interceptação legal também têm um lugar à mesa e essas especificações técnicas. Então, a palavra final definitivamente não está aqui, mas é muito bom que possamos ter essa discussão.

**Robin Wilton - Internet Society:** Acho que você nos deu uma visão realmente importante dos bastidores, porque tenho certeza de que não é coincidência que você mencionou 28 atos de implementação diferentes para isso.

E esse número parece coincidentemente próximo ao número de estados membros da UE, com uma ou duas variações, infelizmente falando. Eles entenderam, eu acho, porque você também disse que ouviu o argumento de que, se isso é seguro o suficiente para satisfazer o governo, então deve ser bom para o cidadão.

E ainda assim, entre esses mais de 20 estados membros, vemos governos de naturezas extremamente diferentes e muito complexas politicamente. Então, o que você está realmente dizendo é que, por um lado, temos esse conjunto global de regras sobre como os certificados TLS entram na lista de confiança dos principais navegadores. E, por outro lado, queremos possivelmente até 27 regras nacionais diferentes sobre como esses certificados entram na mesma lista.

E isso me parece ser o cerne absoluto deste problema. Então, com isso, Alexis, posso falar com você um pouco aqui? Sugerimos a ideia de que há um conjunto de regras através das quais os certificados TLS entram nos navegadores. E, como Dennis disse, esses, por sua vez, dependem de políticas e procedimentos sobre como as autoridades certificadoras alocam e atestam esses certificados.

Essas são as mesmas regras para os certificados QOX? Porque não parece.

**Alexis Hancock - EFF:** Então, não, e eu quero analisar isso sob a perspectiva de um incidente de segurança com um certificado emitido de forma inadequada ou nefasta. Alguns anos atrás, o governo do Cazaquistão basicamente estava colocando um certificado para espionar o tráfego dos seus cidadãos.

E eles fizeram isso no nível do navegador, porque eram previamente confiáveis. E uma vez que a Mozilla descobriu, uma vez que o Chrome descobriu, eles foram descredibilizados porque estavam agindo não apenas fora do âmbito dos direitos civis

em geral, mas agindo mal como uma autoridade certificadora. Isso não é algo que se deve fazer como uma autoridade certificadora.

E parte disso é ser capaz de agir rapidamente. Assim que as pessoas ficaram cientes do que estava acontecendo a partir do nível de monitoramento, a CA e o certificado do Cazaquistão foram removidos e perderam a confiança. Quando você coloca a lei nesse processo sem consultar as partes envolvidas, isso desacelera significativamente a resposta a incidentes de segurança, porque agora os navegadores teriam que passar por um processo legal apenas para remover uma CA ou um QTSP se eles estivessem agindo fora dos limites.

Agora vamos falar sobre esses limites, certo? Então, você tem programas de Rootstore. Agora, todos os principais navegadores têm um. Isso nem sempre foi assim. Eu sempre gosto de mencionar isso porque, nesta conversa dos últimos três anos, abordamos o TLS e o ecossistema como se fosse o mesmo de 10 anos atrás, e simplesmente não é o caso.

Agora temos programas de root store. Temos programas de root store que se comunicam entre si. Você tem diretrizes básicas, orientações. Temos transparência de certificados. Temos controles de conta mais rigorosos. Há uma série de coisas acontecendo que são mais úteis do que antes. Então, você tem programas de root store, suas regras e seu processo de auditoria agora.

E não apenas os repositórios raiz, mas quem decide que uma AC pode entrar lá, um processo real de monitoramento, auditoria, e um processo transparente de expulsar essa AC, se necessário. Então, já existe um processo estabelecido para isso. O QTSP com Quox e o Artigo 45 seriam capazes de contornar completamente esse processo e automaticamente ganhar confiança nos repositórios raiz do navegador.

Então você pode ver agora onde estaria a sobreposição em termos de democracia, transparência, e como isso se parece quando você tem, essencialmente, uma AC patrocinada pelo estado, neste caso, capaz de contornar esses tipos de regras, e não apenas contornar as regras, mas agora legalmente obrigada a ser exigida nesses navegadores.

E quando os navegadores adotam a posição de que uma AC não está à altura de seus padrões, agora temos um novo processo legal a seguir, apenas para que essa AC seja desacreditada se algo foi emitido incorretamente, mal administrado ou inserido de forma nefasta.

**Robin Wilton - Internet Society:** E então, sim, parte do seu medo é que esse processo legal demore para se desenrolar, e, na verdade, do ponto de vista da segurança operacional, você precisa que isso aconteça muito mais rápido, em um prazo mais curto.

Thomas, vou falar com você e depois, Dennis, tenho uma pergunta para você também.

**Thomas Lohninger - epicenter.works:** Bem. Obrigado, Alexis, por abordar esse ponto e você está absolutamente certo. Existem alguns obstáculos adicionais criados por isso, mas também quero fazer uma distinção importante: quando você olha para os considerandos e o debate jurídico, o que seria visto como uma razão para excluir um provedor de serviços de confiança do repositório de CA raiz é algo mais como o caso do DIGI Notar, ou seja, uma violação de segurança na CA. Mas se houvesse um caso de interceptação legal e um provedor de serviços de confiança de um país, vamos pegar um país com fraco estado de direito, como a Hungria, emitisse um certificado, totalmente legal para fins de agência de inteligência, por exemplo, então eu nem sei como isso seria classificado. Queríamos ter uma linguagem mais forte em torno da interceptação legal porque essa é uma preocupação principal para nós.

Mas, infelizmente, isso não é algo onde vemos uma linguagem forte na lei.

**Robin Wilton - Internet Society:** Sim, você pinta um quadro preocupante e eu ia voltar para você, Alexis, sobre isso, antes de passarmos para o ponto de Dennis. Realmente, me parece que. Ao incluir essas autoridades certificadoras mandatadas pelo governo na mesma lista como se fossem equivalentes às que entram lá pelo processo de autoridade certificadora e navegador, não só abre a porta para, como você deu o exemplo do Cazaquistão, e eles não são os únicos, acho que Maurício tentou a mesma coisa, de um governo tomar medidas para instalar um certificado raiz que permitiria a ele, a, a, a descriptografar e interceptar todo o tráfego entrando e saindo daquele país.

Mas há outro tipo de dano também, não é? Que é, se autoridades certificadoras estão na lista de raízes confiáveis do navegador que manifestamente não são confiáveis. O que isso faz à confiabilidade das outras autoridades certificadoras, que, na visão do usuário, entraram lá pelo mesmo processo?

Então, qual é o impacto em coisas como TLS?

**Alexis Hancock - EFF:** Eu acredito fortemente que é necessário criar políticas de Internet e tecnologia voltadas para os problemas de amanhã, em vez de apenas os problemas de hoje. Nem todos os membros da UE estão operando da mesma maneira, como Thomas mencionou. Sendo uma das entidades que podem estar agindo, talvez não em conformidade com os mesmos princípios democráticos que outros estados membros da UE.

Então, você precisa olhar desse ponto de vista, de ser capaz de criar políticas tecnológicas que não pensem apenas em linhas geopolíticas. Você tem que considerar como a Internet realmente é. E é algo global. É uma comunidade de cidadãos globais, na Internet.

E eu gostaria de pensar que, em qualquer momento em que ouvi governos falarem sobre soberania e criar barreiras na Internet em torno de fronteiras geopolíticas, nunca me senti bem depois de ouvir esses termos e nomenclaturas sobre a Internet. Porque, se você começar a criar políticas com base nesse aspecto e não pensar em um aspecto mais global de cidadania na Internet e em quem está interagindo com ela, e não criar políticas que protejam as pessoas amanhã e não apenas hoje.

Você não sabe quem estará no poder amanhã. Então, você deve fazer políticas tecnológicas para quem estará no poder amanhã e criar essas salvaguardas. O Artigo 45 teria colocado em risco essa salvaguarda de confiança. Definitivamente, especialmente se você tivesse diferentes partidos agindo de maneira diferente dentro dos estados membros da UE.

O que aconteceria com um usuário se você tivesse um QTSP da Hungria em vez de outro país? Onde eles poderiam até avaliar isso? E eu acredito que não devemos colocar esse fardo nos usuários comuns para avaliar isso. Cabe a nós, como especialistas, políticos e educadores nesse assunto, chegarmos a um consenso sobre como isso deve ser, em vez de deixar o fardo para os usuários descobrirem como essa confiança se manifesta na web.

**Robin Wilton - Internet Society:** Sim. E definitivamente vamos precisar voltar aos impactos na privacidade, pseudonimato e direitos fundamentais disso. Mas quero trazer o Dennis de volta. Desculpe, Dennis, você tem esperado pacientemente. Então, há algumas coisas que eu adoraria que você abordasse, se puder. E a primeira segue muito bem o que Alexis acabou de dizer.

Então, uma das, uma das, uma das resistências que eu enfrentei, há alguns anos, quando estava fazendo algumas pesquisas sobre fatores de confiança na Internet aqui, foi que, essa objeção à implementação e ao desdobramento do Artigo 45, objetar a isso era antidemocrático no sentido de que você tinha uma regulamentação, que havia sido produzida através do processo democrático, a União Europeia.

E, por outro lado, você tinha um punhado relativamente pequeno de especialistas em autoridades certificadoras dizendo, não, isso é uma má ideia. Não vamos deixar você fazer isso. Isso é realmente algo antidemocrático, ou há uma justificativa a ser considerada?

**Dennis Jackson - Mozilla:** Acho que, para responder a isso, realmente precisamos entender como o Artigo 45 surgiu.

E voltando, como Thomas mencionou, em 21, houve um processo público em torno da elaboração desta lei e da identificação do que ela poderia precisar fazer. E o principal resultado disso foi uma sugestão de que, uma exigência de que os navegadores reconhecessem esses certificados e os usassem para exibir esse tipo de informação adicional de identidade.

E a Mozilla, a Edry e muitos outros grupos se envolveram nessa questão e discutiram os méritos dos certificados EV versus os certificados DV e assim por diante. E por volta do meio de 20, desculpe, início de 23, essa lei caminhou para sua finalização. E no processo da UE isso significa entrar no Trílogo, que é uma série de negociações finais a portas fechadas para produzir o texto final.

E foi somente nesse ponto que o Artigo 45 começou a se metastatizar e assumir um caráter completamente novo. E foi durante essas negociações privadas que um novo texto foi introduzido para impor esses requisitos aos provedores de navegadores, para reconhecer QTSPs da UE, CAs da UE, e para não removê-los a menos que os governos da UE concordassem.

em termos de princípios democráticos, este texto foi introduzido em privado, acordado em privado, e quase se tornou lei essencialmente através de um processo de lobby privado que não foi transparente para o público, e do qual os especialistas e acadêmicos em cibersegurança simplesmente não estavam cientes e não puderam participar.

O que aconteceu como resultado disso, como uma reação a isso, foi que essas ONGs, os fabricantes de navegadores, acadêmicos e especialistas em cibersegurança se uniram para dizer que isso está errado, que isso não deveria ser feito, que isso não traria valor para os cidadãos europeus, e essencialmente pediram ao Parlamento Europeu que se opusesse a isso.

E, por fim, o Parlamento Europeu decidiu atender a esse chamado e optou por pressionar para que o texto fosse emendado e alterado no último minuto, literalmente dias antes de ser publicado, para introduzir novas salvaguardas que restringiriam o impacto da lei e não exigiriam que os fabricantes de navegadores confiassem nessas ACs com base em decretos governamentais.

**Robin Wilton - Internet Society:** Joe fez uma pergunta na sessão de perguntas e respostas, dizendo que as emendas ao Artigo 25, que permitem a tomada de ações urgentes de segurança, permitindo a adesão às melhores práticas de segurança do usuário, aliviam a pressão sobre alguns dos problemas aqui? Se não, você gostaria de ver mais? Dennis, quero te dar a chance de responder primeiro, e acho que Alexis, você pode ter algumas considerações sobre isso.

Além disso, Thomas, levante a mão se quiser comentar sobre isso. Então, Dennis, continue.

**Dennis Jackson - Mozilla:** um segundo. Sim, então o principal resultado dessas mudanças de última hora foi introduzir uma nova exceção para dizer que nenhuma obrigação de reconhecer charlatães contradiz os direitos dos fabricantes e distribuidores de navegadores de autenticar sites de uma maneira e meios a seu critério.

E isso é fundamentalmente a salvaguarda essencial, que protege contra abusos de grande parte disso. Embora os navegadores ainda reconheçam quacks e exibam essas informações de identidade aos usuários, isso não se estende às chaves criptográficas contidas nesses quacks, e os fornecedores de navegadores ainda podem usar seus próprios procedimentos de segurança para isso.

Então, eu acho que isso é uma salvaguarda essencial e poderosa, mas assim como com a carteira, isso agora precisa ser implementado em um Ato de Implementação e realizado em um padrão técnico. E parte do meu trabalho na Mozilla tem sido colaborar com a Etsy sobre como esses padrões técnicos vão se parecer.

E um foco central disso tem sido dividir o átomo, por assim dizer. Então, pegar os padrões QAC existentes, onde as informações de identidade e as informações TLS estão contidas no mesmo certificado, e dividi-los em dois, para que tenhamos um certificado TLS, que está puramente sob o controle do navegador e usa as práticas transparentes existentes que temos usado nos últimos 20 anos.

E então o próprio QAC, que conterá informações sobre o nome de domínio do site e informações sobre a identidade legal do site, mas não será usado para estabelecer essas conexões criptografadas. E isso tem sido um processo muito longo, concordar com esses padrões, e ainda não está concluído, e como Thomas mencionou, pode não estar concluído por mais seis meses, enquanto diferentes partes das disputas técnicas e legais continuam, mas isso tem aliviado a pressão, e acho que o pior cenário foi evitado.

**Robin Wilton - Internet Society:** Thomas, parece que estamos apenas passando por um processo passo a passo de descrever o que a regulamentação diz, o que isso significa e quais são suas implicações. Parece que estamos muito longe dos objetivos do tipo EI DAS que descrevemos no início, em termos de coisas como funções de carteira, confiança aprimorada do usuário, porque, meu Deus, não tenho uma ótima sensação sobre isso a partir desta discussão.

Mas, para ser direto, o Artigo 45 é adequado para o propósito?

**Thomas Lohninger - epicenter.works:** Não, não realmente. Mas a questão é, qual é o propósito que ele serve? E se o propósito é realmente criar confiança na World Wide Web, então acho que ele já era falho desde o início. Se o objetivo era minar a arquitetura de segurança da web, então o veredito ainda está em aberto, mas, no final das contas, quero voltar enquanto estamos passando pela linha do tempo, o que aconteceu quando, e posso confirmar que as negociações do Trilog foram realmente um momento desastroso.

Não é a minha primeira lei da UE, estou fazendo isso há 10 anos, por isso tenho cabelos grisalhos. E foi um momento bastante esperançoso quando organizamos esta carta de 400 acadêmicos e ONGs que realmente conseguiu trazer essa questão

finalmente à atenção do público, porque o IDAS é super nerd. É uma lei muito técnica e complicada que foi negociada principalmente sem muita fiscalização pública.

Acho que fomos a única ONG a fornecer constantemente análises de cada versão da lei, incluindo as versões não públicas que foram discutidas em tribunal. para permitir algum debate público e escrutínio sobre o que realmente está acontecendo. Mas foi com esta grande carta que conseguimos realmente assustar os MEPs e a presidência do conselho a voltar à mesa para nos dar concessões que nos permitem agora uma chance de lutar na aplicação.

E conseguimos, pelo menos, incluir algumas das principais disposições de privacidade no texto legal, e sua lei está realmente avançando muito lentamente. Então, quando você tem algo assim, geralmente dura uma década. Isso significa o efeito real na prática, nos navegadores das pessoas, nos smartphones das pessoas, quando você vai ao médico, ao dentista, ao supermercado ou atravessa a fronteira.

Dê-nos mais dois ou três anos e então você realmente verá isso, porque os estados membros terão que oferecer toda a gama dessas novas tecnologias e tudo o que pode impactar nossas vidas diárias. O argumento que é nosso métrico de sucesso e que, curiosamente, também é o argumento político mais forte com os legisladores é que um grande projeto como o eIDAS é, em última análise, julgado pela confiança que os cidadãos depositam nele.

A confiabilidade do ecossistema que criamos, quão resiliente ele é contra atores mal-intencionados ou fraudulentos que tentam abusar ou minar o sistema. E isso ainda é algo em que precisamos ser muito atentos. Temos que prestar muita atenção. É por isso que estou realmente atento a como será a votação amanhã.

E eu realmente espero que falhe. Espero que tenhamos mais tempo e que a comissão tenha que voltar à prancheta com algumas dessas coisas. O Ato de Implementação do eIDAS só será proposto, acho que por volta de maio do próximo ano, então ainda há tempo. E a questão específica que foi levantada por Joseph diz respeito ao Considerando 65.

E sim, há uma linguagem suficientemente boa, como mencionei anteriormente, para lidar com algo como uma violação de segurança de um provedor de serviços justo, com medidas de precaução pelo fornecedor do navegador. Eles têm que notificar a comissão, as autoridades nacionais, mas podem agir. Quando se trata de interceptação legal, talvez com uma ordem de silêncio, dependendo do país e das leis nacionais, não tenho certeza.

E não estou tranquilo de que o Considerando 65 seja realmente uma salvaguarda significativa o suficiente para prevenir esse tipo de abuso.

**Robin Wilton - Internet Society:** Sim, fantástico. Uma das minhas perguntas favoritas quando me mostram algo assim e dizem o quão maravilhoso seria, é dizer: mostre-me o que neste sistema realmente previne o abuso da funcionalidade que você está descrevendo.

e sim, acho que essa é uma pergunta frutífera a se fazer neste caso, mas quero, faltando 10 minutos, e quero usar parte desse tempo, Alexis, com você, se me permite. então ali você tinha Thomas, que trabalha para uma organização especializada em entender, comentar e tentar influenciar esse tipo de legislação da UE.

e é difícil o suficiente dentro da UE. Como é quando você começa a olhar para as implicações transfronteiriças disso? Como você, Alexis, explica aos formuladores de políticas fora dos EUA o que é um trílogo, para começar? Que tipo de problemas você encontrou lá?

**Alexis Hancock - EFF:** Sim, então esta foi minha primeira rodada aprendendo as principais diferenças entre os comitês, a comissão, os parlamentos, os trilogos.

E como este é meu primeiro ciclo, os cabelos grisalhos ainda não apareceram. Mas tenho certeza de que em alguns ciclos eles virão. Tentando entender isso no contexto de como isso se parece, não apenas nos EUA, mas no exterior, de forma ampla, na Internet. E como isso se parece para a rede de confiança? Como alguém que trabalha.

Meio que em uma linha mais neutra de poder vangloriar os ganhos da segurança TLS automatizada, que é onde isso chamou mais minha atenção, isso inibe, isso dificulta na verdade a capacidade de automatizar certificados TLS, em grande escala, e diferentes estruturas, especialmente estruturas que definitivamente precisam disso, como no EIDIS, onde você tem carteiras digitais, você precisa ser capaz de agir rapidamente, precisa ser capaz de manter a segurança de uma maneira como nunca antes, se você realmente quer implementar uma identidade digital em larga escala para alguém, você precisa ter um sistema de confiança que faça sentido.

E retroceder um sistema de confiança para pontos de vista mais arcaicos não fazia sentido para mim, e traduzir isso para fora dos EUA e ver como isso poderia ser, não os EUA, não os EUA, a UE, mas também olhando para isso nos EUA, onde eles também estão considerando a identidade digital de várias maneiras diferentes.

Ainda não está em nível federal, mas diferentes estados já implementaram carteiras de motorista móveis. Quero dizer que um pouco mais de 20 estados já implementaram carteiras de motorista móveis e implementaram carteiras digitais ou contrataram com a Apple e o Google para usar suas carteiras nos sistemas nativos de iOS e Android, respectivamente.

Então, o que temos aqui é uma possível influência. Os EUA olham para o GDPR para muitos dos avanços em privacidade de dados em torno de legislação e políticas, e eu temia que, se isso fosse aprovado como está, as pessoas olhassem para isso como um exemplo na UE, dizendo, ok, veja, a UE conseguiu isso com o Artigo 45, talvez devêssemos adotar uma linguagem semelhante e aplicar isso.

Eu nem sei como seria se alguém de outro país visitasse um site respaldado por QTSP e fosse potencialmente fraudado se esse sistema fosse abusado. Quais são os meios de contestar isso ou obter algum tipo de compensação ou retribuição por ter sido fraudado?

O que foi isso? Como seria isso para alguém? E há muitas pessoas fora da UE usando sites baseados na UE. Não teria sido contido apenas nesse ecossistema de ser um cidadão da UE. Então, não tenho muita certeza de como isso teria sido, mas ser capaz de explicar isso e implorar aos meus políticos dentro da UE, dizendo que vocês estão dando o exemplo, vocês deram o exemplo com o GDPR, então realmente precisamos que vocês acertem isso nesse sentido, ou pelo menos sejam capazes de garantir ganhos básicos de segurança aqui, que obtivemos nos últimos 10 anos e não retroceder para um tempo em que o TLS era caro, oneroso, você.

E, honestamente, não tão rigoroso como costumava ser, ou como é agora em termos de apoiar a automação e ser capaz de, na verdade, automatizar a segurança de uma maneira que faça sentido para todos e permitir que os participantes do ecossistema tomem as decisões como fazem agora, porque é um processo transparente.

É um processo que ocorre fora da UE, mesmo que tenhamos membros da UE em diferentes órgãos de normalização, eles estão tomando essas decisões juntos. Não é algo isolado. Então, tomar essa decisão de forma isolada não fazia muito sentido para mim. E foi isso que eu tentei explicar para audiências fora da UE, para não necessariamente seguir esse caminho específico se isso acontecesse.

**Robin Wilton - Internet Society:** Sim, e acho que podemos ver isso por analogia com outros produtos e serviços, que a última coisa que você quer é um navegador que só funcione na UE. Não é assim que essas redes ou fabricantes de navegadores devem desenvolver produtos diferentes para mercados geográficos diferentes, isso realmente começa a corroer alguns dos benefícios fundamentais de ter uma Internet global.

Ok, então temos apenas alguns minutos restantes. Eu só quero, por assim dizer, dar uma volta na mesa novamente para algumas últimas considerações. Dennis, você está otimista neste momento, do ponto de vista técnico, e se a resposta for sim ou não, o que dizer do otimismo não técnico?

**Dennis Jackson - Mozilla:** Acho que me descrevo como um otimista, mas tenho dificuldade em ser otimista quanto ao processo pelo qual isso foi alcançado e à forma como esses regulamentos e padrões técnicos estão sendo atualmente redigidos.

Eu acho, você sabe Então há

**Robin Wilton - Internet Society:** um pouco disso que é aberto e transparente e no processo democrático. Você mencionou, por exemplo, o Parlamento Europeu assumindo o caso contra isso, mas antes de chegar a esse ponto, também houve as sessões mais problemáticas a portas fechadas.

**Dennis Jackson - Mozilla:** Sim, e acho que não só antes desse ponto, mas também agora depois desse ponto, onde a Comissão acabará por redigir um Ato de Implementação para realizar isso, com base em um padrão técnico, e esse padrão técnico será desenvolvido a portas fechadas na ETSI, o que exige um tipo extenso de acordo comercial para contribuir.

Não será um padrão em que qualquer pessoa possa opinar, ou como no ITF, onde você tem uma norma mais participativa, e esse Ato de Implementação não será supervisionado pelo Parlamento. Fundamentalmente, caberá ao Conselho Europeu, aos estados membros, decidir se o consideram adequado.

E isso limita a oportunidade de escrutínio e controle sobre esses processos, tornando muito mais difícil para o cidadão europeu médio se envolver de maneira significativa. E essa Europa

**Robin Wilton - Internet Society:** O Conselho, é claro, é composto por políticos nacionais. Sim. Então, Thomas, talvez você possa encerrar isso para nós com algumas reflexões sobre o impacto mais amplo disso em coisas como anonimato e pseudonimato e outros direitos fundamentais e a tecnologia que os apoia.

**Thomas Lohninger - epicenter.works:** Sim, claro. Concordo com o Dennis. Sempre digo que sou otimista por profissão. E, de certa forma, é bastante difícil ver as ações dos nossos governos expostas aqui diante de nós com consequências devastadoras. Ao mesmo tempo, há motivos para ter esperança, porque podemos conseguir mudanças significativas no processo, nas negociações, com pressão pública.

desde que nós, como um público informado, como especialistas da sociedade civil, nos incluamos nesses processos. Podemos fazer a diferença. Nos atos de implementação que serão votados amanhã, um quarto das nossas emendas foram aceitas pela comissão. Portanto, há oportunidade de realmente influenciar essas decisões se prestarmos atenção.

Esse escrutínio público é fundamental. E estamos em um momento decisivo. Alexis mencionou como os sistemas de identidade digital já estão proliferando em muitos estados americanos. Eu faço parte de um projeto da ONU sobre infraestrutura pública digital que se baseia no sistema indiano ATAR e em muitas outras regiões onde esses sistemas surgem.

Então, acho que é exatamente o momento de prestar muita atenção e usar essas experiências de outros países para aprender e talvez não repetir os mesmos erros. E quando se trata do processo concreto do eIDAS, há uma obrigação legal de ter um período de consulta de quatro semanas após os atos de implementação do Artigo 45.

Então, há uma maneira de ter um registro oficial de todas as contribuições em torno disso. Essa é uma ótima oportunidade para uma campanha. E, como alguém que tem, não tenho certeza de como será a votação amanhã e o conselho é mais difícil do que o parlamento, mas estamos pelo menos ao alcance de bloquear esses atos de implementação.

Então, definitivamente há uma chance e há um motivo para ter esperança se todos fizermos nosso trabalho e continuarmos a prestar muita atenção a essas questões muito técnicas. Ainda tenho esperança de que possamos chegar a um bom resultado e fazer com que esses grandes sistemas técnicos respeitem nossos direitos fundamentais.

**Robin Wilton - Internet Society:** Maravilhoso. Olha, acho que aproveitamos bem nossos 50 minutos com uma discussão incrível.

Tenho alguns agradecimentos. Gostaria de agradecer a Seema Karaman e à equipe da Mozilla por organizar este workshop e este painel, Thomas Loeninger, Dennis Jackson, Alexis Hancock. Como prometi, que seleção fantástica de especialistas no assunto. Muito obrigado por participarem hoje, como parte do Dia Global da Criptografia.

E, obrigado a todos que se conectaram para ouvir, participar e enviar suas perguntas. Muito obrigado. Espero falar com vocês na próxima vez também.

**Alexis Hancock - EFF:** Obrigado.

**Robin Wilton - Internet Society:** Obrigado. Adeus. Obrigado.