Entrevista de Julian Assange com Criptopunks

CRIPTOPUNKS – PARTE 1

[OFF] Eu sou Julian Assange. Editor do Wikileaks. Nós expusemos os segredos do mundo. *Esses documentos pertencem ao governo americano*. Fomos atacados pelos poderosos. *Os Estados Unidos condenam fortemente... Ei, pare de fazer perguntas! Ele infringiu a lei. Atirem ilegalmente no filho da...* Há 500 dias eu estou detido sem acusação, mas isso não nos deteve. Hoje estamos em busca de ideias revolucionárias que possam mudar o mundo amanhã.

PROGRAMA

JA: Uma guerra frenética pelo futuro da nossa sociedade está em andamento. Para muitos, esta guerra é invisível. De um lado, uma rede de governos e corporações vasculham tudo o que fazemos. Do outro, os Criptopunks. Ciberativistas virtuosos que são desenvoledores e também moldam políticas públicas. Este é o movimento que gerou o WikiLeaks.

Eu me juntei a três amigos Criptopunks Andy Müller-Maguhn, da Alemanha, Jeremie Zimmermann, da França e dos Estados Unidos, Jacob Appelbaum. Eu vou perguntar a eles: o futuro do mundo é o futuro da internet?

JA: Eu quero focar nas três liberdades básicas. Quando entrevistei o líder do Hezbollah, Hasan Nasrallah, houve uma pergunta se o Hezbollah...

JACOB A: O que é aquilo ali?

JA: Bem, ele tem sua própria prisão domiciliar também porque ele não pode sair de seu esconderijo secreto.

JACOB A: Eu não tenho certeza se eu faria esta comparação. Por favor, não faça esta comparação.

JZ: Você pode editar isso, certo?

JA: Eu quero voltar às três liberdades fundamentais liberdade de comunicação, liberdade de ir e vir e liberdade de interação comercial.

Se nós olharmos a transição de nossa sociedade global pela internet, quando nós fazemos esta transição, a liberdade pessoal de ir e vir permanece essencialmente inalterada, a liberdade de comunicação é ampliada tremendamente de muitas maneiras já que agora podemos nos comunicar com muito mais gente.
Por outro lado, ela também é tremendamente degradada, porque não há mais privacidade e nossas comunicações podem ser espionadas e são monitoradas e arquivadas, e como resultado, podem ser usadas contra nós.

AMM: A privacidade está disponível, mas a um certo custo.

JÁ: Sim, numa espécie de militarização deste tipo de interação e nossas interações econômicas têm sofrido estas mesmas consequências.

AMM: Julian, o que você diz não está errado, mas eu não estou certo se você pode distinguir entre o segundo e o terceiro ponto porque a internet como existe hoje é uma infraestrutura para nossa sociedade, nossa economia, nossa política, todas nossas coisas. Qualquer que seja a arquitetura de comunicação, Finanças são apenas bits. Este é apenas um dos usos da internet.

JÁ: Andy, você estudou telefones criptográficos por anos, segurança de ligações telefônicas, vigilâncias em massa que ocorrem em telecomunicações. Qual é o estado da arte nesta arte, no que tange à inteligência dos governos e à indústria de vigilância em massa?

AMM: Bem, armazenamento em massa gravando todas as telecomunicações tornou-se...

JÁ: Isso significa todas as chamadas por voz...

AMM: Sim, todas as chamadas por voz, todas conexões de internet. Na verdade, o que você tem que focar é... se você comparar o gasto no orçamento militar para vigilância e o custo também para soldados virtuais, os sistemas de armas convencionais custam muito mais dinheiro se você comparar com soldados virtuais ou vigilâncias em massa como essa, que são muito baratos. Isso é super barato se comparado com um só avião. Um avião militar comparado...

JÁ: ...Cem milhões.

JZ: Sim, mas nós temos duas questões aqui. Nós temos por exemplo o Eagle, o sistema da empresa Amesys que foi vendido para Gadaffi na Líbia. E no documento, sabe, no documento comercial, estava escrito “mecanismo de interceptação de alcance nacional”. Isso é uma grande caixa que você coloca em algum lugar e você escuta todas as conversas das pessoas do lugar. Nós podemos discutir sobre tecnologia... e eu estou muito interessado nisso...

JÁ: E isto, há 10 anos, era visto como fantasia. Era algo em que apenas gente paranoica acreditava. Mas o custo disso caiu ao ponto de até países com poucos recursos como a Líbia estarem fazendo isso com tecnologia francesa.

JZ: Exatamente! Agora isso é um fato. A tecnologia permite vigilância total de toda forma de comunicação. E há este outro lado da moeda, que é o que eu faço. Nós podemos admitir isso para o que você chama de uso tático. Existem alguns usos legítimos. Detetives investigando indivíduos maus e redes de suspeitos podem precisar disso sob supervisão de autoridade judicial para que seja permitido o uso de tais ferramentas. Mas a questão é onde usar esta supervisão judicial. Quem delegará para que o cidadão possa ter controle do uso de tais tecnologias? Isto é uma questão política. E quando nós atentamos a estas questões políticas - e nós as evocamos antes - tem políticos que são requisitados para apenas assinar algo sem entender a tecnologia subjacente.

JACOB A: É por isso que nós somos os que vemos essa efervescência sobre a guerra virtual. É por conta de algumas pessoas que parecem estar no comando de guerra falando sobre tecnologia como se entendessem isso. E todas essas pessoas falando sobre guerra cibernética, nenhuma delas – nem ao menos uma – fala sobre uma paz cibernética. Eles estão sempre falando sobre guerra porque este é o negócio deles e estão tentando cooptar tecnologia para isso. Enquanto nós não tivermos controle sobre nossa tecnologia, estas pessoas vão usá-la para os seus objetivos, para a Guerra, especificamente. Isso é uma receita para coisas bem assustadoras.

JÁ: Vejo que agora há uma militarização do ciberespaço porque nós temos revistas em todas as fronteiras nacionais...

JACOB A: Sistemas-alvo...

JÁ: E tem os hackers militarizados operando em massa com programas para atacar setores da internet e espionar partes da internet.

AMM: Posso discordar sobre o uso de hackers neste contexto. Você está falando de soldados usando computadores com fins militares. Isto não hacking e eles não são hackers.

JÁ: Tudo bem, não vamos entrar na definição de hacker. Mas, a questão é que se trata de vidas civis. Não vemos tanques vindo... Esta sala é um caso à parte, mas a maioria das pessoas não veem os tanques ou suas salas de estar sendo grampeadas normalmente, ou até suas comunidades locais. Mas agora publicamos toda nossa vida privada no Facebook, nos comunicamos pela internet, nos comunicamos por celulares que estão ligados à internet e os militares detêm o controle, as agências de inteligências controlam estes dados e os examinam. Ou seja, é uma espécie de militarização da vida civil.

AMM: Totalmente!

JZ: Existe uma questão sobre se devemos ou não regular o ato de comprar e possuir e usar esta tecnologia.

JÁ: Você fala do equipamento de interceptação que pode cobrir toda um país ou uma cidade ou...

JZ: Uma arma nuclear, não se pode vendê-la facilmente. Você não pode vender uma arma nuclear e os países que querem construir uma podem ter problemas. É uma tecnologia que é regulada. E eles fazem desta forma quando falamos de sistemas bélicos... Então, eu acho que o debate pode ser sobre se estas tecnologias podem ou não ser consideradas bélicas.

JACOB A: São armas, e não há dúvida que são usadas como arma em lugares como a Síria ou a Líbia. Eles usam especificamente esse equipamento de vigilância para atingir politicamente pessoas na Líbia, alvejam pessoas no Reino Unido usando equipamento francês que seria ilegal na França. Eles vendem isso com total consciência.

AMM: Eles nunca fariam isso, certo?

JACOB A: Bem... Eles foram pegos por seus próprios documentos internos no Spy Files, certo?

JÁ: Jeremy...

JZ: Autoridades e civis é de fato a maior questão que desafia a estrutura de todas democracias e a forma como elas funcionam. Mas agora é a hora apropriada para lembrar que também há vigilância privada e potencialmente coletas massivas privadas de dados. Na verdade, é só olhar o Google. O Google sabe, se você é um usuário padrão do Google, o Google sabe com quem você se comunica, quem você conhece, do que você pesquisa, potencialmente sua orientação sexual, sua religião e pensamento filosófico mais que sua mãe e talvez mais que você mesmo. O Google sabe quando você está online e quando não está.

AMM: Você sabe o que você pesquisou há dois anos, três dias e quatro horas atrás? Você não sabe. O Google sabe, certo?

JZ: Não... Na verdade, eu tento não usar mais o Google exatamente por estas razões.

JZ: Mas o que eu digo é que não é apenas a vigilância promovida pelo Estado. É a questão da privacidade, do modo como informações são manuseadas por terceiros e o conhecimento verdadeiro que as pessoas têm do que está sendo feito com essas informações.

JÁ: Você pode falar também do Facebook, Jeremy.

JZ: Bem... na verdade, eu não uso o Facebook. Então, eu não sei muito sobre ele. Graças ao Facebook, você vê o comportamento atual dos usuários que estão muito satisfeitos em entregar qualquer tipo de informação pessoal. E é claro que quando você vê adolescentes mandando fotos deles mesmos bêbados, ou o que seja, eles podem não a noção do que isso significa – de que todo o resto do mundo, potencialmente por muito tempo, terá acesso a esta informação. E então o Facebook arma seu negócio confundindo esta linha entre privacidade, amigos, publicidade e está inclusive

armazenando informações quando você pensa que só se trata dos seus amigos e das pessoas que você ama.

JÁ: Esta linha entre governo e corporações Eu acho… que está confusa! A Agência de Segurança Nacional, que é a maior agência espiã no mundo, antes tinha dez prestadores de serviços diretos em seus registros com quem trabalhavam. Agora ela tem, dois anos atrás, mais de mil. Existe uma propagação, uma deturpação da fronteira entre o que é governo...

JZ: E podemos dizer que as agências americanas de espionagem têm acesso a todos dados armazenados do Google.

JÁ: Eles têm.

JZ: E todos dados do Facebook. Logo, de algum modo, Facebook e Google, talvez sejam suas extensões...

JÁ: Você já foi intimado?

JACOB A: Eu quero dizer, eu sei que...

JÁ: Recebemos duas ontem.

JACOB A: No nosso caso com o Twitter até agora... O que infelizmente eu não posso comentar porque eu não vivo em um país livre...

JÁ: Estas intimações também são secretas? Quer dizer, vocês são proibidos de falar sobre elas? Mas isso é inconstitucional, não?

JACOB A: Não é certo. Você sabe que no caso do Twitter é público que nós perdemos a alegação na qual dizíamos que revelar estas informações ao governo causaria danos irreparáveis e eles não podem esquecer estes dados uma vez que os receberem. E o governo disse: "Bem, sua alegação foi negada". Agora o Twitter tem que revelar estas informações. Nós estamos no processo de apelação especificamente sobre o sigilo de categorizações. E eu não posso falar sobre isso porque estamos no processo de apelação. Mas a esta altura, a corte descobriu que eles alegaram que na internet você não tem expectativa de privacidade, quando você revela informações espontaneamente a terceiros. E por falar nisso, todos na internet são terceiros. Disseram que a situação é como com a privacidade bancária e os números telefônicos. Você espontaneamente revela o número à companhia telefônica ao utilizá-la. E você sabia disso, certo? Mas, quando você usa um telefone, você obviamente está dizendo "eu não espero privacidade sobre os números digitados". As pessoas não entendem como a internet funciona. Elas também não entendem as redes telefônicas. Mas os tribunais julgaram constantemente que este é o caso. É loucura absoluta imaginar que nós damos nossas informações pessoais a estas companhias, e as companhias essencialmente se tornaram uma polícia secreta privatizada. No caso do Facebook, nós temos vigilância democratizada, em vez dar propinas em troca de informações, como a Stasi fazia. Agora a recompensa é… Você

consegue transar. Sabe, eles vigiam seus amigos e são como... "Fulano e beltrana noivaram... Oh, Fulano e Beltrana terminaram… Agora eu sei a quem ligar, certo?". E esta é a diferença entre uma privacidade por meio de políticas e uma privacidade por modelo de abordagem, que é necessária para criar sistemas seguros de fato. Digo, quando você tenta espionar pessoas, e você sabe que vive num país que explicitamente espiona pessoas então você... Veja, se o Facebook colocasse seus servidores na Líbia de Gadaffi ou na Síria de Assad, isso seria absolutamente negligente. Então, sabendo desta realidade, estas empresas possuem responsabilidades éticas sérias que se baseiam no fato de que estão construindo estes sistemas e fizeram uma escolha basicamente econômica – a a de vender seus usuários. E isto nem é algo técnico. Não se trata de uma questão sobre tecnologia, de forma alguma. Isto é sobre economia, e eles decidiram que é mais importante colaborar com o Estado, vender seus usuários e violar a privacidade deles e ser parte do sistema de controle, ser pago por ser parte de uma cultura de vigilância, ser parte de uma cultura de controle em vez de resistir a isso. Então eles instalaram, eles fizeram parte disso. São cúmplices e responsáveis.

JÁ: Eu quero focar nisso: o que eu vejo como uma diferença entre uma perspectiva Criptopunk americana e uma perspectiva europeia. Eu acho bem interessante. A segunda emenda americana dá o direito de portar armas. Agora pouco, assistindo a imagens que um amigo fez nos EUA sobre o direito de portar armas… Logo acima de uma loja de armas está escrito "Democracia armada e carregada". E este é o modo como vocês asseguram que não se chegue a um regime totalitário. As pessoas se armam e se estiverem suficientemente revoltadas, então elas simplesmente pegam suas armas e reconquistam o poder à força. Vamos voltar à elaboração de códigos secretos, que o governo não possa espionar isso foi de fato a munição na guerra que lutamos nos anos 1990 para tentar tornar a criptografia acessível a todos. O que nós, em grande parte, conseguimos na verdade.

JACOB A: No Ocidente?

JÁ: Sim, no Ocidente. Nós conquistamos isso em grande parte e agora a criptografia está em todos os navegadores, mas agora talvez seja deturpada de diversas maneiras. É a ideia de que você não pode confiar que um governo implemente as políticas que prometeu, e por isso nós precisamos usar como armas as ferramentas subjacentes, ferramentas criptográficas que nós controlamos como uma forma de uso da força, de modo que um governo, não importa o quanto tente, se os códigos são bons ele não consegue invadir suas comunicações diretamente. Talvez grampear a sua casa ou outra coisa...

JACOB A: A força da autoridade é derivada da violência. As pessoas deveriam conhecer criptografia. Nenhuma quantidade de violência resolverá um problema matemático. E esta é a chave-mestra. Não significa que você não pode ser torturado, não significa que eles não podem tentar grampear sua casa ou te sabotar de alguma forma, mas se eles acharem alguma mensagem criptografada, não importa se eles têm força de autoridade. Por trás de tudo que eles fazem, eles não podem resolver um problema matemático. No entanto, isto não é algo óbvio para as pessoas que não são técnicas e isso tem de ser levado para as casas dessas pessoas. Se nós pudéssemos resolver todos esses problemas

matemáticos seria uma história diferente e claro que o governo também conseguiria se qualquer um pudesse. Mas esta é a diferença, certo? É algo que muda tudo.

JÁ: Assim como você pode construir uma bomba atômica, existem problemas reais que você pode criar e que até o Estado mais forte não poderá deter diretamente. E eu acho que foi muito interessante para os libertários californianos e outros que acreditavam nessa forma de democracia armada e carregada. E aqui temos uma forma muito inteligente de fazer isso com alguns sujeitos que, com a criptografia, enfrentam o poder absoluto das superpotências mundiais. E continuamos fazendo isso, talvez um pouco. Mas creio que o possível resultado disso é que são forças econômicas e políticas realmente fortes, como disse Jeremy. E a eficiência real de suas tecnologias, em comparação com o número de seres humanos, significa que aos poucos vamos rumando para uma sociedade de vigilância global totalitária. E por totalitário quero dizer uma vigilância total e que talvez haverá algumas últimas pessoas livres. E estas últimas pessoas livres serão aqueles que entendem como usar isso, a criptografia, para proteger-se desta vigilância total e completa. Estamos rumando em direção a este cenário?

JZ: Primeiramente, se você olhar isso de uma perspectiva mercadológica, eu estou convencido de que há um mercado da privacidade que tem sido amplamente inexplorado. Então, talvez haja uma demanda econômica para empresas desenvolverem ferramentas que deem a usuários a habilidade individual de controlar essas informações e a sua comunicação. Talvez esta seja uma forma para resolver este problema. Não tenho certeza que funcione por si só. Mas isso pode acontecer, não sabemos ainda. É interessante notar que... O que você descreve é o poder dos hackers de um certo modo. Hackers no sentido puro da palavra, não criminosos. Um hacker é um entusiasta de tecnologia, alguém que gosta de entender como a tecnologia funciona. Não ser escravizado pela tecnologia, mas sim aprimorá-la. Eu acho que vocês dois, quando tinham 5 ou 6 anos, tinham uma chave de fenda e tentaram abrir aparelhos para entender como era dentro, não? Isto é que é ser um hacker. Os hackers construíram a internet por muitas razões, e também porque era divertido, e as desenvolveram e entregaram para todos. Assim, empresas como o Google e o Facebook se deram conta de que podiam construir um modelo de negócio capturando informações pessoais dos usuários. Mas mesmo assim, nós vemos uma forma de poder nas mãos dos hackers. E o que me interessa hoje em dia é que nós vemos estes hackers ganhando poder, inclusive na arena política.

JÁ:

Esta radicalização política da juventude na internet nestes dois últimos anos especialmente... Você tem conversado com gente de todo mundo sobre anonimato. Elas querem privacidade em relação ao próprio governo. Você deve ter visto esse fenômeno em muitos países. Isto é algo significativo?

JACOB A: Lógico! Quero dizer, eu acho que é totalmente significativo. Eu fui à Tunísia logo depois da queda do regime de Ben Ali. E você vê que há uma espécie de despertar para isso. Eu acho que você está equivocado ao dizer que isso só aconteceu nos últimos

anos. E me desculpe por dizer isso no seu show. Mas você é parte da radicalização da minha geração. Tipo, eu seria um Criptopunk de terceira geração se eu fizesse parte disso. E você sabe que o trabalho que você e Ralf fizeram sobre o sistema de arquivos Rubberhose foi parte do que inspirou meu trabalho com criptografia. O sistema de arquivos criptografados que ele escreveu foi uma resposta a coisas como as forças de investigação no Reino Unido, onde o Estado decidiu que uma regulação negativa era a resposta à criptografia. Ele pode, por exemplo, obter a sua senha. Você sabe, no caso de Julian quando eles criaram isso foi por conta de regimes opressivos que torturavam pessoas para que dessem suas senhas. E eles tinham que dizer várias. Como resposta à tortura. E eu notei, quando vi que isso existia, que você pode usar a tecnologia para dar poder às pessoas comuns para mudar o mundo. E os criptopunks estão voltando, eu quero dizer... Isso realmente vem de muito antes. Você conhece a antiga lista de email, o mailing list Criptopunk de Tim May, e lendo todos seus antigos posts... Quer dizer, toda uma geração de pessoas se radicalizaram porque percerebam que não eram mais fechados em pequenos núcleos, que elas podiam tomar um tempo para escrever um programa que poderia depois ser usado para dar poder a milhões de pessoas. Mas o uso destas ferramentas tem algumas consequências não calculadas. Porque as pessoas que criaram o Google não o fizeram para criar a melhor máquina de vigilância que já existiu. Mas foi isso que se criou. E assim que as pessoas começam a notar isso, começam a enviar aquelas cartas para a Agência de Segurança Nacional, certo?

JZ: Eu acho que há três pontos cruciais nisso que você disse...

JACOB A: Só três!

JZ: Sim, dentre outros… Um deles é o regime autoritário e os poderes que regimes autoritários têm numa era de tecnologias digitais. No caso do regime de Ben Ali, isso é óbvio. Em tantos regimes como os de hoje é óbvio que você pode decidir o que as pessoas podem aprender ou com quem elas podem se comunicar. E isso é um poder tremendo. Isto deveria ser enfrentado. E a internet, a internet livre, é uma ferramenta de enfrentamento disso. Outra coisa que você disse… Bem, esta é sua área de atuação, e é construir ferramentas para... implementar uma tecnologia melhor. Uma tecnologia que possa solucionar problemas como a censura. Mas basicamente, construir ferramentas que façam parte de uma infraestrutura que nos ajude a derrubar ditadores. E ainda tem a questão da narrativa política: o pretexto usado todos dias por políticos na mídia é que todos nós vamos morrer por causa do terrorismo. E portanto precisamos do Patriot Act. Pornógrafos infantis estão em todo lugar. Existem pedófilos-nazistas por toda internet. Portanto, nós precisamos de censura…

JACOB A: Aqueles malditos pedófilos-nazistas!

JZ: É, pedófilos-nazistas! A URL Peadonazi.com já está reservada. E os artistas vão morrer e não haverá cinema mais, logo nós temos que dar o poder a Hollywood para censurar a internet e assim por diante... Então, eu acho... De novo a internet é uma ferramenta... A internet pode não ser o antídoto para a narrativa política. A narrativa política se baseia no emocional e se baseia no fim imediato que se dá em curto prazo. Uma informação aparece e desaparece 24 horas depois e é substituída por outra,

sucessivamente. Com a internet, eu sinto que nós estamos construindo o que chamo de "tempo da internet". Como a grande internet não esquece, nós podemos construir por anos, dia após dia, dossiês, e podemos refiná-los... Isto é o que fizemos nos últimos três anos contra o ACTA. Nós fizemos nossa própria linha política com o tempo da internet, com análise precisa, com trabalho duro, conectando pessoas para participar.

JÁ: Nós vencemos a narrativa. Mas nos bastidores, tratados bilaterais secretos são armadas, e eles estão conseguindo o mesmo tipo de resultado de qualquer maneira, isso está deturpado.

JACOB A: Uma coisa que devo pontuar é que as pessoas que estão lutando contra o ACTA estão na verdade... Estão usando tecnologia, e a tecnologia as permite resistir. Mas é na verdade a ação das pessoas comuns que é importante entender aqui. O tecno-blá-blá-blá não é o importante. O que importa é pessoas se envolvendo de fato na narrativa e mudando isso enquanto elas ainda têm o poder de fazê-lo. E o aspecto humano disso é o fato mais importante. Parte disso e o fato do WIkiLeaks ter lançado documentos que permitem isso. É o compartilhamento de informação que é importante. Mas também são as pessoas que pegam esta informações importantes e passam pra frente porque ali há ao menos o argumento de que nós vivemos numa democracia. De que somos livres, de que deveriamos, pelo menos, ser governados por consentimento. Então, se todos entendem o que se passa e nós acharmos que não é algo que nós consentimos, então será difícil continuar desse jeito e apenas aprovar estas coisas através de leis sem o consentimento daqueles que são governados.

JZ: Trata-se de aumentar o custo politico para os governantes de se tomar essas más decisões. E nós podemos fazer isso coletivamente com uma internet livre, contanto que ela esteja em nossas mãos.

JÁ: Espere…

JZ: Antes que você seja pessimista, por favor…

END CREDITS

Tradução: Marcus V F Lacerda

Agência Pública – apublica.org