Cidadania, Privacidade e Vigilância no Mundo Virtual

Citizenship, Privacy and Surveillance in the Virtual World

Gustavo Sumares
Universidade de São Paulo. Escola de Comunicações e Artes, São Paulo, Brasil

2013 foi um ano marcante para a história da internet. As revelações de Edward Snowden sobre os programas de espionagem virtual da National Security Agency (NSA) dos Estados Unidos jogaram luz sobre um aspecto bastante desconcertante da nossa vida virtual: toda a nossa atividade na internet pode estar sendo monitorada e armazenada em algum servidor, em algum lugar, e essas informações sobre nossos hábitos online podem vir a ser usadas contra nós algum dia.

Além disso, foi também um ano marcado pelas discussões sobre o Marco Civil da Internet, projeto de lei do poder executivo, redigido coletivamente através de um blog, que tem como objetivo regular o uso da internet e a atuação das operadoras de telecomunicações, estabelecendo princípios para o funcionamento da rede.

O professor doutor Jorge Alberto Silva Machado leciona no curso de Gestão de Políticas Públicas da Escola de Artes, Ciências e Humanidades (EACH-USP), é docente colaborador do *Programa de Pós-Graduação em Sistemas de Informação* da USP e um dos coordenadores do *Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação* (GPOPAI). Ele conversou conosco sobre o potencial político da internet, as ameaças à sua neutralidade e sobre como podemos proteger nossas informações pessoais num ambiente tão fortemente vigiado quanto a internet.

Jorge Alberto Silva Machado
é professor doutor da Escola de Artes, Ciências e Humanidades da Universidade de São Paulo

Rev. Cult. e Ext. USP, São Paulo, n. 11, p.19-25, maio 2014
DOI: http://dx.doi.org/10.11606/issn.2316-9060.v11i0p19-25

Revista Cultura e Extensão USP – *Como a internet pode contribuir para a vida política das pessoas?*

Jorge Machado – Acho que a internet permite mais transparência, permite que as pessoas se conectem e possam trocar ideias em função de seus interesses: é um espaço público de formação de opinião muito importante, que não havia antes. E já ganhou tal dimensão como meio livre e aberto que a própria imprensa tradicional hoje se pauta também pelo que acontece na rede, nas redes sociais, nos blogs e fóruns, então, hoje a internet tem uma importância fundamental. Mas nós ainda não vimos todo o impacto que ela pode ter porque boa parte da população ainda não está conectada, ou não está bem conectada (tem uma conexão muito ruim, o que proporciona outra experiência de navegação). Mas o potencial é enorme e a gente vê isso nas mobilizações que estão acontecendo por todo o país, até mesmo nos "rolezinhos", o que revela que a periferia também está usando essa rede.

RCE – *É como se fosse, então, a "praça" onde as pessoas se reuniam para discutir notícias e falar de política?*

JM – Sim, e de certa forma em uma escala muito maior, sem os limites físicos de uma praça. No mundo virtual, as pessoas se reúnem em função de interesses comuns, não apenas por compartilhar um espaço. Assim, o potencial de troca é enorme. Da mesma forma, pode acontecer de você publicar coisas que ninguém vai ler – isso depende de muitos fatores. Mas essa enorme liberdade é algo sempre positivo na rede.

RCE – *Quer dizer, o potencial de ser lido sempre existe, o que não é o caso de um indivíduo que produz de forma isolada.*

JM – Sim, sempre existe. Da rede surgiram muitos escritos e escritores: gente que produz blogs de diferentes assuntos, que acabam repercutindo bastante, pessoas que eram desconhecidas e que hoje falam dos mais variados temas através de blogs e, com isso, conseguem oportunidades econômicas, profissionais etc. Então é um ambiente inovador, que realmente mudou a forma como as pessoas se comunicam e como a sociedade se organiza política e socialmente.

RCE – *Como o senhor vê a participação da internet na questão, por exemplo, dos "rolezinhos", ou nas manifestações do ano passado?*

JM – Possivelmente, nada disso aconteceria sem a internet. Ela foi o meio para que isso acontecesse. Antes disso, você tem as marchas: *marcha da maconha*, *marcha da liberdade*, *marcha das vadias*, protestos que foram articulados nas redes sociais, nos fóruns e grupos criados em cada cidade. Então, eu acho que esse é um fenômeno de escopo muito amplo, que mostra que as redes sociais são ferramentas muito maleáveis. Mas há um fenômeno de concentração da internet: ela já não é a mesma de quando foi criada. Antigamente, havia muitos servidores e as pessoas podiam criar negócios próprios com uma estrutura mínima, havia muita competição; hoje, você tem algumas poucas e grandes plataformas, que são privadas e fechadas. O Facebook é um grande exemplo disso. Essa é uma preocupação que foi crescendo ao longo do tempo e que é quase como um pesadelo que se realiza: as corporações tomando conta da internet, privatizando esse espaço. Outra coisa que pode mudar a cara da internet é a ameaça à neutralidade da rede, que é outra questão que está sendo pouco discutida porque ainda não estamos vendo seus efeitos de forma clara.

> "ISSO SIGNIFICA QUE A INTERNET É UMA REDE *NEUTRA*: OS CONTEÚDOS QUE TRAFEGAM POR ELA, NÃO CABE AO PROVEDOR DE ACESSO OU À OPERADORA DE TELEFONIA DIZER QUAIS TÊM PRIORIDADE. SERIA COMO A NOSSA REDE ELÉTRICA: A ELETROPAULO NÃO VAI FALAR QUE VOCÊ NÃO PODE LIGAR O CHUVEIRO, SÓ PODE USAR A GELADEIRA E AS LUZES DA CASA."

RCE – *O que é o princípio de neutralidade da rede?*

JM – Em minha opinião, isso significa que a internet é uma rede *neutra*: os conteúdos que trafegam por ela, não cabe ao provedor de acesso ou à operadora de telefonia dizer quais têm prioridade. Seria como

a nossa rede elétrica: a Eletropaulo não vai falar que você não pode ligar o chuveiro, só pode usar a geladeira e as luzes da casa. O novo modelo de negócio que está sendo feito pelas "telecoms" no mundo inteiro é oferecer uma assinatura que possibilita, por exemplo, acesso ao Facebook, mas que não permite acesso a outros sites. Com isso, essas empresas estão interferindo na conexão que o usuário faz. Elas têm um filtro: dependendo do pacote de serviços contratado pelo usuário, ele pode ou não acessar determinados sites. É como se a internet, um dia, se tornasse igual à TV a cabo. E isso não era para acontecer, mas já está acontecendo, e pode ter um efeito nefasto na internet. Essa é a grande preocupação do momento, além da questão da privacidade.

RCE – *Defender o princípio de neutralidade não reforça a questão da anonimidade e da irresponsabilidade de comportamento na internet?*

JM – Isso é uma questão, eu diria, secundária. A primeira questão é a gente pensar a privacidade como um direito humano. O direito à privacidade é um direito fundamental: ninguém pode abrir sua correspondência ou escutar seu telefone sem autorização judicial. Então, as comunicações sigilosas são um padrão. O direito à privacidade é fundamental para a liberdade de expressão, porque se você sabe que as pessoas estão te ouvindo, você não vai falar da mesma maneira como falaria de forma "protegida", e isso afeta a liberdade de expressão. É algo muito perigoso porque a liberdade de expressão é fundamental num sistema democrático. Se você cria um sistema de vigilância global, você vai causar um impacto muito grande na sociedade nesse sentido. Quanto à questão do anonimato, ele pode ser quebrado no caso de uma pessoa que cometeu algum tipo de delito. Mas você não pode partir do pressuposto de que todas as pessoas são suspeitas. Aí, como padrão, você teria o fim da privacidade para facilitar qualquer tipo de investigação. Muita gente da área de segurança, da polícia, como não conhece essa discussão [sobre direitos humanos], acha que seria o ideal, porque daí seria muito mais fácil para investigar. Um problema da privacidade também é que a informação sobre o comportamento das pessoas (seus hábitos de navegação, suas preferências) gera um valor econômico que também pode ser empregado pelas empresas. Elas podem cruzar uma série de informações, traçar o perfil do consumidor e vender esse perfil para ajudar na competição de mercado. Por isso, é muito atrativo para as empresas armazenar todo tipo de informação.

RCE – *E os usuários ainda não parecem estar cientes de que essa informação gera valor para as empresas.*

JM – As pessoas não têm noção disso. Elas estão abrindo mão da sua privacidade. Se você for usar o Facebook em um dispositivo móvel, você abre mão de praticamente tudo: o Facebook pode controlar seu dispositivo e ter acesso a mais informações mesmo quando você acessa a rede social através de um navegador. Mas, se você não fizer isso, não consegue usar o aplicativo de uma forma eficiente. As pessoas são muito estimuladas a baixar esses aplicativos, e geralmente elas não leem os termos de uso e vão abrindo mão da sua privacidade. Essa é uma questão importante, porque hoje há quem fale que "a informação é o petróleo do século XXI": quanto mais informação você tem sobre as pessoas, mais vantagens competitivas você vai ter. Então essas grandes empresas oferecem plataformas, não cobram nada e falam "coloque tudo aqui". O Google fala "põe tudo na nuvem", te dá uma conta de e-mail infinita, uma série de serviços que você pode utilizar e eles vão coletando informações suas. E eles têm uma quantidade de informações gigantesca, que qualquer serviço de inteligência gostaria de ter sobre as pessoas, porque eles sabem *tudo*. E, então, aparecem as revelações que a gente teve no ano passado com o Snowden.

"HOJE HÁ QUEM FALE QUE 'A INFORMAÇÃO É O PETRÓLEO DO SÉCULO XXI': QUANTO MAIS INFORMAÇÃO VOCÊ TEM SOBRE AS PESSOAS, MAIS VANTAGENS COMPETITIVAS VOCÊ VAI TER."

RCE – *E no caso do Snowden, era uma espionagem com o aval do Estado, sobre seus cidadãos e o de outros países, o que parece ainda mais grave.*

JM – E ainda há indícios de que eles podem utilizar esse sistema de monitoramento para fins de espionagem industrial, como, por exemplo, no caso dos dados vazados sobre a Petrobras e o Ministério de Minas e Energia. Hoje, qualquer centro de inovação cientifica e tecnológica, seja público ou privado, corre o risco de ter todas as suas informações acessadas pelo governo dos Estados Unidos ou outros governos que, porventura, estejam filtrando informações nos cabos de telecomunicações ou tenham relação com alguma empresa de software proprietária, cujos programas têm códigos que não podem ser auditados. Duas questões aí envolvidas são fundamentais para a questão da privacidade: primeiro, para você se proteger, você tem que criptografar. Segundo, você tem que usar softwares que permitam algum tipo de auditoria, porque, caso contrário, você não sabe o que tem neles. Quem programa é quem manda. Em qualquer tipo de dispositivo: quem fez o programa e determinou como funciona esse dispositivo é quem está mandando. Então, se você não tem o conhecimento desse código, você não sabe exatamente o que ele está fazendo, que tipo de informação ele está enviando e para quem. Isso já acontece há muito tempo, mas hoje passou a ser uma preocupação. Em geral, centros de pesquisa e inovação no Brasil não têm o cuidado de usar uma criptografia segura.

> "HOJE, QUALQUER CENTRO DE INOVAÇÃO CIENTÍFICA E TECNOLÓGICA, SEJA PÚBLICO OU PRIVADO, CORRE O RISCO DE TER TODAS AS SUAS INFORMAÇÕES ACESSADAS PELO GOVERNO DOS ESTADOS UNIDOS OU POR OUTROS GOVERNOS."

RCE – *E o conhecimento sobre programação e tecnologia de telecomunicação ainda é restrito a alguns grupos: são poucas as pessoas que conseguiriam saber exatamente o que os programas fazem e perceber alguma irregularidade nisso.*

JM – Eu acho que a segurança só pode ser validada por meio de uma comunidade. Você não precisa conhecer o código, mas precisa saber que pessoas de confiança já auditaram o código dos programas que você utiliza. Caso contrário, ele pode ter o chamado *backdoor*, a porta dos fundos [maneira pela qual o programa enviaria informações sem o conhecimento do usuário]. Recentemente foi revelado que os roteadores D-Link, por exemplo, que quase todo mundo usa, têm um *backdoor*, um código malicioso que fica mandando informações sobre as páginas que você visita e conecta seu dispositivo a um servidor remoto. Isso foi mais uma descoberta que mostra o atual contexto em que vivemos, em que você não pode confiar nos dispositivos que adquire. Existem vários pontos de fragilidade. Pode ser no hardware, na transmissão da informação ou até a própria criptografia pode ser quebrada, e eu acho que isso deveria ser tema de uma política pública, em que o governo pense no conhecimento gerado nas nossas universidades e também na questão de segurança estratégica do Estado. Mas é comum a gente trocar e-mails com gente do governo e eles passarem um endereço do Gmail para mandar um arquivo, ou colocarem documentos no Google Docs para que a gente trabalhe em cima deles, e isso é exposição pública. Então, o governo não tem muita preocupação com isso, embora haja um esquema de vigilância global. Não é uma teoria conspiratória. O governo americano não negou nada. A única segurança que a gente pode ter é se utilizarmos uma criptografia segura e programas que possam ser auditados por alguma comunidade confiável. Fora isso, nós estamos expostos.

RCE – *E se você usa criptografia é pior ainda, porque eles percebem que você estava tentando esconder a sua navegação, não?*

JM – Se você usar criptografia, automaticamente você vai passar a ser alvo da NSA. Então, na comunidade de pessoas que trabalham com isso, há esse entendimento: se você usa criptografia, você se sente seguro, mas passa a ser alvo, porque pouca gente usa criptografia. Mesmo entre quem usa software livre, tal cuidado é pouco adotado. Mas se todo mundo

começar a usar, vai ser difícil para eles ter todas essas pessoas como alvo. Então, por isso, é muito bom que as pessoas comecem a usar, porque vai tornar o trabalho de vigilância muito mais oneroso. Há alguns tipos de criptografia que são acessíveis a qualquer usuário e que são muito difíceis de quebrar. Uma frase do Jacob Applebaum [pesquisador norte-americano de segurança de computadores] diz: "não existe violência que possa resolver uma equação matemática". Quer dizer, a matemática é muito mais forte. Vai ser preciso muito trabalho computacional para quebrar pela força bruta a criptografia.

RCE – *Como desdobramento do caso Snowden, o marido do Glenn Greenwald [jornalista que divulgou as declarações de Snowden], David Miranda, ficou detido durante muitas horas no Reino Unido, o que parece mandar um recado aos jornalistas que estejam dispostos a divulgar informações perigosas sobre o governo.*

JM – No caso, ele encontrou também a Laura Poitras, que é a colaboradora do [Julian] Assange [fundador da Wikileaks]. Mas em todo caso, foi um recado dado. Vale lembrar que, na mesma época, alguns dias antes de ele ser preso, a Wikileaks liberou arquivos de segurança em *torrents*. São arquivos gigantescos, o maior deles acho que tinha 256 gigabytes. Especula-se que lá estão, parcial ou totalmente, documentos da NSA. Mas os arquivos foram criptografados e não se liberou a chave que pode decriptar. Então, o que acontece: existem cópias dos arquivos de segurança da Wikileaks, mas ninguém pode abrir, porque ninguém consegue quebrar aquela criptografia. É muito pesado. Mesmo usando um supercomputador, daqueles que fazem previsão meteorológica, você não consegue quebrar. Mas, se o Snowden for preso, pode ser que, em instantes, alguém libere a chave criptográfica. Isso pode ser algo terrível. Por exemplo, nesses arquivos pode estar a lista dos nomes e a localização de todos os agentes da NSA no mundo. É algo super perigoso. Eu não sei se estaria aí, mas logo na primeira entrevista que ele [Snowden] deu, ele disse "eu tenho acesso à lista de todas as pessoas que trabalham para a NSA". O Snowden era o principal administrador do sistema, então o estrago que ele fez foi muito grande, pois como tinha acesso a todas as senhas do sistema, ele logava com a senha dos usuários. Tiveram que entrevistar centenas de funcionários da própria NSA para poder fazer o levantamento de onde ele chegou, que informações ele tem, mas isso é algo incompleto também. Ninguém sabe que informação ele tem, quem tem cópia disso, o que mais ele pode liberar. Isso, eu diria, é a segurança dele.

RCE – *Com relação a Wikileaks, não existe perigo em expor certas informações sigilosas do governo?*

JM – Com certeza, mas a Wikileaks tem um instrumento de filtragem. Eles têm jornalistas de confiança que recebem a informação e levam em consideração se essa informação pode colocar em risco a segurança nacional ou a vida de uma pessoa. Assim, há documentos que eles revelam só uma parte, ou que eles tarjam. Eles têm uma responsabilidade nesse sentido. Acho que liberar todos os arquivos da NSA de uma vez é algo que eles só fariam numa situação muito extrema, em que o Assange ou o Snowden fosse assassinado, algo assim. Não sei se essa é a percepção que as pessoas têm em geral, mas eles me parecem muito cuidadosos. Eles sempre tiveram o cuidado de preservar a identidade das pessoas. Às vezes, alguns nomes apareceram porque, claro, eram pessoas que tinham responsabilidade política e pública, mas cujas vidas não estavam em risco. E, até onde eu sei, não houve caso de uma pessoa que esteve com a vida em risco ou foi assassinada em função das revelações da Wikileaks. Então, eles têm esse cuidado. Mesmo que você acesse os sites que eles criaram, você pode ver que as informações ali estão tarjadas também. Tem um banco de dados riquíssimo, uma informação histórica muito interessante para pesquisa, mas, mesmo assim, tem algumas restrições. Tudo aquilo foi lido por alguém. É um trabalho colaborativo, custa muito tempo, mas eles fizeram isso. Então de falta de cuidado ninguém pode acusar o Assange.

RCE – *Mas, por mais que tenha um filtro, não é um filtro muito tênue? Porque são questões globais, e a*

decisão sobre o que sai ou não está na mão de umas poucas pessoas.

JM – Com certeza. Mas, se fosse o filtro do governo americano, não iria aparecer nada. Então, você tem dois extremos. É difícil avaliar até que ponto a sociedade está reagindo ou vai reagir em função dessas revelações. Eu acho que o fato dessas informações chegarem à opinião pública é um grande ganho. Mas mudanças concretas são algo gradual. Esse fórum que discutiu a governança da internet no Brasil em abril, por exemplo, é resultado da diplomacia brasileira e de outros países tentando tirar o controle dos Estados Unidos sobre a estrutura da internet. É uma coisa que não será fácil de ser feita porque envolve a infraestrutura da rede. Enquanto eles fornecerem boa parte da infraestrutura, essa vigilância vai continuar acontecendo de alguma forma. O que o governo brasileiro já está fazendo com outros governos é buscar mudar o tráfego de dados, por exemplo. Mas isso envolve o mercado também, porque o custo de hospedagem é muito mais barato nos Estados Unidos. Enfim, isso descentraliza a internet, mas não garante a privacidade. Nós podemos começar a ser monitorados também pela China ou pela Rússia. Na verdade, a única garantia que a gente tem de que a privacidade pode ser respeitada é através da criptografia. Há uma discussão também sobre como podemos ter redes livres. Ter sub-redes locais? Nós conseguimos ter transmissão de dados sem passar pelos satélites? Então, você tem várias alternativas que estão sendo discutidas, mas a melhor alternativa a curto prazo é a utilização generalizada de criptografia. As pessoas estão percebendo, primeiro, a privacidade como um direito humano importante e fundamental para a liberdade de expressão, e, segundo, como podem, com um pouco de conhecimento, utilizar a criptografia no seu próprio computador e conseguir ter uma navegação privada.

RCE – *O senhor acha que, no Brasil, nós conseguimos usar a internet para melhorar a nossa vida política?*

JM – Eu acho que sim, mas ainda há um potencial muito maior. Existem os portais de transparência, mas quem vai lá pesquisar a informação, ver os contratos, ver quem está recebendo o quê de quem, o quanto está sendo pago nas aquisições de produtos e serviços do Estado? Poucas pessoas acessam os dados e têm essa capacidade de captar, analisar e fazer uso dessa informação. Primeiro, as pessoas ainda têm dificuldade de utilizar essa informação. Segundo, muitas informações públicas são colocadas de formas inadequadas para exploração, como, por exemplo, a publicação em *.pdf*. Terceiro, há inconsistência nos dados públicos. E quarto, no que se refere ao combate à corrupção, nem sempre aquilo que está no papel é o que está acontecendo. Então, são várias as questões envolvidas quando falamos da promoção da transparência. É um sistema que deve ter o governo como um ator fundamental; a sociedade civil organizada e as ONGs que trabalham nessa área também. É preciso ter toda uma concertação para que o governo publique de forma adequada e faça sua parte, para que a sociedade tenha condição de fiscalizar e o cidadão se capacite cada vez mais para poder usar esses dados. Isso é algo bastante complexo, mas nós estamos caminhando.

"A LEI DE ACESSO À INFORMAÇÃO É FUNDAMENTAL, É UM INSTRUMENTO QUE TODO REGIME DEMOCRÁTICO TEM QUE TER. MAS AS PESSOAS AINDA ESTÃO UTILIZANDO MUITO POUCO ESSA LEI E O ESTADO AINDA NÃO ESTÁ PREPARADO PARA RESPONDER."

RCE – *E quanto à Lei de Acesso à Informação, que obriga os órgãos do governo a disponibilizar os documentos públicos aos cidadãos?*

JM – Sim, ela entrou em vigor em 2012.

RCE – *Mas, por mais que a lei esteja lá, nós ainda não parecemos tê-la incorporado à nossa cultura.*

JM – Tem a cultura do sigilo, o desconhecimento da lei. Se você faz uma lei boa, mas não capacita o funcionário, você tem um problema porque ele mesmo não cumpre a lei. Muitas vezes eles negam alguma informação, mas não sabem que para fazer

isso é preciso ter uma justificativa. Se o dado for sigiloso, ele tem que ser classificado, tem que indicar a autoridade que classificou, o período em que foi classificado, tem que ter o canal para recurso... É raro uma solicitação de informação em que a resposta do setor público atende àquilo que a lei pede. Eu diria que esse é o grande entrave da Lei de Acesso à Informação: a falta de capacitação do Estado para responder às demandas da própria lei. Então, se o cidadão também não conhece a lei, pode ser que ele desista na primeira tentativa. Toda a burocracia tem que se adaptar à lei. E no Brasil, tem aquela coisa: leis que "pegam" e leis que "não pegam". Então nós temos que praticar a lei para que ela "pegue". Se não, ela pode cair no esquecimento. A Lei de Acesso à Informação é fundamental, é um instrumento que todo regime democrático tem que ter, mas as pessoas ainda estão utilizando muito pouco essa lei e o Estado ainda não está preparado para responder. É uma questão até de amadurecimento da nossa sociedade civil, de se organizar e começar a reivindicar mais, e aos poucos ir criando uma"cultura da transparência". E cada vez mais o funcionário público vai se ver não como um "dono" da informação, mas como um "guardião" da informação, no máximo. A informação não pertence a ele. A informação é pública, ela já deve nascer pública. E hoje toda a internet existe para isso, ela propicia essa transparência.

RCE – *O senhor poderia dar alguma indicação de como usar a internet de forma segura?*

JM – Primeira coisa: o ideal seria utilizar um software livre. Eu sei que isso não é fácil. A maior parte das pessoas, e eu também, quando começou a usar computador, utilizava o Windows, você se acostuma a um sistema, então não é fácil mudar. Mas, se tiver oportunidade, pegue uma distribuição que é fácil, como o Ubuntu [sistema operacional de código aberto], instale no computador (ele pode ser instalado em paralelo, sem apagar seus dados) e comece a usar para ir se acostumando, e então faça a migração. Porque com o software livre, você tem uma comunidade por trás, que vai garantir a transparência, a segurança, a estabilidade etc. Isso é a primeira coisa, dar esse salto. A segunda coisa é utilizar criptografia. Isso é algo mais complexo, mas é importante para manter o sigilo das comunicações. Hoje em dia, por exemplo, você tem um *plugin* que adiciona no gerenciador de e-mails e gera duas chaves criptográficas: uma é pública, e você pode trocá-la com seus amigos pela chave pública deles. A outra é uma chave privada, que você usa para abrir as mensagens. Essa é a chamada "criptografia assimétrica". Uma mensagem que foi cifrada com a chave pública só pode ser aberta pela chave privada correspondente. Então, você manda para a pessoa e, com a chave, ela consegue abrir suas mensagens. Você pode escolher algumas pessoas com quem você quer ter comunicação privada. Isso é muito importante para ativistas políticos, dirigentes sindicais e jornalistas. Então, são duas coisas diferentes: garantir a segurança dos dados e nas comunicações. Do ponto de vista político, elas são super importantes hoje em dia.

GUSTAVO SUMARES *graduando em Jornalismo da Escola de Comunicações e Artes da Universidade de São Paulo (ECA-USP) e repórter da Revista Cultura e Extensão USP – e-mail: gsumares@gmail.com*