Documento elaborado en el marco del "PICT-2019-02093 - Préstamo BID” (Directora: Lucía Cantamutto-CIEDIS/UNRN)

Protocolo ético para el registro de interacciones digitales

Las investigaciones con un enfoque cualitativo tienden a tener mayor amparo en la forma en que los datos se generan y resguardan, debido a la profundidad que este tipo de estudios suele alcanzar. Por tanto, es importante que las decisiones metodológicas favorezcan, simultáneamente, la validez externa de la muestra, la calidad de los datos y las consideraciones éticas pertinentes.

La ética atraviesa todas las instancias/etapas de la investigación. Esta premisa no es inherente al campo de estudio del discurso digital pero, en este ámbito, surgen problemas novedosos tales como la trazabilidad de los datos, la identificación de los participantes y las expectativas de privacidad que tienen los usuarios de cada aplicación.

a) trazabilidad de los datos:

A diferencia de las muestras de lengua de intercambios ocurridos presencialmente, los enunciados escritos y las imágenes, tal como ha sido señalado por de-Matteis (2016: 245), refiere a la posibilidad de que “un texto que el investigador selecciona como dato para su uso y reproducción explícita pueda ser rastreado e identificado”.

Debido a la posibilidad de que, a partir del texto utilizado como ejemplo, pueda ser rastreada la identidad del colaborador, el investigador debe realizar diferentes procesos de anonimización y/o reconstrucción de los enunciados para evitar la identificación del informante: cualquiera de los sistemas de comunicación digital tiene mayor persistencia que la comunicación oral (Gobato, 2014: 220–221) y, por lo tanto, será en mayor o menor medida recuperable.

b) identificación de los participantes

Ligado a la trazabilidad, la posibilidad de identificar a los participantes tiene varias aristas. Por un lado, por la identificación de los nombres que pueden ser (pseudo)anonimizados a partir de diversas técnicas (cambio por nombres ficticios, enmascaramientos, por ejemplo). Para evitar la identificación de los participantes, es necesario eliminar datos de direcciones, nombres de negocios, barrios, teléfonos, así como cualquier otra información sensible. En el caso particular de las interacciones digitales escritas, acceder a estas conversaciones implica irrumpir en la vida privada de los usuarios e involucrar información que puede perjudicar a otras terceras personas.

c) expectativas de privacidad

Diversas discusiones se han desarrollado en torno a la ética de las investigaciones que utilizan datos de fuentes públicas de internet sin pedir consentimiento a los usuarios o a los dueños de las plataformas en las que ocurre el discurso, cuyos límites no están en la dicotomía público/privado (Estalella y Ardèvol, 2007). En tal sentido, los autores señalan que la postura ética y epistemológica de los investigadores puede ser contradictoria. En una síntesis de aportaciones de otras investigaciones donde se reflexiona en torno a la cuestión

del grado de privacidad/publicidad y los permisos requeridos para trabajar con esas muestras de lengua. En las discusiones iniciales algunos autores, como Herring (1996b), señalan que algo que se encuentra en un espacio *público* manifiesta carácter *público* aún incluso cuando las expectativas de *privacidad* que suponen los participantes no siempre coinciden con la visión de los investigadores (Walther, 2002). Otros grupo de trabajos proponen criterios más concretos –relacionados con la arquitectura tecnológica del sitio– que aluden a factores como presencia/ausencia de contraseña para el acceso a la información, políticas de resguardo, o sensibilidad del tópico que se trata (Bruckman, 2004). Un tercer aspecto a considerar son las cláusulas legales que las páginas, redes sociales y dispositivos tengan respecto a los contenidos que ahí se producen. Estalella y Ardèvol (2007) recuperan la noción *expectativas de privacidad* de los usuarios. La noción de *comunidad* complementa esta idea, como otro límite difuso que influye sobre este continuum: es la sensación de relativa privacidad entre los miembros de dicha comunidad, como, por ejemplo, *Twitter*. Los autores finalizan esta reflexión con las siguientes ideas: “En primer lugar, la percepción de lo público y lo privado puede variar según la posición del sujeto observador (externa o interna al colectivo) y por tanto, no podemos juzgar “desde fuera” sin tener en cuenta la percepción de los actores. En segundo lugar, el tipo de tecnología o la arquitectura tecnológica, no determina el carácter privado o público de un espacio de interacción, depende una vez más de la percepción que tienen los usuarios sobre lo que están haciendo, es resultado de la negociación y del sentido que le atribuyen a esas interacciones cada colectivo. En tercer lugar, y como corolario, lo público y lo privado no son categorías absolutas que podamos determinar “a priori” con relación a las interacciones de internet, son contextuales y dependen de la negociación que cada colectivo lleve a cabo” (Estalella y Ardèvol, 2007: s/p.).

En cualquier caso, cada investigador deberá sopesar la *trazabilidad* entre el enunciado y el usuario y si se disponen de recursos para evitar la identificación, sin caer en el supuesto de que los datos de la CMC en internet son fácilmente accesibles (Herring, 2002: 110). Si bien un usuario puede utilizar un blog como espacio de interacción público eso no implica que los materiales contenidos ahí estén a disposición de un investigador. Lo mismo sucede con las redes sociales públicas como *Twitter*, en cuyo caso, la temática abordará será un factor decisivo para solicitar consentimiento y autorización al usuario. En esta línea, de-Matteis (2016: 245) sugiere:

> Además de estos factores inherentes a la seguridad de las cuentas en distintas plataformas, en la identificación de la fuente de un enunciado resulta clave la indexación del texto en los principales buscadores en línea. En el caso de las redes sociales, los textos no son indexados y sus autores están –en cierta medida– protegidos. Sin embargo, las plataformas que adoptan el etiquetado de los enunciados (los denominados hashtags) introducen una nueva manera de encontrar al emisor de un texto determinado desde *dentro* de la plataforma.

En tal sentido, se deben implementar diversas estrategias para proteger a los participantes voluntarios de cualquier investigación, respetando su autonomía y cuidando de no afectar su privacidad. En particular, a partir de la firma de autorizaciones y consentimientos informados por parte de todos los interactuantes y, en el caso de que fueran menores, preferentemente también por parte de sus padres.

El protocolo que hemos seguido en esta investigación no ofrece riesgos potenciales para los participantes ya que los resultados publicados han sido a partir de datos totalmente anonimizados (Christians, 2000: 145) y que no son rastreables a través de los buscadores. En definitiva, como toda investigación, se aboga por criterios éticos básicos y generales indicados en el *Informe Belmont* (1979) –beneficencia, respeto, justicia (véase Mertens, 2006: 33) – así como las aplicaciones correspondientes: 1) consentimiento informado, 2) evaluación de riesgos y beneficios y 3) selección de sujetos.

1) Consentimiento informado y consenso expreso

El acceso a toda la información relativa a la investigación en la cual los sujetos formarán parte, y el consecuente conocimiento de lo que sucederá con los datos obtenidos tras su participación en el estudio. En general, esta información se incluye en el consentimiento informado:

a) Procedimiento de la investigación.

b) Propósitos, riesgos y beneficios previstos.

c) Concesión al sujeto para hacer preguntas sobre la investigación y retirar su participación en cualquier momento.

Sin embargo, esta lista no acabada de información que tiene que brindar el documento entra en conflicto cuando se le brindan datos al sujeto participante respecto a la investigación que puede invalidar la misma. En tal caso, se debe explicitar que una vez finalizada la muestra se consignará la información completa (*Informe Belmont*, 1979).

Los consentimientos pueden ser orales o escritos. Sin embargo, en nuestro proyecto, utilizaremos preferentemente consentimientos escritos y expresos.

Por un lado, al comienzo de la recolección. Por otro, en los casos en los que sea posible, al finalizar la recolección de datos se solicitará autorización expresa para utilizar el conjunto de intercambios de la investigación.

2) evaluación de riesgos y beneficios

En todos los casos, se priorizará minimizar los posibles daños a los participantes, anonimizando las muestras, eliminando toda información que pudiera resultar perjudicial para los participantes y que permitiera identificarlos. Asimismo, se eliminarán todas las fotografías (indicándose solo descriptivamente el contenido) y los audios serán transcritos y luego eliminados para evitar identificar a los participantes.

3) selección de sujetos

La selección de los participantes será a partir del contacto prolongado previo con los investigadores. De ese modo, se garantizará una mayor riqueza contextual de los datos. En

segundo lugar, se priorizará la técnica de bola de nieve para poder acceder a otros grupos etarios y a otros dominios de uso.